Honeywell

Experion PKS
C200/C200E Troubleshooting and Maintenance Guide

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-XX10-en-431A	431	0	February 2015

Disclaimer

Contents

1 About This Document

Provides information to help maintain and troubleshoot C200/C200E control hardware components hardware. It also includes information about using the Network Tools (Ntools) and DBadmin utilities as well as the Series C Firmware Load Tool (CTool) utility.

Revision history

Revision	Date	Description
A	February 2015	Initial release of the document.

2 Isolating C200/C200E Faults

This document focuses on the process of C200/C200E Process Controller Fault Isolation.

To support this process, this section includes descriptions of diagnostic tools and definitions of various fault indicators. It then assists the user with fault isolation through a series of questions and hyperlinks that eventually take the user to fault definitions and corresponding recovery recommendations.

You can use this information to either address a specific fault or to better understand C200/C200E Process Controller diagnostic tools and fault symptoms.

This manual focuses on the C200/C200E Process Controller, which includes any component within a Controller or remote I/O chassis, as well as the interconnecting networks and I/O devices.

The C200E Controller is an enhanced C200 Controller with additional user memory and an enhanced function block set. The C200E Controller provides increased user memory from 4 MB to 16 MB.

> **Attention**
> The operational states and the front panel displays of the C200E Controller are same as the C200 Controller.

2.1 Related Documentation References

Additional troubleshooting and maintenance information can be found in the following Implementation Guides for the given functions listed in the following table.

Function	Reference
Fault Tolerant Ethernet Bridge	In Fault Tolerant Ethernet Bridge Implementation Guide
DeviceNet Interface	In DeviceNet Implementation Guide
Fieldbus Interface	In Series A Fieldbus Interface Module User's Guide
HART I/O	In HART I/O Implementation Guide
PROFIBUS Interface	In PROFIBUS Implementation Guide
Rail I/O	In Rail I/O Series A Implementation Guide In Rail I/O Series H Implementation Guide
PM I/O Processors	In PM I/O Troubleshooting and Maintenance Guide

2.2 To Learn More

About …	Then go to …
Why the C200/C200E module faulted	• "C200/C200E Battery Extension Module (BEM) Fault Isolation" on page 43
	• "ControlNet Interface (CNI) Fault Isloation" on page 45
	• "C200/C200E CPM Fault Isolation" on page 47
	• "C200/C200E RM Fault Isolation" on page 48
Fault Indicators	Front Panel Indicators:
	• "Battery Extension Module (BEM)" on page 50
	• "ControlNet Interface (CNI)CNI Normal Runtime Displays" on page 50
	• "Control Processor Module (CPM)" on page 54
	• "Series A Chassis Input Modules" on page 58
	• "Series A Chassis Output Modules" on page 59
	• "C200/C200E I/O Link Interface Module (IOLIM)" on page 66
	• "C200/C200E Serial Interface Module (SIM)" on page 60
	• "C200/C200E Redundancy Module (RM)" on page 63
	Fault Codes
	• "CNI Fault Codes" on page 68
	• "C200/C200E CPM Fault Codes" on page 70
	• "Exchange Block ERRCODE Fault Codes" on page 87
	• "Series A Chassis I/O Fault Codes" on page 105
	• "C200/C200E RM Fault Codes" on page 107
	Experion Notifications
	• "CPM FB Generated Notifications" on page 374
	• "Network Diagnostic Manager (NDM) Detected Notifications" on page 378
	• "Network Diagnostic Manager Generated Notifications" on page 380
	Redundancy Module Events
	• "About RM Log" on page 392
	• "CNI Generated C200/C200E RM Events" on page 393
	• "CPM Generated C200/C200E RM Events" on page 418
	• "C200/C200E RM Generated Events" on page 443
	Test Sequence Numbers
	• "C200/C200E CPM" on page 484
	• "C200/C200E RM" on page 488
	• "Serial Interface Module (SIM)" on page 493
Corrective Actions	• "General Corrective Actions" on page 499
	• "Battery Extension Module (BEM) Corrective Actions" on page 499
	• "ControlNet Interface (CNI) Corrective Actions" on page 500

About …	Then go to …
	• "C200/C200E Control Processor Module (CPM) Corrective Actions" on page 501
	• "CPM_CA21" on page 505
	• "C200/C200E Rack and Supply Corrective Action" on page 505
	• "C200/C200E Redundancy Module (RM) Corrective Action" on page 506
Diagnostic Tools & Utilities	• "NetworkTools (NTools) for Chassis Based Components (C200/C200E)" on page 528
	• "Series A Chassis and Rail I/O Maintenance Tool" on page 538
	• "Using C200/C200E CPM Tools" on page 552
	• "Database Administration Utility (DBADMIN)" on page 559
	• "Series CSeries C Firmware Load Tool (CTool) for Series C Components" on page 593
	RM (Workstation) Displays
	• "Redundancy Module Displays" on page 515
	• "Redundancy Terminology" on page 516
	• "Accessing C200/C200E RM Displays" on page 518
	• "RM Summary (CB) or Main (Stn) Panes" on page 519
	• "RM Profiles (CB and Stn) Panes" on page 520
	• "RM Configuration (CB and Stn) Panes" on page 521
	• "RM Synchronization (CB) and Synch (Stn) Panes" on page 522
	• "Redundant Chassis Profiles (CB and Stn) Panes" on page 523
	• "RM Display (CB) Pane" on page 524
	• "RM Server Parameters (CB) Pane" on page 525
Reporting a problem	• "Effective Trouble Reporting" on page 607
Spare Parts	• "ControlNet Interface (CNI) Spare Parts" on page 610
	• "Periodic Maintenance Parts for C200/C200E Controller" on page 613

2.3 C200/C200E Battery Extension Module (BEM) Fault Isolation

Related topics

"Fault Isolation Table" on page 43

"Background" on page 43

"Out-Of-The-Box Assembly Required for BEM" on page 44

"Out-Of-The-Box Capacity of BEM" on page 44

2.3.1 Fault Isolation Table

If ...	then ...
the BEM OK LED is off,	Ensure chassis power is applied and/or BEM is fully inserted into the chassis. If the BEM OK LED remains off, then go to BEM Corrective Action "BEM_CA01" on page 499.
the BEM OK LED is solid red,	Go to BEM Corrective Action "BEM_CA02" on page 499.
If the BEM OK LED is solid green,	No action is required. The BEM is operating normally.

2.3.2 Background

The BEM is a separate, singlewide module that plugs into the Controller chassis. It incorporates the standard ICP plastic module cover and front door. Connection to the chassis backplane is though the standard ICP connector.

The Battery Extension Module (BEM) provides battery backup power for volatile memory IC's contained within chassis modules, such as the Control Processor Module (CPM). The battery backup is useful for maintaining memory contents, such as configuration databases, during temporary power outages and weekend shutdowns.

Three (3) series-connected, sub-C size, nickel-cadmium cells constitute the battery pack. Its sourcing capacity is rated at 1200mAh. In terms of what is required by the CPM, this means it can provide 10 milliamps of DC current at 3.6 volts for a period of 120 hours on a full charge. This figure represents the worst-case scenario for CPM operation. The CPM typically draws 5 milliamps at reference temperature conditions and with nominal components.

> **Attention**
>
> Since aging occurs, even if the batteries have been regularly recharged throughout their lifetime, the NiCad battery pack Honeywell model TC-BATT03 should be replaced after every two years of operation.

There is self-test circuitry on the BEM that periodically tests for battery pack presence and the battery-pack under load. These tests are performed only when chassis power is present.

A front panel LED shows the state (health) of the battery system. An integral status contact supports a user supplied annunciatior circuit for external/remote alarming in the event of battery deterioration or failure. The normally-open relay contact remains closed (and the normally-closed contact remains open) when the BEM is able to provide 3.0 to 3.6 Vdc battery backup power. The normally-open relay contact opens (and the normally-closed contact closes) when the BEM is not able to provide at least 3.0 Vdc battery backup power.

2.3.3 Out-Of-The-Box Assembly Required for BEM

The BEM is shipped from the factory without the battery pack installed. Please refer to the *Control Hardware Installation Guide* for battery pack installation details.

2.3.4 Out-Of-The-Box Capacity of BEM

Since Ni-Cd batteries have a high self-discharge rate, we recommend that users let the BEM module installed in a powered chassis for 24 hours prior to use. Technically, it takes 30 to 32 hours to fully charge a set of completely discharged batteries. However, from a practical standpoint, completely discharged batteries can never be charged. What typically happens is that a user receives a BEM module with a battery pack charged from 60% to 80% capacity available.

2.4 ControlNet Interface (CNI) Fault Isloation

Related topics

2.4.1 CNI Not Compatible

Diagnostic check

On the RM Detail display (either Summary pane or Synchronization pane) the large list shows the Compatibility (4th column) for the CNI as INCOMPATIBLE? When I look at the 4 character display of the CNI I see '!CPT'.

Cause

CNIs are not compatible. Incompatibility may occur for several reasons:

1. Mismatch between hardware revisions.
2. Mismatch between firmware version.
3. Mismatch between configured ControlNet parameters.

Solution

Launch NetworkTools with the appropriate switch/option, select a suspect CNI and click the toolbar button that looks like a blue wrench. Go to the Present Keeper Tab. You may need to reprogram you CNI's network parameters. See "Invalid Keeper" on page 386 notification for more information.

Solution

Select the suspect CNI in NetworkTools and click on the toolbar button that has the letters 'ID'. Record the Product Type and Product Code values. Do the same on the partner CNI. If the two do not match. Replace the one that is not Type 'c' and Code '8'.

2.4.2 Incorrect CNI Keeper Values

Diagnostic check

My CNI show the words KPR ERR. NetworkTools just popped up a dialog box indicating bad Network values. My Monitoring pane has started to show red for many items.

Cause

Bad network parameters.

Solution

Launch NetworkTools with the appropriate switch/option, select a suspect CNI and click the toolbar button that looks like a blue wrench. Go to the Present Keeper Tab. You may need to reprogram you CNI's network parameters. See "Invalid Keeper" on page 386 notification for more information.

Solution

Cycle power to the CNI.

2.4.3 NTools Related Questions

Diagnostic check

I have a large system and NetworkTools CNI Stats display shows many non-concurrences. Is there a way to diagnose ControlNet parameters? I am planning an upgrade and know my ControlNet parameters should change. Do I need to do this to all CNIs?

Cause

ControlNet parameters may need to change.

Solution

Launch NetworkTools with the appropriate switch/option, select a suspect CNI and click the toolbar button that looks like a blue wrench. Go to the Present Keeper Tab. You may need to reprogram you CNI's network parameters. See "Invalid Keeper" on page 386 notification for more information. If you are creating a network with parameters other than those in the previous discussion, you must reprogram all CNIs on that network (and potential spares). You can diagnose the parameters by using the first toolbar button in NetworkTools. Go the to Options tab. Check the box called Enable ControlNet Parameter Checking. NetworkTools will perform a diagnostic each time it is launched, if the checkbox is clicked ON or after a change of network parameters. This check only uses the standard Experion values (it is no utility for non-standard network parameteres).

Solution

Refer to the Installation manual and the Planning manual.

2.4.4 General CNI Questions

Diagnostic check

In a pinch can I use a CCR012 in a remote I/O chassis? In a pinch can I use a CCN01x as a buddy node in a redundant media system?

Cause

Spares/emergencies questions.

Solution

At this time a CCN011 cannot be used as a buddy node in a redundant media system. A CCR012 or CCR013 can be used in a remote I/O chassis.

Solution

Try the current CNI module TC-CCN014 or TC CCR014. Call TAC

2.5 C200/C200E CPM Fault Isolation

Related topics

"C200/C200E Flash ROM Programming Errors" on page 47
"C200/C200E Fault Isolation Table" on page 47

2.5.1 C200/C200E Flash ROM Programming Errors

Errors and faults encountered in the process of programming CPM Application and/or Boot firmware are not addressed in this document. In general, an error programming the Application personality shall permit repeated attempts, while an error programming the Boot personality may require returning the module to the factory.

2.5.2 C200/C200E Fault Isolation Table

If the . . .	Then See . . .
CPM is stuck displaying the same Test Sequence Number for more than 30 seconds,	"C200/C200E CPM Test Sequence Numbers" on page 484
CPM is in the Fail State,	"C200/C200E CPM Fault Codes" on page 70
CPM Health LED is solid red,	"CPM_CA05" on page 502
problem persists,	"CPM_CA06" on page 502
CPM Battery LED is solid red,	"CPM_CA07" on page 503
CPM is being used in a redundant configuration and unable to synchronize.	"CPM_CA03" on page 502

2.6 C200/C200E RM Fault Isolation

If …	then …
'THxy' on stalled RM front panel display. ('xy' represents any 2 alphanumeric characters)	The RM has failed a startup test. Go to RM "C200/C200E RM Test Sequence Numbers" on page 488
'Exyz' error code on RM front panel display. ('xyz' represents any 3 alphanumeric characters)	The RM has encountered a run-time error. Go to the corresponding code at "C200/C200E RM Fault Codes" on page 107
'OK' LED solid red on RM front panel. (with no 'Exyz' error code displayed).	The RM has encountered a severe run-time error. First, take RM Corrective Action "RM_CA02" on page 507. If the problem persists, take RM Corrective Action "BEM_CA01" on page 499. And if it still persists, take General Corrective Action "GEN_CA01" on page 499

3 C200/C200E Front Panel Indicators

Related topics

3.1 Battery Extension Module (BEM)

The only BEM front panel indicator is the OK LED.

Related topics

"BEM - OK LED" on page 50
"ControlNet Interface (CNI)CNI Normal Runtime Displays" on page 50
"CNI Abnormal Displays" on page 51
"CNI Controller Redundancy Specific Displays" on page 52
"CNI Common questions" on page 53

3.1.1 BEM - OK LED

This Display:	Means:	Corrective Action:
Off	No Power.	See "BEM_CA01" on page 499.
Toggling Red/Green	N/A	N/A
Flashing Green	N/A	N/A
Flashing Red	N/A	N/A
Solid Green	The battery voltage is within spec (3.0V to 4.6V), and a simple hardware diagnostic passes.	N/A
Solid Red	The battery voltage is out of spec and/or something is wrong with the module	See "BEM_CA02" on page 499.

3.1.2 ControlNet Interface (CNI)CNI Normal Runtime Displays

A ControlNet interface module in either a standalone or redundant configuration normally displays the following messages. Note that the messages are listed in the sequence in which they are displayed.

4 Character Display Message	Description of Cause
(A,#,x,x)	Address indication where xx indicates the ControlNet Mac ID.
(,O,K, ,)	CNI is operating normally
'Redundancy State'	Refer to "CNI Controller Redundancy Specific Displays" on page 52 if CNI resides in a redundant chassis.
(%,C,x,x)	Percentage of CPU usage where xx is in the range 00 - 99%. Because of display limitations, the maximum value displayed will be 99% even if CPU usage reaches 100%.
(K,p,x,x)	Module's keeper state, where xx can be one of the following abbreviations:
	Ov - the keeper is powering up or off line with valid keeper information that may or may not match the network keeper signature.
	Oi - the keeper is powering up or off line with invalid keeper information.
	Av - the keeper is the active network keeper, with valid keeper information, whose keeper signature defines the network keeper signature.
	Iv - the keeper is an inactive network keeper with valid keeper information that matches the network keeper signature.
	Ai - the keeper is the active network keeper either with invalid keeper information or with a keeper signature that does not match the network keeper signature.

4 Character Display Message	Description of Cause
	Ii - the keeper is an inactive network keeper either with invalid keeper information or with a keeper signature that does not match the network keeper signature.
(n,C,x,x)	Number of open connections used by the CNI, where xx is in the rage of 00 to 64 connections.
(n,U,x,x)	Number of unconnected buffers used by the CNI, where xx is in the range of 00 to 20 buffers.
(B,x,n,n)	Number of bandwidth exceeded occurrences since the last power cycle or module reset, where nn is in the range of 00 to 99 occurrences after which the display rolls over to 00 and continues counting.
	A bandwidth exceeded error occurs whenever module has all its receive buffers in use at the same time and an additional buffer is needed. At that point, the module clears all of the received buffers thus destroying their contents, in an effort to recover from the resource overload.
	A bandwidth exceeded error might also occur when the module firmware is flash updated. In this case, clearing of the buffers is necessary to begin the flash update process. This error is automatically cleared after the flash process by way of the module reset after the flash update.
	The bandwidth exceeded count display is disabled until the first bandwidth exceeded event is detected. Once one has occurred, the display will remain activated and be a part of the display sequence. The count and display is cleared whenever the module is reset or power cycled.

3.1.3 CNI Abnormal Displays

A ControlNet interface module in either a standalone or redundant configuration can display the following messages.

OK Status Light	4 Character Display Message	Description of Cause	Corrective Action
GREEN	(I,N,I,T,)	CNI is performing post powerup initialization.	Wait
GREEN	(,O,K, ,)	CNI is operating normally	None needed
FL.RED	(R,O,M, ,U,P,D,T)	flash loading from application is in progress	Wait
GREEN	(,S,W, ,E,R,R,)	Mac ID Switch changed after powerup or when in a redundant secondary, Mac ID not set the same as primary.	Adjust switch settings
FL.GRN	(C,N,F,G,E,R,R,)	ControlNet Config error	Call SSC
RED	(A,D,D,R,E,R,R,)	Two node 1's, or node set to 00 or node 99 if redundant	Adjust switch settings
RED	(R,A,C,K,E,R,R,)	Cannot read backplane EPROM or rack/slot address incorrect	Call SSC
RED	(D,U,P,L,N,O,D,E)	There is another node on the network at the same address (May be a temporary condition during redundant switchover)	Adjust switch settings (unless temporary condition during switchover)
FL.GRN	(N,E,T, ,E,R,R,)	CNI cannot find network connection	Check that all drop cables are attached, check for faulty drop, check cabling in general
RED	(C,N,I,C,E,R,R,)	Cnet ASIC Error	Call SSC

OK Status Light	4 Character Display Message	Description of Cause	Corrective Action
RED	(B,P,I,C,E,R,R,)	Backplane ASIC error	Call SSC
RED	(B,P,R,X,E,R,R,)	Backplane receiver error	Call SSC
RED	(B,P,A,#,E,R,R,)	Backplane address # (slot number) error	Call SSC
GREEN	(,B,W, ,>,M,A,X)	Bandwidth exceeded, temporary Cnet scheduling problem	wait
RED	(S,T,O,P,)	CNI commanded to stop functioning by the Redundancy Module (Occurs when a non redundancy compliant CNI is placed into a redundant secondary chassis)	Check that the stopped CNI is redundancy capable (TC-CCx012 or TC-CCx013 where x equals N or R)

3.1.4 CNI Controller Redundancy Specific Displays

A redundant compliant ControlNet interface module in only a redundant configuration can display the following messages.

OK Status Light	4 Character Display Message	Description of Cause	Corrective Action
RED	(W,A,I,T, ,R,M,)	CNI waiting for the Redundancy Module to complete powerup	wait
GREEN	(P,w,D,S)	CNI is primary with a disqualified secondary partner	Synchronize Secondary
GREEN	(P,w,Q,g)	CNI is primary with a qualifying secondary partner	wait
GREEN	(P,w,Q,S)	CNI is primary with a qualified secondary partner	None needed
GREEN	(P,w,N,S)	CNI is primary with a no secondary partner	Inspect secondary
GREEN	(Q,U,A,L)	Primary CNI is qualified with its partner	wait
GREEN	(C,M,P,T)	Secondary CNI is compatible with its partner	wait
GREEN	(D,I,S,Q)	Secondary CNI is disqualified	Synchronize Secondary
GREEN	(Q,f,n,g)	Secondary CNI is qualifying	wait
GREEN	(,Q,S,)	Secondary CNI is qualified	None needed
GREEN	(D,S,N,P)	Secondary CNI is disqualified with no partner	Inspect partner and RMs

The following messages would be displayed only if the CNI module failed during transition from one phase to another and are provided as diagnostic tools.

OK Status Light	4 Character Display Message	Description of Cause	Corrective Action
GRN/off	(S,O, ,1)	Old primary switchover phase 1 in progress	
GRN/off	(S,O, ,2)	Old primary switchover phase 2 in progress	
GRN/off	(S,O, ,3)	Old primary switchover phase 3 in progress	
GRN/off	(S,N, ,1)	New primary switchover phase 1 in progress	
GRN/off	(S,N, ,2)	New primary switchover phase 2 in progress	
GRN/off	(S,N, ,3)	New primary switchover phase 3 in progress	

OK Status Light	4 Character Display Message	Description of Cause	Corrective Action
GRN/off	(s,e,t,C)	CNI set to be compatible with its partner	
GRN/off	(s,e,t,!)	CNI set to not be compatible with its partner	
GRN/off	(?,C,p,t)	CNI has not determined if it is compatible	
GRN/off	(!,C,p,t)	CNI has determined that it is not compatible	See "CNI Not Compatible" on page 45

3.1.5 CNI Common questions

Question	Answer
My CNI shows the word !CPT. Is this an error?	A display of !CPT is not normal and needs corrective action. See "CNI Not Compatible" on page 45.
My CNI shows the word FAULT or ASSERT scrolling across it. Is this an error?	If the CNI is displaying FAULT or ASSERT or the health LED is solid Red, copy down the exact sequence of symbols being shown on the 4 character display. See "Getting CPM Breadcrumbs in NetworkTools" on page 536 and "Getting RM Events in NetworkTools" on page 535 from the Primary and Secondary, if this is a Redundant C200/C200E Controller. Cycle power to the chassis.

3.2 Control Processor Module (CPM)

The C200/C200E front panel indicators include two LEDs and the Alphanumeric Display.

Related topics

"C200/C200E OK LED" on page 54
"C200/C200E Battery LED" on page 54
"C200/C200E 4-Character Display" on page 55

3.2.1 C200/C200E OK LED

The OK LED, on the right, indicates the overall health of the C200/C200E.

This Display:	Means:	Corrective Action:
Off	No Power.	Check the "CPM_CA01" on page 501.
Toggling Red/ Green	N/A	N/A
Flashing Green	While in the CPM Alive, Ready or Loading States (i.e. executing CPM Boot firmware), the flashing green Health LED serves as a heartbeat indication that the module is functioning properly. However, the module is not capable of performing control.	Load CPM firmware "CPM_CA02" on page 501.
	While in the CPM Backup State (i.e. executing CPM Application FW), the flashing green Health LED serves as a heartbeat indication that the module is functioning properly. However, synchronization with the primary redundant partner has not yet been achieved.	Isolate reason for loss of synchronization "CPM_CA03" on page 502.
	While in the CPM is in one of the NotLoaded, NoCEE, or Idle state, the flashing green Health LED indicates that the module is operating as expected.	N/A
Flashing Red	Indicates that the CPM is currently in the Fail State (i.e. executing CPM Boot firmware).	Recover from CPM Fail State "CPM_CA04" on page 502.
Solid Green	The Health LED is only ever solid green when executing CPM Application firmware. While the Alphanumeric Display indicates that the CPM is in one of the Run or Backup States, a solid green Health LED indicates the module is operating as expected. Furthermore, while in the CPM Backup State, a solid green LED indicates that the secondary CPM is synchronized with its primary partner.	N/A
Solid Red	Upon initial CPM startup, the Health LED is solid red until the CPM successfully completes startup diagnostics and settles in the Application or Boot personality.	N/A
	If after CPM startup has completed or CPM startup halted (i.e. Alphanumeric Display indicating the same test sequence number for more than 30 seconds) a major fault has occurred. The CPM must be restarted and/or replaced.	Restart the CPM "CPM_CA05" on page 502.

3.2.2 C200/C200E Battery LED

The Battery LED, on the left, indicates whether the C200/C200E is capable of retaining any loaded control strategy after AC power loss.

> **Attention**
> - A green battery LED indication only indicates that a battery is present and at the proper voltage. It is not an indication of how much backup time remains. You must install a new Honeywell model TC-BATT01 battery to assure full backup capacity.
> - Refer to the "Recommended replacement parts" on page 613 section for more information on the battery replacement schedules.

This Display:	Means:	Corrective Action:
Off	No Power.	Check the CPM "CPM_CA01" on page 501.
Toggling Red/ Green	N/A	N/A
Flashing Green	N/A	N/A
Flashing Red	N/A	N/A
Solid Green	Upon initial CPM startup, the Battery LED is solid green until the completion of the Alphanumeric Display test so that all LED colors can be checked by the factory test technician.	N/A
	After the CPM settles in the Application or Boot personality, a solid green Battery LED indicates that the startup diagnostics have been successfully completed, and that one, and only one, battery is present and of proper voltage.	N/A
Solid Red	During CPM startup, the Battery LED is solid red until the completion of the startup diagnostics.	N/A
	After the CPM settles in the Application or Boot personality, a solid red Battery LED indicates the battery is defective/missing or an invalid battery configuration exists.	Replace defective battery or correct invalid battery configuration "CPM_CA07" on page 503.

3.2.3 C200/C200E 4-Character Display

The purpose of the Alphanumeric Display is to provide a local view of the status of the C200/C200E only; it is not meant to provide any definitive information about other modules residing in the same chassis.

This display:	Means:	Take this action:
ALIV	The startup diagnostics have successfully completed but no Application firmware exists. ICP Communication is enabled and the CPM remains in the CPM Alive State until the user commands Application firmware download which results in the transition to the CPM Loading State.	Load CPM firmware "CPM_CA02" on page 501.
BKUP	The CPM startup diagnostics have successfully completed and the CPM is executing the Application personality. Furthermore, the CPM is in the secondary redundancy role. Note that whether the secondary CPM has achieved synchronization with its primary partner or not is indicated by the Health LED.	N/A
BOOT	Upon completing the CPM startup diagnostics, the CPM enters the transient Booting State during which the operating system is started. Prior to starting the operating system within the Application FW, the Alphanumeric Display is updated to display 'BOOT'. The CPM normally transitions to the NotLoaded, NoCEE, Idle, Run, or Backup State within 30 seconds. Initially, ICP Communication is not active, but it is enabled prior to completion of the Booting State.	N/A

This display:	Means:	Take this action:
	An abnormal condition exists if the CPM remains in the Booting State for more than 30 seconds. Note that if a RM is present in the chassis, the CPM remains in the Booting State while the RM performs its startup diagnostics.	Check the RM "CPM_CA08" on page 503.
FAIL	A fault condition was encountered which results in the termination of any control activity. A transition to the CPM Fail State may occur from any CPM State. ICP communication is enabled in an attempt to remain visible so that error information may be queried from the failed module.	Recover from CPM Fail State "CPM_CA04" on page 502.
IDLE	The CPM is executing the Application personality firmware in the Idle State. Although a control strategy is loaded, the control strategy in inactive. Note that if the CPM was in the Run State prior to a Retention Startup, the CPM State is forced to Idle so that the user may judge whether it is safe to immediately go on control (e.g. based upon the length of the power down).	Activate CPM control strategy "CPM_CA09" on page 503 .
IISC	A backplane send related error has occurred and is stored in memory Likely cause is removal and insertion of a module under power or hardware defect in the backplane or module's board. The C200/C200E continues to operate. Refer to the IISR code for more information. The system generates an alarm and the LED indicators display the alarm. The Rockwell modules crash under the same conditions and the system must be restarted immediately.	N/A
IISQ	A backplane message queue related error has occurred and is stored in memory. Likely cause is removal and insertion of a module under power or hardware defect in the backplane or module's board. The C200/C200E continues to operate. Refer to the IISR code for more information. The system generates an alarm and the LED indicators display the alarm. The Rockwell modules crash under the same conditions and the system must be restarted immediately.	N/A
IISR	Both IISC and IISQ errors have occurred at least one time and are stored in memory. Note that while C200/C200Es continue to operate after the occurrence of backplane errors, their performance is degraded. When the number of backplane errors exceeds the tolerance threshold, the C200/C200E will no longer be able to communicate.	To clear the display, disconnect the battery and restart the CPM "CPM_CA21" on page 505
LOAD	Upon commencing Application or Boot personality firmware download (user commanded action), the CPM transitions from the CPM Alive/Ready/Fail State to the CPM PI Loading State. The CPM remains in the transient CPM PI Loading State throughout the firmware download operation.	N/A
	Upon encountering an error programming the CPM Application or Boot personality, reattempt the firmware download operation. Note that an error programming the Boot personality may require the CPM to be returned to the factory to be reprogrammed.	Reload CPM firmware "CPM_CA02" on page 501.
NODB	The CPM is executing the Application personality firmware in the NotLoaded State. This implies that no control strategy exists. Note that the CPM State remains NotLoaded until the first load of the CPM FB. If power is lost before the load of the CPM FB, the CPM State settles back into the NotLoaded State after powerup.	Create/Load CPM control strategy "CPM_CA10" on page 503.

This display:	Means:	Take this action:
	If the CPM was in the Idle or Run State prior to loosing power, Retention Startup may not have been possible due to a very long power down or a marginal battery.	Replace defective battery or correct invalid battery configuration "CPM_CA07" on page 503.
NOEE	The CPM is executing the Application personality firmware in the NoCEE State. The transient NoCEE State is visible between the load of the CPM FB and the CEE FB. Since the user initiated load of the CPM FB automatically loads the CEE FB, the CPM normally transitions to the Idle State.	N/A
	An abnormal condition exits if the CPM remains in the NoCEE State. This implies that the CPM FB was loaded but the CEE FB has not been loaded.	Reload the CPM FB "CPM_CA11" on page 503.
PASS	Upon completing the CPM startup diagnostics, the CPM enters the transient Booting State during which the operating system is started. Prior to starting the operating system within the Boot FW, the Alphanumeric Display is updated to display 'PASS'. The CPM normally transitions to the Alive, Ready, or Fail State within 30 seconds. Initially, ICP Communication is not active, but it is enabled prior to completion of the Booting State.	N/A
	An abnormal condition exists if the CPM remains in the Booting State for more than 30 seconds. Note that if a RM is present in the chassis, the CPM remains in the Booting State while the RM performs its startup diagnostics.	Check the RM "CPM_CA08" on page 503.
RDY	The CPM is executing the Boot personality firmware in the Ready State. A valid Application personality exists. ICP Communication is enabled. The CPM remains in the CPM Ready State until the user either commands Application FW download or issues the Start command. The CPM transitions to the CPM Loading State in the former case or reboots into the Run, Idle, NoCEE, NotLoaded or Backup State in the latter case, respectively.	Restart the CPM "CPM_CA05" on page 502.
RUN	The CPM is executing the Application personality firmware in the Run State. This implies a control strategy is loaded and the control strategy in active.	N/A
Txxx	Upon being released from reset, the CPM enters the transient Testing State during which the CPM executes startup diagnostics. Prior to executing each diagnostic, a test sequence number, 'Txxx', is posted to the Alphanumeric Display so that if a test fails or hangs, the Alphanumeric Display indicates the test that was in progress at the time of failure. The test of longest duration takes much less than 30 seconds to complete.	N/A
	An abnormal condition exists if the CPM remains displaying the same Test Sequence Number for more than 30 seconds.	Interpret the CPM Test Sequence Number "C200/C200E CPM Test Sequence Numbers" on page 484.
wait	Once the new Application or Boot firmware is loaded, the CPM disappears from the ICP backplane while the personality is programmed into flash ROM. The CPM reboots within 30 seconds.	N/A
	An abnormal condition exists if the CPM remains displaying 'wait' for more than 30 seconds.	Restart the CPM "CPM_CA05" on page 502.
WDT	Indicates the CPM Watchdog Timer has timed-out.	Recover from CPM Watchdog Timer Timeout "CPM_CA13" on page 503.

3.3 Series A Chassis Input Modules

Display:	LED:	Means:	Take this action:
OK	Steady green light	The inputs are being multicast and in normal operating state.	None.
OK	Flashing green light	The module has passed internal diagnostics but is not multicasting inputs or it is inhibited	None.
OK	Flashing red light	Previously established communication has timed out.	Check controller and chassis communication.
OK	Steady red light	The module must be replaced.	Replace the module.
I/O State	Yellow	The input is active.	None.
I/O Fault	Red	A fault has occurred for this point.	Check this point at the controller.

3.4 Series A Chassis Output Modules

Display:	LED:	Means:	Take this action:
OK	Steady green light	The outputs are actively controlled by a system processor.	None.
OK	Flashing green light	The module passed internal diagnostics, but is not actively controlled, or is inhibited.	None.
OK	Flashing red light	Previously established communication has timed out.	Check controller and chassis communication.
OK	Steady Red light	The module must be replaced.	Replace the module.
I/O State	Yellow	The output is active.	None.
I/O Fuse	Red	A short overload fault has occurred for this point.	Check wiring for short overload.
I/O Fault	Red	A fault has occurred for this point.	Check this point at the controller.

3.5 C200/C200E Serial Interface Module (SIM)

Related topics

3.5.1 SIM 4-Character Display

This Display:	Means:	Corrective Action:
Tnnn	Selftest - Current Test Sequence Number.	If the SIM stalls with one of these numbers displayed, replace the SIM.
TEST	Factory Test Mode. Entered on command or because the backplane test signal was asserted.	Can be loaded.
PASS	Completed Selftest. Attempting to execute Boot.	None.
ALIV	Running in Boot; no personality is present.	Can be loaded.
WDT	(LED Green/Red) Factory Test Mode Commanded WDT test - waiting for timeout interrupt. Health LED will turn from GREEN to RED upon WDT timeout.	None.

This Display:	Means:	Corrective Action:
ALIV	Running in Boot; no personality is present.	Can be loaded.
RDY	Running in Boot; personality is present but shut down.	Can be loaded or started.
LOAD	Running in Boot with an open loader connection.	None.
BOOT	Completed Selftest. Attempting to execute personality.	None.
wait	Attempting to program Flash ROM. (Health LED is RED during actual programming)	None.
stop	Shutting down (transitional)	None.
WDT	Watchdog Timer Fault. A power cycle is required to recover the module.	If the problem persists, call SSC.

3.5.2 SIM Display of Runtime Information

The SIM will alternately display module status and status of channels A and B.

This Display:	Means:	Corrective Action:
OK	Running in personality - alternates with display of channel states.	None.
A ok B ok	Channel is operating normally, communicating with FTA, and FTA is communicating with attached device.	

This Display:	Means:	Corrective Action:
Aerr Berr	Channel cannot communicate with FTA	
A st B st	Channel can communicate with FTA but FTA is reporting a soft failure. Information about the error can be obtained through pcmana or NTools.	
Acfg Bcfg	Channel is being configured. This is normally a transient display. A bad configuration will make it appear permanent.	

3.5.3 SIM Display of Failure Information

When the CPM is in the Fail state, the alphanumeric display will alternate the numeric fail code and 'FAIL'.

This Display:	Means:	Corrective Action:
FAIL alternating with nnnn	Software error nnnn has occured. Running in Boot. Can be loaded, recovered or restarted.	A power cycle is required to recover the module. If the problem persists, contact SSC.
WDT	Watchdog Timer Fault.	A power cycle is required to recover the module. If the problem persists, contact SSC.
WDT	(Let from Green to Red) Factory Test Mode Commanded WDT test - waiting for timeout interrupt. Health LED will turn from GREEN to RED upon WDT timeout.	None

3.5.4 SIM Health Indicator

The Health LED is used to indicate the general state of the module.

This Display:	Means:	Corrective Action:
OFF	No power; significant fault.	None
Solid RED	During load it means programming the Flash ROM. Selftest in progress or failed - accompanied by a test number in Alphanumeric display; Hardware Fault, unrecoverable WDT Timeout.	A power cycle is required to recover the module. If the problem persists, contact SSC.
Flashing RED	Fail State, running under software control.	
Alternating RED/GREEN	Factory Test Mode.	
Solid GREEN	OK - At least one I/O data connection active.	
Flashing GREEN	During load it means getting ready to program Flash ROM. During run, it means no active I/O connection.	

3.5.5 SIM Channel Activity Indicators

There is a status/activity indicator for each channel of A and B.

This Display:	Means:	Corrective Action:
OFF	No activity - Alive	
Flashing GREEN	Transmit or Receive in progress, but not normal continuous communications.	

This Display:	Means:	Corrective Action:
Brief GREEN flash every 0.5 sec	FTA is not present or not communicating - a retry is performed every 0.5 second.	
Solid GREEN	Normal communications with FTA produces continuous illumination.	

3.5.6 Cannot connect to serial devices

Diagnostic check

See MVIP report

Cause

Not available on the web

Solution

3.5.7 Serial Interface (SI) communication timeout

Diagnostic check

1. Check the SI to 3rd party device communication cable.
2. Response not available from 3rd party system.
3. Check the SI card configuration

Cause

1. SI card to 3rd party communication cable fault
2. 3rd party system offline
3. SI card configuration problem

Solution

1. Replace faulty cable.
2. Replace failed SI card.

3.6 C200/C200E Redundancy Module (RM)

Related topics

3.6.1 RM OK LED

This Display:	Means:	Corrective Action:
Off	No Power	
Toggling Red/ Green	Powerup LED Self Test	Wait
Flashing Green	Module OK, but not communicating with other chassis modules	
Flashing Red	Configured Improperly or Non-Critical Failure or NVS Update	
Solid Green	OK	
Solid Red	Critical module Failure or RM Powerup Self Test	-- Wait

3.6.2 RM PRI LED

This Display:	Means:	Corrective Action:
Off	No Power or RM Powerup Self Test or Redundancy State = SECONDARY or RM Failed	
Toggling Red/ Green	Powerup LED Self Test	
Flashing Green	N/A	--
Flashing Red	N/A	--
Solid Green	Redundancy State = PRIMARY	
Solid Red	N/A	--

3.6.3 RM COM LED

This Display:	Means:	Corrective Action:
Off	No Power or RM Powerup Self Test	
Toggling Red/ Green	Powerup LED Self Test	
Flashing Green	No (or intermittent) partner connections.	
Flashing Red	N/A	--
Solid Green	Normal partner communications.	
Solid Red	Partner connection occurred.	

3.6.4 RM 4-Character Display

RM Startup/Selftest Mode

This Display:	Means:	Corrective Action:
(all pixels on)	Visual test. The display will flash twice to allow the user to quickly check the condition of the display.	
THnx	RM startup self test, Phase I. T - designates a startup test. H - designates the Self Test subsystem. n x - Numeric Subtest ID. The 'n' signifies a number. When this character is a number, the RM is executing test code out of its flash ROM. Most of the tests are against the RM's RAM. The Subtest ID is presented at the start of a test and held only for the duration of a test. Most tests execute too quickly for the operator to read the code. However, should a test fail, the RM will tend to hold the display so the user can identify the failed test.	
TH**	RM self test decompressing its executive code into RAM, after which the RM will begin executing out of RAM.	
THax	RM startup self test, Phase II. T - designates a startup test. H - designates the Self Test subsystem. a x - Alphabetic Subtest ID. The 'a' signifies a letter. When this character is a letter, the RM is executing test code out of its RAM. Most of the tests are against non-RAM subsystems, and require the use of RAM-based functions such as the stack and exception handlers. The Subtest ID is presented at the start of a test and held only for the duration of a test. Most tests execute too quickly for the operator to read the code. However, should a test fail, the RM will tend to hold the display so the user can identify the failed test.	
????	RM resolving its initial Redundancy State. During this time, the RM will wait for other modules to complete startup, then it will gather information and work its way through a series of tests to ascertain its position in the Primary/ Secondary relationship.	

RM Normal/Operational Mode

This Display:	Means:	Corrective Action:
PRIM	Primary - This RM and its chassis' modules are responsible for the chassis' Assigned Functions.	
DISQ	Disqualified Secondary - The RM and its chassis' modules are a backup to the Primary, but are not able to carryout the Primary chassis' Assigned Functions. The other chassis modules may either be Disqualified or Synchronizing when then RM is in the Disqualified state.	

This Display:	Means:	Corrective Action:
SYNC	Synchronized Secondary - The RM and its chassis' modules are a backup to the Primary, in a Synchronized state, and able to carry out the Primary chassis' Assigned Functions, should a switchover occur.	

RM Fault/Failure Mode

This Display:	Means:	Corrective Action:
Exxx	Indicates a major fault (Error) situation, where 'xxx' represents an error code.	
(Error Brief)	An Error Brief summarizes the cause.	
(Recovery Message)	A Recovery Message summarizes the recommended user action.	
(Pause)	A 1 second pause to delimit the Exxx - Error Brief - Recovery Message sequence.	

RM Firmware Upgrade Mode

This Display:	Means:	Corrective Action:
BOOT	Boot mode - awaiting further instructions	
ERAS	Boot mode - erasing firmware	
PROG	Boot mode - loading new firmware	

3.7 C200/C200E I/O Link Interface Module (IOLIM)

Related topics

"IOLIM 4-Character Display and 'OK' LED" on page 66
"IOLIM LINK Status LEDs" on page 66

3.7.1 IOLIM 4-Character Display and 'OK' LED

The IOLIM has one four-character display and three two-color LEDs on its front panel. The LEDs provide Link 1 status, Link 2 status, and module health status (OK). The following table summarizes some typical indications for reference.

OK LED is . . .	And, 4-Character Display shows . .	Then, IOLIM is . . .
Solid Red	TEST	Factory test mode
	T###	Executing hardware diagnostic tests (display shows T###, where ### is the test number)
Solid Green	BOOT	Booting firmware
Flashing Green/off	ALIV	No application loaded
	RDY	Ready for firmware upgrade
	LOAD	Loading firmware
Solid Red	PROG	Downloaded firmware is being programmed into Flash ROM
	FAIL	Failed
Solid Green if secondary is synchronized. Flashing green if secondary is not synchronized.	BKUP	Secondary IOLIM
Solid Green if there are CDA connections to the module. Flashing green if no CDA.	NODB	No database
	NOEE	IOLIM block loaded, IOLINK block not loaded.
	OK	IOLIM block loaded and running.
	OK - SF (display alternates OK and SF)	IOLINK detects a soft failure.

3.7.2 IOLIM LINK Status LEDs

Two LEDs indicate the status of Link A and Link B. The following table describes possible conditions.

If CHANNEL A or B LED is . . .	Condition
Solid Red	IOLIM self test
Flashing Red	Channel communications error
Solid Green	Channel communications OK
Flashing Green	Channel communications warning

4 C200/C200E Fault Codes

Related topics

4.1 CNI Fault Codes

The CNI utilizes a fault reporting protocol that pinpoints the location in CNI firmware where an illegal condition occurs.

The fault is reported via a 3 part message shifted across the CNI front panel display. The 3 message parts include:

Fault Type	'ASSERT' or 'FAULT'
	(Note: The difference between these two terms is inconsequential.)
Source file name	e.g., 'smacisr.c'
Line number (within file)	e.g., '0733'

In the event a CNI enters such a faulted (a.k.a. Asserted) state, reset the CNI via "CNI_CA02" on page 500.

go to "GEN_CA01" on page 499.

Related topics

"CNI0101 reporting UMAX exceeded errors" on page 68

"UMAX error alarms on CNI" on page 68

"ControlNet cable failure alarms" on page 69

"UMAX exceeded alarms from supervisory CNI in C200 chassis that also contains a supervisory FTEB" on page 69

4.1.1 CNI0101 reporting UMAX exceeded errors

Diagnostic check

1. Verify if the CNI has been set for UMAX of 20 or 24.

    > **Attention**
    > - The UMAX should be set to 20 when it is a downlink device (I/O network).
    > - The UMAX should be set to 24 (or 32) when it is an uplink device on the supervisory network.

2. Check if cable length is less that of 1000 feet.

Cause

Incorrect UMAX settings for the CNI card.

Solution

Configure the ControlNet parameters as per the guidelines.

4.1.2 UMAX error alarms on CNI

Diagnostic check

CNI card setting

Cause

CNet parameters configured for Master keeper are incorrect or there is no master keeper.

Solution

Configure the ControlNet parameters per guidelines in KB.

4.1.3 ControlNet cable failure alarms

Diagnostic check

ControlNet cable failure alarms

Cause

ControlNet cable problem of CNI card failure

Solution

1. Check A and B cables of the supervisory network.
2. Check A and B cables of the I/O network.

4.1.4 UMAX exceeded alarms from supervisory CNI in C200 chassis that also contains a supervisory FTEB

Diagnostic check

UMAX exceeded alarms from supervisory CNI in C200 chassis that also contains a supervisory FTEB.

Cause

This occurs in an FTE supervisory installation where a PCIC is also installed to communicate to a CL5550. The chassis with the CL5550 must contain both an FTEB and a CNI. The Network Diagnostic Manager (NDM) defaults to use the FTE network to discover active modules. In doing so, NDM recognizes the CNI as an IO network downlink. The IO network's UMAX is limited to 20. If the CNI has a UMAX configured greater than 20, the error occurs.

Solution

Configure UMAX in affected CNI to 20 and set all MAC IDs on associated ControlNet network within the range of 1 to 20.

> **Attention**
> * The UMAX must be set to 20 for downlink CNIs.
> * The UMAX must be set to 24 (or 32) for uplink CNIs.

4.2 C200/C200E CPM Fault Codes

Upon detection of a hard fault or critical failure, the CPM reboots into the Fail State. Hardware permitting, ICP communications to the module is enabled. An 'error block' is generated (at the time of failure) to store information useful in diagnosis following the occurrence of a fault. The error block survives power cycles as long as no RAM parity/edac errors are introduced (i.e. single battery of proper voltage is present).

Each discernible type of detectable fault is assigned a unique faultcode. If the CPM generated fault code is not defined in one of the following subsections, perform the following general corrective action. First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

Related topics

4.2.1 0x0000

The CPM faulted without generation of a fault code.

Cause

Software defect or memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.2 0x0002

The CPM encountered an unexpected Machine Check fatal exception.

Cause

Memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.3 0x0003

The CPM encountered an unexpected Data Access fatal exception.

Cause

Memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.4 0x0004

The CPM encountered an unexpected Instruction Access fatal exception.

Cause

Unable to access ROM and/or memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.5 0x0006

The CPM encountered an unexpected Alignment fatal exception.

Cause

Memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.6 0x0007

The CPM encountered an unexpected Program fatal exception.

Cause

Memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.7 0x0008

The CPM encountered an unexpected Floating Point Unavailable fatal exception.

Cause

Memory corruption.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.8 0x000D

The CPM encountered an unexpected Trace fatal exception.

Cause

Defective CPU (since this feature is only enabled in a development scenario).

Solution

Replace the CPM "CPM_CA06" on page 502.

4.2.9 0x0013

The CPM encountered an unexpected Instruction Address Breakpoint fatal exception.

Cause

Defective CPU (since this feature is only enabled in a development scenario).

Solution

Replace the CPM "CPM_CA06" on page 502.

4.2.10 0x0014

The CPM encountered an unexpected System Management Interrupt fatal exception.

Cause

{1} Watchdog Timer timeout.

{2} ICP ASIC Fault signal asserted.

Solution

First, recover from the CPM Fail State "CPM_CA04" on page 502. If the problem persists, replace the CPM "CPM_CA06" on page 502.

4.2.11 0x0401

PLTCLLSInvalidCrashCodeRange

Cause

Software defect (i.e. impossible condition that should never occur).

Solution

4.2.12 0x0402

PLTCLLSCantReserveCEEDB

Cause

Solution

4.2.13 0x0403

PLTCLLSCantReleaseCEEDB

Cause

Solution

4.2.14 0x0404

CEEUBTCantGetIdForStartUpTask

Cause

Solution

4.2.15 0x0405

CEEUBTCantSendCompleteToStartUpTask

Cause

Solution

4.2.16 0x0406

CEEUBTErrorOnWaitForStartUpTask

Cause

Solution

4.2.17 0x0407

CEEUBTCantGetIdForCEEUBTask

Cause

Solution

4.2.18 0x0408

CEEUBTCantGetPriorityForCEEUBTask

Cause

Solution

4.2.19 0x0409

CEEBTCantGetIdForStartUpTask

Cause

Solution

4.2.20 0x040A

CEEBTCantSendCompleteToStartUpTask

Cause

Solution

4.2.21 0x040B

CEEBTErrorOnWaitForStartUpTask

Cause

Solution

4.2.22 0x040C

CEEBTCantSetUpCycleTimingEvent

Cause

Solution

4.2.23 0x040D

CEEBTErrorOnWaitForFirstCycleTimingEvent

Cause

Solution

4.2.24 0x040E

CEEBTErrorOnWaitForNthCycleTimingEvent

Cause

Solution

4.2.25 0x040F

CEEBTCantGetIdForCEEBTask

Cause

Solution

4.2.26 0x0410

CEEBTCantGetPriorityForCEEBTask

Cause

Solution

4.2.27 0x0411

CEEBTCantCreateCEEFB

Cause

Solution

4.2.28 0x0412

CEEBTCantCreatePCMFB

Cause

Solution

4.2.29 0x0413

CFCMFBMAssignXferInstSize

Cause

Solution

4.2.30 0x0414

CFCMFBExecuteDFLOX

Cause

Solution

4.2.31 0x0415

CFCMFBUnBindBlocks

Cause

Solution

4.2.32 0x0416

CEEBTCantAllocateSchedulerMemory

Cause

Solution

4.2.33 0x0417

CEEBTCantAllocateBlockManagerMemory

Cause

Solution

4.2.34 0x0418

CEEBTCantAllocateConnectionManagerMemory

Cause

Solution

4.2.35 0x0419

CEEBTCantCreatePhysicalPool

Cause

Solution

4.2.36 0x041A

CEEBTCantCreateMemoryManager

Cause

Solution

4.2.37 0x041B

BMCantAccessRCOAMemory

Cause

Solution

4.2.38 0x041C

CCLITCantGetIdForStartUpTask

Cause

Solution

4.2.39 0x041D

CCLITCantSendCompleteToStartUpTask

Cause

Solution

4.2.40 0x041E

CCLITErrorOnWaitForStartUpTask

Cause

Solution

4.2.41 0x041F

CCLMBindCallOutWasCalled

Cause

Solution

4.2.42 0x0420

CCLITMinorVersionChangeFailed

Cause

Solution

4.2.43 0x0421

CEEBTCantAllocateBlockTypeManagerMemory

Cause

Solution

4.2.44 0x0422

CEEBTCantAllocateCCLManagerMemory

Cause

Solution

4.2.45 0x0423

CCLITAcquireLibrariesFailed

Cause

Solution

4.2.46 0x0424

CCLITCantGetIdForCEEBTask

Cause

Solution

4.2.47 0x0425

CEEBTCantGetIdForCCLITask

Cause

Solution

4.2.48 0x0426

CEEBTCantSendInitEventToCCLITask

Cause

Solution

4.2.49 0x0427

CEEBTErrorOnWaitForCCLITask

Cause

Solution

4.2.50 0x0428

CCLITUnloadLibrariesFailed

Cause

Solution

4.2.51 0x0429

CEEBTCantSendEventToCCLITask

Cause

Solution

4.2.52 0x042A

CCLITCantGetIdForCEEUTask

Cause

Solution

4.2.53 0x042B

CFCMFBCfInitialize

Cause

Solution

4.2.54 0x042C

CEEUBTInvalidTaskIDForGuaranteedStore

Cause

Solution

4.2.55 0x042D

ROLETCantGetROLETaskPriority

Cause

Solution

4.2.56 0x042E

ROLETCantSetCCLITaskPriority

Cause

Solution

4.2.57 0x042F

ROLETCantGetIdForCCLITask

Cause

Solution

4.2.58 0x0430

ROLETCantSendEventToCCLITask

Cause

Solution

4.2.59 0x0431

CEEUBTSharedRamDecodeFailure

Cause

Solution

4.2.60 C200/C200E controller will not load or activate

Diagnostic check
1. Check the CPM/FTEB status.
2. Check the ControlNet status.

Cause
1. Controller not in database
2. ControlNet cable problem

Solution

4.2.61 Unable to download to controller from Control Builder

Diagnostic check
1. Verify that the controller is powered on.
2. Check the controller firmware.

Cause
1. Controller has no power.
2. Controller firmware is incorrect version.

Solution
Load correct controller personality before starting with the project.

Diagnostic check
1. Is the supervisory network connected and terminated properly?
2. Verify the CNI MAC address.

Cause
1. ControlNet link is not terminated.
2. CNI MAC addressing is incorrect.

Solution
Terminate the ControlNet links and have regular preventive maintenance checks.

4.2.62 Unable to load new C200/C200E for the first time

Diagnostic check

'Unable to connect to CEE.'

Check the APP image of the C200/C200E using NTools.

Cause

CPM module is shipped with no APP. The controller needs to be flashed.

Solution

After installing a new C200/C200E controller, check its APP using NTools.

4.2.63 Unable to load a C200/C200E with different data

Diagnostic check

Get error invalid CEE.

Verify that the C200/C200E does not show 'No DB' in the display area on the board.

Cause

C200/C200E already has data loaded and will not permit loading another set of data over it.

Solution

Clean the memory of the C200/C200E before loading new data.

4.2.64 Cannot download to C200/C200E from Control Builder on a client

Diagnostic check

Check user password for inconsistencies.

Cause

Password for that user changed on the Experion Server.

Solution

Maintain an updated list of users and their passwords.

4.2.65 Redundant C200/C200E return to RUN after power failure

Diagnostic check

Check the LED display on CPM module for NODB (No database)

Cause

After power failure, the primary C200/C200E needs to return to power first, otherwise, the data can be scrubbed.

Solution

1. Ensure that the old primary C200/C200E is powered up first.
2. Should have separate power circuits so that both primary and secondary won't lose power at the same time.

4.2.66 C200/C200E process input data does not update

Diagnostic check

1. Verify that the controller status is ACTIVE.
2. Verify that the controller has no OVERRUNS.

Cause

1. Loss of communication with the controller.
2. Controller is downloading.

Solution

1. Reduce the load configuration of the controller.
2. Balance the controller load across the execution cycle.

4.2.67 Control execution is stopped while exchanging data between C200/C200E and Rockwell PLCs

Diagnostic check

Check if the PLC MSG instructions are overloading the C200s/C200Es.

Cause

Control strategies that exchange data between C200/C200E and Rockwell PLCs do so by running C200/C200E Exchange Blocks and PLC relay ladder MSG instructions. MSG instructions have a communication option named 'Cache Connections.' When this option is selected, the connections are kept open.

However, when this option is not selected, every time a PLC executes a MSG instruction, it opens a connection, transfers data, and closes the connection. The opening and closing of each connection for every MSG instruction execution at relay ladder scan rates overloads the C200/C200E. When C200/C200E detects this overload condition, under which they are unable to maintain communications, it stops executing.

This intended behavior is beneficial with redundant C200Es in case of an overload due to a hardware fault. The overload detection results in a switchover to the partner which is anticipated to be free of fault. However, in case of improper ladder program configuration, the C200E which has newly taken control immediately experiences the overload and also stops executing.

Solution

1. Configure the MSG instructions with the 'Cache Connections#8221; communication option selected.

   Note: Do not configure more than the number of Exchange Blocks specified. For more information, refer to the section C200/C200E communication performance (Peer-to-Peer Capacity using Exchange FB) in *Control Builder Components Theory*.
2. Restart the C200/C200E.

4.2.68 Cannot acknowledge C200/C200E alarm

Diagnostic check

1. Check the actual status of process conditions to verify if the alarm condition still exists.
2. Check the alarm limits of the point.

Cause

Process does not return to normal after alarm occurs.

Solution

4.2.69 Commands to process devices in C200/C200E are not working

Diagnostic check

1. Check if you can communicate with C200/C200E via Control Builder.
2. Check the Uplink CNI Status.
3. Check the FTEB Status.

Cause

1. Failure of Server to C200/C200E communication.
2. Failure of CDA subsystem services.

Solution

4.2.70 Commands to I/O points in C200/C200E are not working

Diagnostic check

1. Check the Downlink CNI status
2. Check the cable status.

Cause

Failure of Downlink ControlNet communication.

Solution

4.2.71 Commands to FTA devices are not working

Diagnostic check

1. Check if the correct field wire is terminated on the FTA.
2. Check the marshalling cabinet fuse.

Cause

1. Loose cable on FTA/Marshalling
2. Blown fuse in Marshalling

Solution

Regular preventive maintenance to check if all connections are tight.

4.2.72 Control program is not executing correctly

Diagnostic check

Check the logic of the Sequential Control Module (SCM).

Cause

Incorrect logic

Solution

Check the logic before implementing the final solution.

4.2.73 Alarm journal gets CEE overruns

Diagnostic check

Overruns in the CPU cycle

Cause

Control strategy phasing and overloading

Solution

Plan your control strategy as per the phasing guidelines in KB.

4.3 Exchange Block ERRCODE Fault Codes

Communication errors and errors reported by the target device are stored without being modified in the ERRCODE parameter of request type Exchange function blocks. All of the PCCC errors and some of the other errors are generated by the target device. Please refer to the Allen-Bradley documentation for additional information about these errors. The fault codes for some common errors are listed below for convenient reference.

Related topics

4.3.1 1

Error name

CONNECTION_FAILED

Cause

A connection could not be established from the CPM to the target device. Possible reasons for this error include:

- An invalid relative path was specified.
- A ControlNet cable on the path between the CPM and the target is broken or has been disconnected.
- The target device or an intermediate CNI on the path between the CPM and the target is powered off.
- The specified maximum number of target devices has been exceeded.

Solution

4.3.2 2

Error name

INSUFFICIENT RESOURCE

Cause

There are insufficient resources in the CPM for this array block.

Solution

Make sure that the specified maximum number of request array blocks in the CPM has not been exceeded. Delete other array blocks that are no longer being used to free resources in the CPM.

4.3.3 3

Error name

INVALID VALUE

Cause

An invalid value has been specified for one or more elements in the array.

This error is generated when the Numeric Array block has been configured as a Write block and one or more values of PV fall outside the limits imposed by the TGTDATATYPE.

For example, if TGTDATATYPE is specified as SIGNEDINT16 and one or more values of PV in the array fall outside the integer range of 16-bit Signed Integers (-32768 to +32767) or are NaNs, this error will be generated.

The entire Write operation will fail (even for PV values that are in range).

Solution

Make sure that the values of PV fall within the appropriate range before attempting the Write operation.

4.3.4 4 - IOI SYNTAX

Error name

IOI SYNTAX

Cause

An invalid tag name has been specified as the FILENAME for a CIP Read or Write operation.

If this error occurs for a PCCC Read or Write, this error indicates that communication is not supported between the CPM and the target device or the specified version of the DHRIO module.

Solution

4.3.5 4 - UNKNOWN DESTINATION ADDRESS

Error name

UNKNOWN DESTINATION ADDRESS

Cause

An invalid tag name (or tag name index) has been specified as the FILENAME for a CIP Read or Write operation.

If this error occurs for a PCCC Read or Write, this error indicates that communication is not supported between the CPM and the target device or the specified version of the DHRIO module.

Solution

4.3.6 8

Error name

SERVICE UNSUPPORTED

Cause

The specified operation is not supported by the target device.

Solution

4.3.7 12

Error name

OBJECT IN WRONG STATE

Cause

The current state of the target device prevents the execution of the specified operation.

Solution

4.3.8 14

Error name

ATTRIBUTE CANNOT BE SET

Cause

The write operation cannot be completed because the value being modified cannot currently be set.

Solution

4.3.9 15

Error name

PERMISSION DENIED

Cause

Permission is denied to carry out the specified operation.

Solution

4.3.10 17

Error name

REPLY WON'T FIT

Cause

The response message is corrupt or is larger than expected and so cannot be processed.

Solution

4.3.11 19

Error name

NOT ENOUGH DATA

Cause

The data received in the response is smaller than expected.

Solution

4.3.12 21

Error name

TOO MUCH DATA

Cause

The data received in the response is larger than expected.

Solution

4.3.13 22

Error name

CONFIGURED RESPONDER NOT FOUND

Cause

The responder block configured in the requestor is not available in the target node. Possible reason for this error is an Invalid responder block name.

Solution

Make sure that the configured responder block exists and is loaded properly in the target node.

4.3.14 31

Error name

CONNECTION RELATED FAILURE

Cause

There is a connection-related failure due to communication problems in the path between the CPM and the target device.

Solution

4.3.15 34

Error name

INVALID REPLY

Cause

The data size or data type of the response is incompatible with the type of array block being used for CIP access. Note that the Flag Array Block can only access Binary (BOOL) files, the Numeric Array block can only access Integer (SINT, INT, DINT) and Single Precision Floating Point (REAL) files, and the Text Array block can only access ASCII files.

Solution

4.3.16 255

Error name

Wrong Data

Cause

There is something wrong in your data that you are writing.

Solution

Check for NaN.

4.3.17 512

Error name

PCCC Error

Cause

Cannot guarantee delivery, link layer timed out or received a NAK.

Solution

4.3.18 768

Error name

PCCC Error.

Cause

Duplicate token holder detected by link layer

Solution

4.3.19 1024

Error name

PCCC Error

Cause

Local port is disconnected.

Solution

4.3.20 1280

Error name

PCCC Error

Cause

Application layer timed out waiting for a response.

Solution

4.3.21 1536

Error name

PCCC Error

Cause

Duplicate node detected.

Solution

4.3.22 1792

Error name

PCCC Error

Cause

Node is off-line.

Solution

4.3.23 2010

Error name

Peer Connection Error

Cause

Internal error or resource constraint in the CEE's processing of a peer connection.

Solution

Be sure system resources are not being exceeded. The maximum number of Exchange blocks per CPM is 32. Contact technical assistance.

4.3.24 2047

Error name

PCCC Error

Cause

User initialy configured large number of Number Of Values and made them visible. Then, user changed Number Of Values to a smaller number than the visible pins.

Solution

User must re-configure original large number of Number Of Values and remove any extra pins.

4.3.25 2048

Error name

PCCC Error

Cause

Hardware Fault.

Solution

4.3.26 2089

Error name

PCCC Error

Cause

User has tried to configure more than the maximum number of parameter connectors on this Control Module (CM). The maximum number is 1000 per CM.

Solution

Reduce number of parameter connectors per CM.

4.3.27 2304

Error name

PCCC Error

Cause

Can't find address in routing table.

Solution

4.3.28 2560

Error name

PCCC Error

Cause

Illegal LSAP value.

Solution

4.3.29 4096

Error name

PCCC Error

Cause

Illegal command or format.

For example, addressing file 13 that does not exist, will generate this error. Or, addressing a file as N7:0 but the file is a Bit file, will generate this error..

Solution

Change command or format.

4.3.30 8192

Error name

PCCC Error

Cause

Node has a problem and will not communicate.

Solution

4.3.31 12288

Error name

PCCC Error

Cause

Remote node is not there, disconnected or shutdown.

Solution

4.3.32 16384

Error name

PCCC Error

Cause

Node could not complete function due to hardware fault.

Solution

4.3.33 20480

Error name

PCCC Error

Cause

Addressing problem or memory protect rungs.

Solution

4.3.34 24576

Error name

PCCC Error

Cause

Function disallowed due to command protection selection.

Solution

4.3.35 28672

Error name

PCCC Error

Cause

Processor is in program mode.

Solution

4.3.36 32768

Error name

PCCC Error

Cause

Compatibility mode file missing or communication zone problem.

Solution

4.3.37 36864

Error name

PCCC Error

Cause

Remote node cannot buffer command.

Solution

4.3.38 45056

Error name

PCCC Error

Cause

Remote node problem, due to download.

Solution

4.3.39 49152

Error name

PCCC Error

Cause

Cannot execute command, due to active IPBs.

Solution

4.3.40 53248

Error name

PCCC Error

Cause

Cannot route request.

Solution

4.3.41 61441

Error name

PCCC Error

Cause

Illegal Data Table Address Format. A field has an illegal value.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.42 61442

PCCC Error

Cause

Illegal Data Table Address Format. Not enough fields specified.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.43 61443

PCCC Error

Cause

Illegal Data Table Address Format. Too many fields specified.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.44 61444

PCCC Error

Cause

Illegal Data Table Address Format. Symbol not found.

Solution

Check type.

4.3.45 61445

PCCC Error

Cause

Illegal Data Table Address Format. Symbol is zero or greater than the number of characters supported by the target device.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.46 61446

PCCC Error

Cause

Illegal Address. Address does not exist, or does not point to something usable by this command.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.47 61447

PCCC Error:

Cause

Illegal size. File is wrong size. Address is past end of file.

Solution

Check the FILENAME parameter to see if it is a valid PLC-5 Data Table Address and that it refers to a valid location in the target device. The end address (which is determined using the PLC-5 Data Table Address in FILENAME and the number of elements to read/write) must not be beyond the end of the file. Also verify that the array block is not being used to access a file of an unsupported type.

4.3.48 61448

PCCC Error

Cause

Cannot complete request. Situation changed (file size, for example) during operation.

Solution

4.3.49 61449

PCCC Error:

Cause

Data or file too large. Memory is unavailable.

Solution

4.3.50 61450

PCCC Error:

Cause

Request is too large. Transaction size plus word address is too large.

Solution

4.3.51 61451

PCCC Error

Cause

Access is denied, privilege violation.

Solution

4.3.52 61452

PCCC Error

Cause

Resource is not available. Condition cannot be generated.

Solution

4.3.53 61453

PCCC Error

Cause

Resource is already available. Condition already exists.

Solution

4.3.54 61454

PCCC Error

Cause

Command cannot be executed.

Solution

4.3.55 61455

PCCC Error:

Cause

Overflow. Histogram overflow.

Solution

4.3.56 61456

PCCC Error

Cause

No access.

Solution

4.3.57 61457

PCCC Error

Cause

Illegal data type information.

Solution

Verify that the array block is not being used to access a file of an unsupported type.

4.3.58 61458

PCCC Error:

Cause

Invalid parameter. Invalid data in search or command block.

Solution

4.3.59 61459

PCCC Error

Cause

Address reference exists to deleted area.

Solution

4.3.60 61460

PCCC Error

Cause

Command execution failure for unknown reason.

Solution

4.3.61 61461

PCCC Error

Cause

Data conversion error.

Solution

4.3.62 61462

PCCC Error

Cause

The scanner is not able to communicate with a 1771 rack adapter.

Solution

This could be due to the scanner not scanning, the selected adapter not being scanned, the adapter not responding, or an invalid request.

4.3.63 61463

PCCC Error

Cause

The adapter is not able to communicate with the module.

Solution

4.3.64 61464

PCCC Error

Cause

The 1771 module response was not valid (size, checksum, etc.).

Solution

4.3.65 61465

PCCC Error

Cause

Duplicated Label.

Solution

4.3.66 61466

PCCC Error

Cause

File is open - another node owns it.

Solution

4.3.67 61467

PCCC Error

Cause

Another node is the program owner.

Solution

4.3.68 61468

PCCC Error

Cause

Disk file is write protected or otherwise inaccessible.

Solution

4.3.69 61469

PCCC Error

Cause

Disk file is being used by another application, update not performed.

Solution

4.3.70 61470

PCCC Error

Cause

Data Table Element Protection violation.

Solution

4.3.71 61471

PCCC Error

Cause

Unable to execute command due to a temporary internal condition in the target device.

Solution

4.4 Series A Chassis I/O Fault Codes

Related topics

"Cannot activate I/O module" on page 105
"Channel failure alarm" on page 105
"Communication with I/O rack CNI fails" on page 105
"TC-ODX081 Discrete AC Output Module" on page 106

4.4.1 Cannot activate I/O module

Diagnostic check

Check the downlink CNI slot number.

Cause

The downlink slot number is incorrect.

Solution

Addressing should be done based on guidelines.

4.4.2 Channel failure alarm

Diagnostic check

Check the channel status on the card.

Cause

Hardware failure

Solution

Replace the I/O card.

4.4.3 Communication with I/O rack CNI fails

Diagnostic check

Check for any duplicate MAC ID on network.

Cause

Duplicate MAC ID on network.

Solution

- Configure MAC IDs as per the guidelines.
- Maintain a list of already used MAC IDs.

4.4.4 TC-ODX081 Discrete AC Output Module

As indicated in the following table, the TC-ODX081 Discrete AC Output Module provides enhanced output diagnostics for each output channel (Fault Conditions), and channel fault indication on the module front panel and on Station displays (Fault Indications)

Faults	Description
Fault Conditions	
Short Circuit Protection/ Overload	Protects the device from damage by sensing when current draw for a given channel is above the limit.
Loss of Field Power	Senses lack of power for a channel, if zero crossing on the ac-line power is not detected which causes the output state to change.
No Load Detected	Senses when the output current draw falls below the threshold or when a hardware output failure occurs (No load is detected on this channel).
	NOTE: Detection only works when the output is in the OFF state.
Output Verification	Verifies if the actual output state matches the commanded output state for field side verification.
	NOTE: Verification only works when the output is in the ON state.
Pulse Test	Periodically checks the output to verify that it still has the ability to change states without causing the load to transition.
	NOTE: This function only operates in systems with software version R120 or greater.
Fault Indications	
I/O Module front panel	A red number will indicate the channel(s) with the fault condition. To determine the actual fault, call up the Station Detail display for the I/O Module.
Station Alarm Summary display	The Alarm Summary display will indicate the fault condition type and time that the fault occurred.
	NOTE: To determine the actual fault, call up the Station Detail display for the I/O Module.
Station Detail display	The Detail will show the status of each output Channel.

4.5 C200/C200E RM Fault Codes

Related topics

4 C200/C200E FAULT CODES

4.5.1 About fault code format

The fault code is a 4 character alphanumeric string. Valid characters are [0-9,A-Z], except [S, O]. The first character is always 'E'. The second character indicates the subsystem in which the error was detected. The third character indicates the subsystem function or group of functions in which the error was detected. The fourth character enumerates the specific error.

Each subsystem within the RM is assigned a range of fault codes as listed in the following table.

Range	Object	Firmware Directory
E 0 _ _	Backup Control Object	/bcoObj
E 1 _ _	OS Board Support Package	/bsp1.1
E 2 _ _	Chassis Profile Object	/chpObj
E 3 _ _	Coordinated System Time Object	/cstObj
E 4 _ _	Device Object	/devObj
E 5 _ _	Extended Device Object	/edoObj
E 6 _ _	Event Log Object	/eloObj
E 7 _ _	Backup Communications Object	/iSBMcomm
E 8 _ _	ICP toolkit	/icptk
E 9 _ _	Indicator Device Driver	/ind
E A _ _	RM State Machine (JABBA)	/jabba
E B _ _	Event Log Device Driver	/ogDrv
E C _ _	Object Communications	/objComm
E D _ _	Wall Clock Time Object	/wctObj
E E _ _	Non-Maskable Interrupt Service Routine	/nmiIsr
E F _ _	Non-Volatile Storage Object	/nvsObj
E G _ _	RM Fault Handler	/rmFault
E H _ _	Self Test Object	/stObj
E I _ _	Workstation Display Object	/wdObj
E J _ _	Industrial Control Platform Object	/icpObj
E K _ _	RM Watchdog Manager	/dog

A solid red OK LED on any module is a sign of total shutdown/failure (or in process or faulted startup self testing). A RM displaying an Exxx code is a sign of an RM failure, including a sign of an RM's inability to resolve a chassis condition without user intervention. For example, an **E054** code is a signal that the RM has lost contact with another chassis module, but the RM still sees that module as present in the chassis through other back plane signals.

4.5.2 E000

Unable to initialize attributes from the configuration log.

Cause

An error value returned from bcoUpdateAttributes.

Solution

Reset RM ("RM_CA02" on page 507). If error persists, replace RM ("RM_CA01" on page 506).

4.5.3 E001

Unable to register class with ICP Toolkit.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.4 E010

Unable to post event to message queue.

Cause

- An error value returned from msgQSend.
- An event which was to be posted.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.5 E020

Unable to read from incoming event message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.6 E021

RM is in invalid state to perform a chassis state change with the partner going first

Cause

A new state requested.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.7 E022

Invalid value for state change coordination order.

Cause

State change coordination order.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.8 E023

Unable to start watchdog timer used to wait for switchover phasing to complete.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.9 E024

Invalid event sent to the backup control object.

Cause

Event type.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.10 E025

Unable to update attributes from the configuration log.

Cause

An error value returned from bcoUpdateAttributes.

Solution

Reset ("RM_CA02" on page 507) or replace ("RM_CA01" on page 506) RM when convenient.

4.5.11 E026

Unable to write display position to configuration log.

Cause

An error value returned from cfgWriteDisplayPosition.

Solution

Reset ("RM_CA02" on page 507) or replace ("RM_CA01" on page 506) RM when convenient.

4.5.12 E027

Invalid service state parameter for coordinated state change (last chassis).

Cause

Service state parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.13 E028

Invalid service state parameter for coordinated state change (first chassis).

Cause

Service state parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.14 E029

Invalid coordinated state change state.

Cause

Coordinated state change state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.15 E02A

Invalid multicast service state parameter.

Cause

State parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.16 E02B

Invalid coordinated state change state reached.

Cause

State of coordinated state change.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.17 E02C

Invalid multicast service state parameter.

Cause

State parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.18 E02D

Unable to start watchdog timer used to time the chassis state change.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.19 E030

Unable to update attributes from the configuration log.

Cause

An error value returned from bcoUpdateAttributes.

Solution

Reset ("RM_CA02" on page 507) or replace ("RM_CA01" on page 506) RM when convenient.

4.5.20 E031

Unable to open module to RM portion of multicast connection.

Cause

Solution

None.

4.5.21 E032

The slot number value for a module opening module to RM portion of multicast connection exceeds largest possible slot number.

Cause

Solution

None.

4.5.22 E033

Unable to open module to RM portion of multicast connection.

Cause

Solution

None.

4.5.23 E034

The slot number value for a module opening module to RM portion of multicast connection exceeds largest possible slot number.

Cause

Solution

None.

4.5.24 E035

Unable to open connection made to the backup control object from another module (not the multicast connection).

Cause

Solution

None.

4.5.25 E036

Unable to close connection made to the backup control object from another module.

Cause

An error value returned from objCommTargClose.

Solution

None.

4.5.26 E037

Unable to send message to the backup control object event handler message queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.27 E038

Unknown state change request from partner RM.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.28 E039

Unable to allocate a response buffer for a state change request service.

Cause

Solution

None.

4.5.29 E03a

Buffer could not be allocated for Fwd_Close_Reply on multicast connection.

Cause

Solution

None.

4.5.30 E03b

There is no specified response routine to which to forward the Fwd_Close_Reply buffer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.31 E03C

The response routine was NULL for the initiate qualification service request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.32 E03D

Unable to prepare response buffer for the initiate switchover service request.

Cause

Solution

None.

4.5.33 E03E

The response routine was NULL for the initiate switchover service request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.34 E03F

Unable to start watchdog timer used to delay switchover request.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.35 E03G

Unable to prepare response buffer for the coordinated switchover service request.

Cause

Solution

None.

4.5.36 E03H

The response routine was NULL for the coordinated switchover service request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.37 E03I

Unable to prepare response buffer for the report event service request.

Cause

Solution

None.

4.5.38 E03J

The response routine was NULL for the report event service request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.39 E03K

Unable to prepare response buffer for the become primary service request.

Cause

Solution

None.

4.5.40 E03L

The response routine was NULL for the become primary service request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.41 E03M

Unable to start watchdog timer used to delay become primary request.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.42 E03N

Unable to prepare response buffer for the disqualify secondary service request.

Cause

Solution

None.

4.5.43 E03P

Unable to send message to the backup control object event handler message queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.44 E03Q

Unable to send message to the delayed service request handler message queue.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.45 E03R

Unable to send message to the delayed service request handler message queue.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.46 E03T

Unable to send message to the backup control object event handler message queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.47 E03U

The response routine was NULL for the disqualify secondary service request

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.48 E03V

Unable to send message to the delayed service request handler message queue.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.49 E03W

The appTable indicates that connection being closed uses non-ICP (Industrial Control Platform) Port.

Cause

- bcoObjTargAppHandle.
- appTable[bcoObjTargAppHandle].port

Solution

None.

4.5.50 E03X

The bcoLinkConsumerTable indicates that connection has already been closed

Cause

- UcmmReceiveSlotNum (slot in which module closing connection resides).
- bcoLinkConsumerTable[ucmmReceiveSlotNum].

Solution

None.

4.5.51 E03Y

Link consumer could not be freed (does not exist)

Cause

- UcmmReceiveSlotNum (slot in which module closing connection resides).
- bcoLinkConsumerTable[ucmmReceiveSlotNum].

Solution

None.

4.5.52 E03Z

Transport could not be restarted following removal of link consumer.

Cause

Solution

None.

4.5.53 E040

Unable to write autoqualification state to the configuration log.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.54 E041

Unable to write autoqualification option to the configuration log.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.55 E042

Unable to prepare response buffer for set single attribute service request (autoqualification option attribute).

Cause

Solution

None.

4.5.56 E043

The response routine was NULL for set single attribute service request (autoqualification option attribute).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.57 E044

Unable to write program command recognition attribute to the configuration log.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506)..

4.5.58 E045

Unable to prepare response buffer for set single attribute service request (program command recognition attribute).

Cause

Solution

None.

4.5.59 E046

The response routine was NULL for set single attribute service request (program command recognition attribute).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.60 E047

Unable to prepare response buffer for set single attribute service request (password scope attribute).

Cause

Solution

None.

4.5.61 E048

The response routine was NULL for set single attribute service request (password scope attribute).

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.62 E049

Unable to write display position attribute to the configuration log.

Cause

Solution
Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.63 E04A

Unable to prepare response buffer for set single attribute service request (display position attribute).

Cause

Solution
None.

4.5.64 E04B

The response routine was NULL for set single attribute service request (display position attribute).

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.65 E04C

Unable to write autoqualification state to the configuration log.

Cause

Solution
Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.66 E04D

Unable to write autoqualification state to the configuration log.

Cause

Solution
Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.67 E050

An invalid port number has been associated with the multicast connection.

Cause

Solution

None.

4.5.68 E051

Attempting to delete a link consumer which has already been deleted (or never allocated).

Cause

Solution

None.

4.5.69 E052

Unable to delete link consumer.

Cause

Solution

None.

4.5.70 E053

Unable to restart server transport for multicast connection after one of the link consumers timed-out.

Cause

Solution

None.

4.5.71 E054

Unable to restart server transport for multicast connection after one of the link consumers timed-out.

The RM requires operator assistance. It has encountered a situation where another chassis module is not responding to Redundancy status queries but is still responding to low level backplane queries. This error can occur anytime after the RM completes Startup Self Test.

If this RM was hosting a Primary with a Synchronized Secondary, a switchover will occur.

If this RM was hosting a Synchronized Secondary, all other functional chassis modules will enter a Disqualified Secondary state.

Cause

- Bitmap of redundancy compliant modules in chassis (determined by pinging).
- Slot number of module not responding, but the module is still responding to low level backplane interface queries ('pings').

Solution

Reset offending module and the RM.

If the identity of the other module is not obvious from displays or chassis indicators, see the RM Event Log, where and E054 fault should be recorded. The Data 2 field of that event record will specify the slot number of the module that triggered the fault.

Go to RM_CA02.

4.5.72 E060

Invalid event received on connection.

Cause

Event received.

Solution

None.

4.5.73 E07A

Invalid multicast service state parameter.

Cause

State parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.74 E070

Invalid multicast service state parameter.

Cause

State parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.75 E071

Invalid coordinated state change state reached.

Cause

State parameter.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.76 E072

Invalid multicast service state parameter.

Cause
State parameter.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.77 E073

Unknown error code received.

Cause
Error code.

Solution
None.

4.5.78 E074

Unknown extended error code received.

Cause
Extended error code.

Solution
None.

4.5.79 E075

Invalid extended error size.

Cause
Extended error size.

Solution
None.

4.5.80 E076

Unknown error code received..

Cause

Error code.

Solution

None.

4.5.81 E077

Invalid service response code received.

Cause

Service response code.

Solution

None.

4.5.82 E078

Invalid multicast service state parameter.

Cause

State parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.83 E079

Invalid coordinated state change state reached.

Cause

State of coordinated state change.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.84 E080

Invalid service parameter for qualification service response.

Cause

Service parameter.

Solution

None.

4.5.85 E090

Invalid service state parameter for coordinated state change (last chassis).

Cause

Service state parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.86 E091

Invalid service state parameter for coordinated state change (first chassis).

Cause

Service state parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.87 E092

Invalid coordinated state change state.

Cause

Coordinated state change state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.88 E093

Invalid multicast service state.

Cause

Multicast service state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.89 E0A0

New state is invalid.

Cause

New state.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.90 E0A1

New state is invalid (for last chassis coordinated state change state).

Cause
New state.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.91 E0A2

New state is invalid (for first chassis coordinated state change state).

Cause
New state.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.92 E0A3

Invalid coordinated state change state.

Cause
Coordinated state change state.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.93 E0A4

New state is invalid (for last chassis coordinated state change state).

Cause
New state.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.94 E0A5

New state is invalid (for first chassis coordinated state change state).

Cause

New state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.95 E0A6

Invalid coordinated state change state.

Cause

Coordinated state change state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.96 E0A7

Status of multicast connection makes it impossible to send state notification.

Cause

Status of multicast connection.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.97 E0A8

Unable to start watchdog timer used to time the chassis state change.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.98 E0B0

Invalid qualification trigger value.

Cause

Trigger value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.99 E0B1

Invalid new phase value.

Cause

New phase value.

Solution

None.

4.5.100 E0B2

Status of multicast connection makes it impossible to send qualification request.

Cause

Status of multicast connection.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.101 E0C0

Unable to close unconnected message manager resource (after unsuccessful send).

Cause
- Service request being made.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.102 E0C1

Unable to close unconnected message manager resource (after successful send and response).

Cause
- Service request being made.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.103 E0C2

Unable to close unconnected message manager resource (after maximum retries reached).

Cause

- Service request being made.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.104 E0C3

Unable to close unconnected message manager resource (after unsuccessful send and unsuccessful attempt to recycle the resource for a retry).

Cause

- Service request being made.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.105 E0C4

Unable to close unconnected message manager resource (after an invalid internal state has been reached).

Cause

- Service request being made.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.106 E0C5

Unable to take semaphore for sending partner service request.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.107 E0D0

Unsuccessful response status received. RM's Backup Control Object experienced a timeout of an unconnected message to its partner RM.

Cause

- Response handle.
- Response status.

- Real or apparent Redundancy Cable disconnection.

Solution

None.

4.5.108 E0D1

Invalid response data size for get single attribute request.

Cause

Data size received.

Solution

None

4.5.109 E0D2

Invalid response service for get single attribute request.

Cause

Response service code.

Solution

None

4.5.110 E0D3

Get single attribute request was unsuccessful.

Cause

Response general status code.

Solution

None

4.5.111 E0D4

Invalid partner state returned in get single attribute request.

Cause

Partner state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.112 E0D5

Invalid response data size for coordinated state change request.

Cause

Data size received.

Solution

None.

4.5.113 E0D6

Invalid response service for coordinated state change request.

Cause

Response service code.

Solution

None.

4.5.114 E0D7

Coordinated state change request was unsuccessful.

Cause

Response general status code.

Solution

None.

4.5.115 E0D8

Invalid response data size for coordinated switchover request.

Cause

Data size received.

Solution

None.

4.5.116 E0D9

Invalid response service for coordinated switchover request.

Cause

Response service code.

Solution

None.

4.5.117 E0DA

Coordinated switchover request was unsuccessful.

Cause

Response general status code.

Solution

None.

4.5.118 E0DB

An invalid coordinated switchover state has been reached.

Cause

Coordinated switchover state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.119 E0DC

Invalid service request response received.

Cause

Response handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.120 E0E0

New switchover phase is invalid.

Cause

New switchover phase.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.121 E0E1

Status of multicast connection makes it impossible to send switchover request.

Cause

Status of multicast connection.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.122 E0E2

The ICP ASIC timer interrupt is not working properly.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.123 E0F0

Invalid parameter for service request being delayed.

Cause

Service request being delayed.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.124 E0G0

Invalid new state requested.

Cause

New state value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.125 E0H0

Unable to update attributes from configuration log.

Cause

An error value returned by bcoUpdateAttributes.

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.126 E0I0

Tried to send more than one request at a time to the partner RM.

Cause

• Service request number of offending service.

- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.127 E0I1

Out of necessary resources to send partner request.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.128 E0I2

Invalid service request.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.129 E0I3

Invalid response state during request.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.130 E0I4

No client resources available to send request.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.131 E0I5

No receive descriptor available for the response.

Cause
- Service request number.
- First service parameter

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.132 E0I6

No transmit descriptor available for the request.

Cause
- Service request number.
- First service parameter

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.133 E0I7

No combuf available for the response.

Cause
- Service request number.
- First service parameter

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.134 E0I8

A bad unconnected message manager handle was used.

Cause
- Service request number.
- First service parameter

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.135 E0I9

A transmit was already in progress for the unconnected message manager..

Cause

- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.136 E0IA

An operating system error occurred.

Cause

- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.137 E0IB

No longer connected to the partner RM.

Cause

- Service request number.
- First service parameter

Solution

None.

4.5.138 E0IC

An invalid service request was made.

Cause

- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.139 E0ID

Maximum retries exceeded.

Cause

- Service request number.
- First service parameter

- Real or apparent Redundancy cable disconnection.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.140 E0IE

The private link transmit queue is full.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.141 E0IF

The unconnected message manager being used was receiving data unexpectedly.

Cause
- Service request number.
- First service parameter

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.142 E0IG

An undefined error value was encountered.

Cause
- An error value.
- Service request number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.143 E0J0

Error taking a semaphore for access to data structures for forwarding report events services to the partner RM.

Cause
- An error value.
- Service request number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.144 E101

Unable to initialize indicator device driver.

Cause

An error value returned from indDrv.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.145 E102

Unable to create '/display' device (4 character display).

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.146 E103

Unable to create '/commLed' device.

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.147 E104

Unable to create '/healthLed' device.

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.148 E105

Unable to create '/priLed' device.

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.149 E106

Unable to create '/secLed' device.

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.150 E107

Unable to create '/relay' device.

Cause

An error value returned from indDevCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.151 E108

Unable to initialize event log object.

Cause

An error value returned from eloInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.152 E109

Unable to initialize coordinated system time object.

Cause

An error value returned from cstInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.153 E10A

Unable to initialize wall clock time object.

Cause

An error value returned from wctInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.154 E10B

Unable to initialize backup control object.

Cause

An error value returned from bcoInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.155 E10C

Unable to initialize chassis profile object.

Cause

An error value returned from chpInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.156 E10D

Unable to initialize device object.

Cause

An error value returned from devInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.157 E10E

Unable to initialize extended device object.

Cause

An error value returned from edoInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.158 E10F

Unable to initialize RM State machine.

Cause

An error value returned from jbaInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.159 E10G

Unable to initialize backup communications object.

Cause

An error value returned from bcInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.160 E10H

Unable to initialize non-volatile storage object.

Cause

An error value returned from nvsInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.161 E10I

Unable to initialize DF_FAIL event handler.

Cause

An error value returned from nmiInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.162 E10J

Unable to initialize workstation display object.

Cause

An error value returned from wdoInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.163 E10K

Unable to initialize self test object.

Cause

An error value returned from stoInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.164 E10L

Unable to initialize watchdog manager.

Cause

An error value returned from dogInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.165 E10M

Unable to initialize display task.

Cause

Unable to initialize display task.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.166 E10N

Unable to initialize ICP object.

Cause

An error value returned from icpObjInit.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.167 E10P

Unable to post event to device object for displaying 'BOOT' when running in boot mode.

Cause

An error value returned from devEventPost.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.168 E201

Error collecting redundancy attribute data from all existing modules.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.169 E202

Error collected device attribute data from all existing modules.

Cause

Solution

None.

4.5.170 E203

Error collecting redundancy attribute data from all existing modules.

Cause

Solution

None.

4.5.171 E204

Error collected device attribute data from all existing modules.

Cause

Solution

None.

4.5.172 E205

Unable to start watchdog timer for collecting module data.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507

4.5.173 E206

Error collecting redundancy attribute data from all existing modules.

Cause

Solution

None.

4.5.174 E207

Error collected device attribute data from all existing modules.

Cause

Solution

None.

4.5.175 E208

Unable to start watchdog timer for collecting module data.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.176 E209

Received a startup time value from a module which is greater than 3 minutes.

Cause

• Startup time value received
• Slot number from which the value was received

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.177 E20A

Unable to update the chassis ID in all redundancy compliant modules.

Cause

Solution

None.

4.5.178 E20B

Unable to send partner present attribute to a specific module.

Cause

Slot number of module.

Solution

None.

4.5.179 E20C

Unable to get partner redundancy map when checking for a partner module.

Cause

Slot number of module for which a partner is being checked.

Solution

None.

4.5.180 E20D

Unable to send partner present service to all redundancy compliant modules that have a partner.

Cause

Solution

None.

4.5.181 E20E

Unable to collect redundancy attribute data for a newly inserted module.

Cause

Solution

None.

4.5.182 E20F

Unable to collect device object attribute data for a newly inserted module.

Cause

Solution

None.

4.5.183 E20G

Unable to read the display position from the configuration log.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.184 E20H

Unable to notify newly inserted module of current chassis ID.

Cause

Solution

None.

4.5.185 E20I

Unable to start watchdog timer to monitor for SYS_FAIL_L deassertion.

Cause

An error value returned from wdStart

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.186 E20J

Unable to update the chassis ID in all redundancy compliant modules.

Cause

Solution

None.

4.5.187 E20K

Invalid event sent to the chassis profile object.

Cause

Invalid event number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.188 E20L

Error reading message from message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.189 E20M

Error in stop service processing.

Cause

- Stop service resulting state.
- The slot number where stop service processing stopped.

Solution

Non-redundant modules at the slot number or past the slot number may have not been stopped.

4.5.190 E210

Unable to allocate a response combuf.

Cause

Solution

None.

4.5.191 E211

Response routine pointer is NULL.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.192 E230

Unable to close an unconnected message manager resource.

Cause

- Service request.

• First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.193 E235

Unable to close an unconnected message manager resource.

Cause
• Service request.
• First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.194 E236

Unable to close an unconnected message manager resource.

Cause
• Service request.
• First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.195 E237

Unable to close an unconnected message manager resource.

Cause
• Service request.
• First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.196 E239

Unable to close an unconnected message manager resource.

Cause
• Service request.
• First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.197 E23B

Unable to close an unconnected message manager resource.

Cause

- Service request.
- First service request parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.198 E250

Unable to allocate combuf

Cause

- Service request.
- First service request parameter.

Solution

None.

4.5.199 E251

Unable to allocate unconnected message manager resource.

Cause

Solution

None.

4.5.200 E252

Unable to send unconnected request.

Cause

Solution

None.

4.5.201 E253

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.202 E254

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.203 E255

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.204 E256

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.205 E257

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.206 E258

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.207 E259

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.208 E25A

Unable to allocate combuf.

Cause

Solution

None.

4.5.209 E25B

Unable to allocate unconnected message manager resource.

Cause

Solution

None.

4.5.210 E25C

Unable to send unconnected request.

Cause

Solution

None.

4.5.211 E25D

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.212 E25E

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.213 E25F

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.214 E25G

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.215 E25H

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.216 E25I

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.217 E25J

Unable to close unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.218 E260

Unable to allocate combuf.

Cause

Destination slot number.

Solution

None.

4.5.219 E261

Unable to allocate unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None.

4.5.220 E262

Unable to send unconnected request.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None.

4.5.221 E263

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.222 E264

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.223 E265

Unable to close unconnected message manager resource.

Cause
- UCMM Handle.
- Destination slot number.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.224 E266

Retries exceeded trying to do primary capability check with module.

Cause
Destination slot number.

Solution
None.

4.5.225 E267

Unable to close unconnected message manager resource.

Cause
- UCMM Handle.
- Destination slot number.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.226 E268

Unable to close unconnected message manager resource.

Cause
- UCMM Handle.
- Destination slot number.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.227 E269

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.228 E26A

Invalid internal state reached.

Cause

- Invalid state number.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.229 E26B

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.230 E270

Unable to collect redundancy attribute data.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.231 E271

Unable to collect device object attribute data.

Cause

Solution

None

4.5.232 E280

Unable to allocate combuf.

Cause

Solution

None

4.5.233 E281

Unable to allocate unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None

4.5.234 E282

Unable to send unconnected request.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None

4.5.235 E283

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.236 E284

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.237 E285

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.238 E288

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.239 E289

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.240 E28A

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.241 E28B

Retry to a module not communicating.

Cause

Destination slot number.

Solution

None.

4.5.242 E28C

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.243 E28D

Bad stop service state number.

Cause

- Stop service state number.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.244 E290

Unable to allocate combuf.

Cause

Destination slot number.

Solution

None.

4.5.245 E291

Unable to allocate unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None

4.5.246 E292

Unable to send unconnected request.

Cause

- UCMM Handle.
- Destination slot number.

Solution

None

4.5.247 E293

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.248 E294

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.249 E295

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.250 E296

Retries exceeded trying to send partner present service to module.

Cause

Destination slot number.

Solution

None.

4.5.251 E297

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.252 E298

Unable to send partner present service to module.

Cause

- Partner present state number.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.253 E299

Unable to close unconnected message manager resource.

Cause

- UCMM Handle.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.254 E2B0

Unable to allocate combuf.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.255 E2B1

Not connected to partner RM.

Cause

Solution

None.

4.5.256 E2B2

Resources not available for partner unconnected request.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.257 E2B3

Combuf not available for unconnected response.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.258 E2B4

Unknown error value returned from bcUcmmOpen.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.259 E2B5

A bad handle was used for partner unconnected request.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.260 E2B6

Not connected to partner RM.

Cause

Solution
None.

4.5.261 E2B7

An unconnected request for the unconnected resource is already in progress.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.262 E2B8

An operating resource error occurred while trying to send unconnect request.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.263 E2B9

The transmit queue is full for private link communications.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.264 E2BA

Unknown error value returned from bcUcmmOpen.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.265 E2BB

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.266 E2BC

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.267 E2BD

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.268 E2BE

Partner RM became disconnected during request.

Cause

Solution

None.

4.5.269 E2BF

Bad handle used when recycling unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.270 E2BG

Tried to recycle unconnected resource in the process of receiving a response.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.271 E2BH

Not connected to partner RM while trying to recycle unconnected resource.

Cause

Solution

None.

4.5.272 E2BI

Unknown error value returned from bcUcmmRecycle.

Cause

An error value returned from bcUcmmRecycle.

Solution

None.

4.5.273 E2BJ

Unable to close unconnected message manager resource.

Cause

Handle of unconnected message manager resource.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.274 E2BK

Invalid internal state reached.

Cause

Invalid state value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.275 E2BL

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.276 E2C0

Unable to allocate combuf.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.277 E2C1

Not connected to partner RM.

Cause

Solution

None.

4.5.278 E2C2

Resources not available for partner unconnected request.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.279 E2C3

Combuf not available for unconnected response.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.280 E2C4

Unknown error value returned from bcUcmmOpen.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.281 E2C5

A bad handle was used for partner unconnected request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.282 E2C6

Not connected to partner RM.

Cause

Solution

None.

4.5.283 E2C7

An unconnected request for the unconnected resource is already in progress.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.284 E2C8

An operating resource error occurred while trying to send unconnect request.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.285 E2C9

The transmit queue is full for private link communications.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.286 E2CA

Unknown error value returned from bcUcmmOpen.

Cause

An error value returned from bcUcmmOpen.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.287 E2CB

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.288 E2CC

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.289 E2CD

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.290 E2CE

Partner RM became disconnected during request.

Cause

Solution
None.

4.5.291 E2CF

Bad handle used when recycling unconnected message manager resource.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.292 E2CG

Tried to recycle unconnected resource in the process of receiving a response.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.293 E2CH

Not connected to partner RM while trying to recycle unconnected resource.

Cause

Solution
None.

4.5.294 E2CI

Unknown error value returned from bcUcmmRecycle.

Cause
An error value returned from bcUcmmRecycle.

Solution
None.

4.5.295 E2CJ

Unable to close unconnected message manager resource.

Cause

Handle of unconnected message manager resource.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.296 E2CK

Invalid internal state reached.

Cause

Invalid state value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.297 E2CL

Unable to close unconnected message manager resource.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.298 E2D0

Unable to start watchdog timer for monitoring.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.299 E2E0

Unable to allocate combuf.

Cause

Slot number of module to be queried.

Solution

None.

4.5.300 E2E1

Unable to allocate unconnected message manager resource.

Cause

Slot number of module to be queried.

Solution

None.

4.5.301 E2E2

Unable to take semaphore for collecting redundancy attributes.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.302 E2E3

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.303 E2E4

Unable to take semphore used to verify a switchover is not in progress.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.304 E2E5

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.305 E2E6

Unable to send unconnected request..

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.306 E2E7

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.307 E2E8

Too much data returned by module being queried.

Cause

- Slot number of module to be queried.
- Number of bytes returned.

Solution

None.

4.5.308 E2E9

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.309 E2EA

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.310 E2EB

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.311 E2EC

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.312 E2ED

Unable to collect data from module.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.313 E2EE

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.314 E2EF

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.315 E2EG

Unable to collect data from module.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
None.

4.5.316 E2EH

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.317 E2F0

Unable to allocate combuf.

Cause

Slot number of module to be queried.

Solution

None.

4.5.318 E2F1

Unable to allocate unconnected message manager resource.

Cause

Slot number of module to be queried.

Solution

None.

4.5.319 E2F2

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.320 E2F3

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.321 E2F4

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.322 E2F5

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.323 E2F6

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.324 E2F7

Unable to collect data from module, maximum retries exceeded.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
None.

4.5.325 E2F8

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.326 E2F9

Unable to collect module data.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.327 E2FA

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.328 E2FB

Unable to take semaphore for collecting device object attributes.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.329 E2FC

Unable to take semphore used to verify a switchover is not in progress.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.330 E2FD

Unable to close unconnected message manager resource.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.331 E2FE

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.332 E2FF

Unable to close unconnected message manager resource.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.333 E2G0

Unable to give semaphore to begin collection.

Cause
An error value returned from semGive.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.334 E2G1

Unable to restart watchdog timer for data collection.

Cause
An error value returned from wdStart.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.335 E2H0

Unable to take semaphore to begin collection.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.336 E2H1

Received a startup time value from a module which is greater than 3 minutes.

Cause

- Startup time value received.
- Slot number from which the value was received.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.337 E2J0

Unable to allocate combuf.

Cause

Slot number of module to be queried.

Solution

None.

4.5.338 E2J1

Unable to allocate unconnected message manager resource.

Cause

Slot number of module to be queried.

Solution

None.

4.5.339 E2J2

Unable to send unconnected request.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

None.

4.5.340 E2J3

Unable to close unconnected message manager.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.341 E2J4

Unable to close unconnected message manager.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.342 E2J5

Unable to close unconnected message manager.

Cause
- Slot number of module to be queried.
- UCMM Handle.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.343 E2J6

Unable to communicate chassis ID to module, maximum retries timed out.

Cause
Destination slot number.

Solution
None.

4.5.344 E2J7

Unable to close unconnected message manager.

Cause

- Slot number of module to be queried.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.345 E2J8

Unable to communicate chassis ID to module.

Cause

- Set chassis ID state number.
- Destination slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.346 E2J9

Unable to close unconnected message manager.

Cause

- Destination slot number.
- UCMM Handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.347 E2K0

Unable to create watchdog timer used for module pinging.

Cause

An error value returned from wdCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.348 E2L0

Unable to restart watchdog timer used for module pinging.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.349 E2L1

Unable to restart watchdog timer used for module pinging.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.350 E2M0

Unsuccesful status returned from partner request.

Cause

- Response handle.
- Status returned.
- Real or apparent Redundancy cable disconnection.

Solution

None.

4.5.351 E2M1

Unexpected response received.

Cause

Response handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.352 E2N0

Unable to take semaphore which allows module data collection.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.353 E2P0

Unable to send event to message queue.

Cause

- An error value returned from msgQSend.
- An event to be sent.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.354 E2Q0

Tried to send more than one request at a time to the partner RM.

Cause

- Service request number of offending service.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.355 E2Q1

Out of necessary resources to send partner request.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.356 E2Q2

Invalid service request.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.357 E2Q3

Invalid response state during request.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.358 E2Q4

No client resources available to send request.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.359 E2Q5

No receive descriptor available for the response.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.360 E2Q6

No transmit descriptor available for the request.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.361 E2Q7

No combuf available for the response.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.362 E2Q8

A bad unconnected message manager handle was used.

Cause
- Service request number.
- First service parameter.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.363 E2Q9

A transmit was already in progress for the unconnected message manager.

Cause
- Service request number.
- First service parameter.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.364 E2QA

An operating system error occurred.

Cause
- Service request number.
- First service parameter.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.365 E2QB

No longer connected to the partner RM.

Cause
- Service request number.
- First service parameter.

Solution
None.

4.5.366 E2QC

Maximum retries exceeded.

Cause

- Service request number.
- First service parameter.
- Real or apparent Redundancy cable disconnection.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.367 E2QD

The private link transmit queue is full.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.368 E2QE

The unconnected message manager being used was receiving data unexpectedly.

Cause

- Service request number.
- First service parameter.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.369 E2QF

An undefined error value was encountered.

Cause

- Service request number.
- An error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.370 E300

Unable to prepare a buffer for response to a CST time maintenance update request.

Cause

Solution

None.

4.5.371 E301

Response routine to a request is NULL.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.372 E400

Error reading configuration log for vendor id.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.373 E401

Error reading configuration log for product type.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.374 E402

Error reading configuration log for product code.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.375 E404

Error reading configuration log for configured bit.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.376 E405

Error reading configuration log for serial number.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.377 E406

Error reading configuration log for product name.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.378 E407

Error creating semaphore for reset service.

Cause
An error value returned from semBCreate.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.379 E408

Error creating watchdog for delay before servicing reset.

Cause
An error value returned from wdCreate.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.380 E409

Error registering the device object class with the toolkit.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.381 E40A

Error setting the initial device object general status to unkeyed, awaiting connection.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.382 E410

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.383 E420

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.384 E430

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.385 E440

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.386 E450

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.387 E451

Error updating attributes.

Cause

An error value returned from devUpdateAttributes.

Solution

None. Defaults to instance one.

4.5.388 E460

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.389 E470

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.390 E480

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.391 E481

Error updating attributes.

Cause

An error value returned from devUpdateAttributes.

Solution

None. Defaults to instance one.

4.5.392 E490

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.393 E4A0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.394 E4B0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.395 E4C0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.396 E4D0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.397 E4E0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.398 E4F0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.399 E4G0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.400 E4H0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.401 E4I0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.402 E4J0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.403 E4K0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.404 E4L0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.405 E4L1

In major fault state, but no fault bits are set.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.406 E4L2

Unknown general state.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.407 E4M0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.408 E4N0

Unknown instance number.

Cause

Solution
None. Defaults to instance one.

4.5.409 E4N1

Error updating attributes.

Cause

Solution
None. Defaults to instance one.

4.5.410 E4P0

Error updating attributes

Cause
An error value returned from devUpdateAttributes

Solution
None. Defaults to instance one.

4.5.411 E4P1

Error preparing success status response buffer for reset service request.

Cause

Solution
None. Defaults to instance one.

4.5.412 E4P2

Response routine pointer used to send reply to reset request is corrupted (had value of NULL).

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.413 E4P3

Error taking semaphore to wait for event log to finish before resetting RM.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.414 E4P4

Error starting watchdog to perform reset.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.415 E4Q0

Error sending event to fault information queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.416 E4R0

Error sending event to display control queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.417 E4T0

Unknown control display event.

Cause

Control display event.

Solution

None.

4.5.418 E4U0

Error opening display.

Cause

An error value returned from open.

Solution

None.

4.5.419 E4U1

Error commanding display to turn shifting off.

Cause

An error value returned from ioctl.

Solution

None.

4.5.420 E4U2

Error writing to display.

Cause

An error value returned from write.

Solution

None.

4.5.421 E4U3

Error closing display.

Cause

An error value returned from close.

Solution

None.

4.5.422 E4V0

Error reading event from display control queue.

Cause

An error value returned from msgQReceive.

Solution

None.

4.5.423 E4V3

Unknown redundancy state for display.

Cause

Redundancy state.

Solution

None.

4.5.424 E4V4

Unknown non-redundancy state for display.

Cause

Non-Redundancy state.

Solution

None.

4.5.425 E4V5

Error starting watchdog to display fault message next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.426 E4V6

Error starting watchdog to display recovery message next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.427 E4V7

Error starting watchdog to display blank next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.428 E4V8

Error starting watchdog to display the next field in the fault message next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.429 E4V9

Error starting watchdog to display recovery message next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.430 E4VA

Error starting watchdog to display blank next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.431 E4VB

Error starting watchdog to display the next field in the recovery message next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.432 E4VC

Error starting watchdog to display blank next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.433 E4VD

Error starting watchdog to display fault code next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.434 E4VE

Error starting watchdog to display new fault code next.

Cause

An error value returned from wdStart.

Solution

None.

4.5.435 E4VF

Unknown event for display control.

Cause

Event.

Solution

None.

4.5.436 E4VG

Error reading event from fault information queue.

Cause

An error value returned from msgReceive.

Solution

None.

4.5.437 E4VH

Error starting watchdog to clear minor recoverable fault in one minute.

Cause

An error value returned from wdStart.

Solution

None.

4.5.438 E4VI

Error starting watchdog to change display intensity (heartbeat).

Cause

An error value returned from wdStart.

Solution

None.

4.5.439 E4W0

Unknown instance number.

Cause

Solution

None. Defaults to instance one.

4.5.440 E4X0

Error starting watchdog to change display intensity (heartbeat).

Cause

An error value returned from wdStart.

Solution

None.

4.5.441 E4X1

Error starting watchdog to change display intensity (heartbeat).

Cause

An error value returned from wdStart.

Solution

None.

4.5.442 E4X2

Error starting watchdog to change display intensity (heartbeat).

Cause

An error value returned from wdStart.

Solution

None.

4.5.443 E500

Error registering the device object class with the toolkit.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.444 E600

Message queue send from service routine to event log task failed when handling absolute or relative event log read.

Cause

Solution

None.

4.5.445 E601

Failed to properly prepare buffer to send reply to get powerdown state service request.

Cause

Solution

None.

4.5.446 E602

Response routine pointer used to send reply to get powerdown state service request is corrupted (had value of NULL).

Cause

Solution

None.

4.5.447 E603

Failed to properly prepare buffer to send reply to get powerdown time service request.

Cause

Solution

None.

4.5.448 E604

Response routine pointer used to send reply to get powerdown time service request is corrupted (had value of NULL).

Cause

Solution

None.

4.5.449 E605

Message queue send from service routine to event log task failed when handling absolute or relative event log read.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.450 E606

Unable to get semaphore for configuration log shadow resource when handling configuration log update service.

Cause

An error value returned from semTake.

Solution

None.

4.5.451 E607

The function cfgReadAllData failed when handling configuration log update service.

Cause

Solution

None.

4.5.452 E608

The function cfgNcWriteNewData failed when handling configuration log update service.

Cause

Solution

None.

4.5.453 E609

Preparing response buffer failed when handling configuration log update service.

Cause

Solution

None.

4.5.454 E610

Unable to wdStart failed to start timer at beginning of task.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.455 E611

Unable to wdStart failed to start timer in task loop.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.456 E612

The function cfgReadAllData failed when handling event from Jabba to indicating RM state is now primary with secondary.

Cause

Solution

None.

4.5.457 E614

Received a bad event in the tasks event queue (the event's type wasn't expected).

Cause

The event type that was sent to the eventlog.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.458 E615

The function msgQReceive failed when trying to receive on the event log objects event queue.

Cause

An error from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.459 E631

Powerup rule received an unrecognized response handle.

Cause

Response handle that wasn't recognized.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.460 E640

Open function call for either partner or local event log failed.

Cause

An error from open.

Solution

None.

4.5.461 E641

Could not prepare buffer for response to event log read service request.

Cause

Solution

None.

4.5.462 E642

Ioctl function call for either partner or local event log failed read relative service.

Cause

An error from ioctl.

Solution

None.

4.5.463 E643

Ioctl function call for either partner or local event log failed for read absolute service.

Cause

An error from ioctl.

Solution

None.

4.5.464 E644

Ioctl function call for either partner or local event log failed for read absolute service.

Cause

An error from ioctl.

Solution

None.

4.5.465 E645

Read function call for read of event log failed with error S_logDrv_BAD_DEVICE_TYPE or S_logDrv_SEM_UNAVAILABLE.

Cause

An error from read.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.466 E646

In read absolute or read relative service request, read system call failed with error S_logDrv_BAD_DEVICE_TYPE or S_logDrv_SEM_UNAVAILABLE.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.467 E647

Open function call for local event log failed in update partner service request.

Cause

An error from read.

Solution

None.

4.5.468 E648

Could not prepare buffer for response to event log update partner service request.

Cause

Solution

None.

4.5.469 E649

Response routine pointer corrupted (NULL) in update partner service.

Cause

Solution

None.

4.5.470 E650

Could not allocate application connection resource for event log connection to partner.

Cause

Solution

None.

4.5.471 E651

Failure to initiate connection opening to partner's event log object.

Cause

Solution
None.

4.5.472 E652

Time required to open connection to partner's event log object is too long.

Cause

Solution
None.

4.5.473 E653

Failed to get pointer to buffer when attempting communications to partner's event log.

Cause

Solution
None.

4.5.474 E654

Failed attempting to send message to partner's event log.

Cause

Solution
None.

4.5.475 E655

Time required to receive response from partner when querying its event log is too long.

Cause

Solution
None.

4.5.476 E656

Time required to receive response from partner when querying its event log is too long.

Cause

Solution

None.

4.5.477 E660

Reply to open failed.

Cause

Solution

None.

4.5.478 E670

Response from partner to request timed-out.

Cause

Real or apparent Redundancy cable disconnection.

Solution

None.

4.5.479 E671

Write failed when attempting to write to local (shadow) copy of partner's event log.

Cause

An error value returned from write.

Solution

None.

4.5.480 E672

Ioctl failed when attempting to configure local (shadow) copy of partner's event log.

Cause

An error value returned from ioctl.

Solution

None.

4.5.481 E673

Open failed when attempting for local (shadow) copy of partner's event log.

Cause

An error value returned from open.

Solution

None.

4.5.482 E680

Data indication function received unrecognized event.

Cause

Unrecognized event.

Solution

None.

4.5.483 E690

Unable to get semaphore for configuration log shadow resource.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.484 E6A0

Unable to get semaphore for configuration log shadow resource.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.485 E6B0

Unable to get semaphore for configuration log shadow resource.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.486 E6C0

Unable to get semaphore for configuration log shadow resource while writing vendor ID.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.487 E6C1

Unable to get semaphore for configuration log shadow resource while writing product type.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.488 E6C2

Unable to get semaphore for configuration log shadow resource while writing product code.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.489 E6C3

Unable to get semaphore for configuration log shadow resource while writing revision number.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.490 E6C4

Unable to get semaphore for configuration log shadow resource while writing serial number.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.491 E6C5

Unable to get semaphore for configuration log shadow resource while writing product name.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.492 E6C6

Unable to get semaphore for configuration log shadow resource while writing autoqualification option.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.493 E6C7

Unable to get semaphore for configuration log shadow resource while writing program command recognition option.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.494 E6C8

Unable to get semaphore for configuration log shadow resource while writing maximum power-up time.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.495 E6C9

Unable to get semaphore for configuration log shadow resource while writing configured bit.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.496 E6CA

Unable to get semaphore for configuration log shadow resource while writing workstation display position value.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.497 E6CB

Unable to get semaphore for configuration log shadow resource while writing autoqualification state.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.498 E6CC

Unable to get semaphore for configuration log shadow resource while writing autoqualification option and autoqualification state.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.499 E6CD

Unable to get semaphore for configuration log shadow resource while writing application revision.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.500 E6D0

Unable to allocate combuf when copying event log to partner.

Cause

Solution

None.

4.5.501 E6D1

Opening unconnected resource to partner to copy event log failed.

Cause

Solution

None.

4.5.502 E6D2

Unable to send UCMM request to partner.

Cause

Solution

None.

4.5.503 E6D3

Getting semaphore that waits for partner send response failed (but this was not due to a message timeout).

Cause

Solution

None.

4.5.504 E6D4

Copy of event log to partner failed.

Cause

Value of cfgCopyStatus.

Solution

None.

4.5.505 E6E0

Unable to get semaphore for configuration log shadow resource while resetting RM configuration log to factory defaults.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.506 E6F0

Message Queue Send function failed when another subsystem tried to post an event to the event log object.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.507 E700

Unable to post to message queue for the backup communications object.

Cause

- An error value returned from msgQSend.
- Event number

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.508 E701

Unable to start watchdog used to keep the partner communication LED red for greater than 1 second at powerup.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.509 E702

Unable to open the /commLed device used for controlling the partner communication LED.

Cause

An error value returned from open.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.510 E703

Unable to perform ioctl command to /commLed device used for controlling the partner communication LED.

Cause

An error value returned from ioctl.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.511 E704

Unable to perform write to /commLed device used for controlling the partner communication LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.512 E70E

Unexpected event while in the INIT state.

Cause

- Current Backup Communications object state.
- Event type received.

Solution

None.

4.5.513 E70G

Unexpected event while in the DISCONNECTED state.

Cause

- Current Backup Communications object state.
- Event type received.

Solution

None.

4.5.514 E70H

Unexpected event while in the DISCONNECTED_S state.

Cause
- Current Backup Communications object state.
- Event type received.

Solution
None.

4.5.515 E70L

Unable to allocate memory for table of available UCMM targets on the partner RM.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.516 E70N

Unable to start watchdog used for collecting private link statistics.

Cause
An error value returned from wdStart.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.517 E70Q

Received an ACK to an unexpected command transmission while in the CONNECTING state.

Cause
- Current Backup Communications object state.
- Command code transmitted.

Solution
None.

4.5.518 E70T

Unable to start watchdog used for RM to RM pinging.

Cause
An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.519 E70U

Unable to start watchdog used to control partner to partner pinging.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.520 E70V

Received an unexpected command from partner RM while in the CONNECTING state.

Cause

- Current Backup Communications object state.
- Command code received from partner RM.

Solution

None.

4.5.521 E70W

Unexpected event while in the CONNECTING state.

Cause

- Current Backup Communications object state.
- Event type received.

Solution

None.

4.5.522 E710

The transmit packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.523 E711

The transmit retry count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.524 E712

The transmit word count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.525 E713

The receive packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.526 E714

The receive valid packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.527 E715

The receive CRC error count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.528 E716

The receive framing error count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.529 E717

The receive word count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.530 E718

Unable to start watchdog used for collecting private link statistics.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.531 E719

Received BC_CMD_START from partner RM while in the CONNECTED state.

Cause

Solution

None.

4.5.532 E71A

Received unexpected command from partner RM while in the CONNECTED state.

Cause

Command code received from partner RM.

Solution

None.

4.5.533 E71B

Unexpected event while in the CONNECTED state.

Cause

• Current Backup Communications object state.
• Command code received from partner RM.

Solution

None.

4.5.534 E71C

Unexpected event while in the DISABLED_S state.

Cause

- Current Backup Communications object state.
- Command code received from partner RM.

Solution

None.

4.5.535 E71D

Unexpected event while in the DISABLED_E state.

Cause

- Current Backup Communications object state.
- Command code received from partner RM.

Solution

None.

4.5.536 E71E

Backup communications object is in an invalid state.

Cause

Current state value of backup communications object.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.537 E71F

Error reading message from message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.538 E71G

Unable to cancel watchdog used for collecting private link statistics.

Cause

An error value returned from wdCancel.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.539 E71H

Unable to cancel watchdog used for collecting private link statistics.

Cause

An error value returned from wdCancel.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.540 E71I

Unable to cancel watchdog used for collecting private link statistics.

Cause

An error value returned from wdCancel.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.541 E71J

Unable to cancel watchdog used for collecting private link statistics.

Cause

An error value returned from wdCancel.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.542 E720

Unable to post message to link producer task.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.543 E721

Unable to post message to unconnected message manager task.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.544 E722

Unknown command in transmit descriptor being recovered.

Cause

- Descriptor id.
- Command character.

Solution

None.

4.5.545 E723

Unable to post message to link producer task.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.546 E724

Unable to post message to unconnected message manager task.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.547 E725

Unknown command in transmit descriptor being recovered.

Cause

• Descriptor id.

• Command character.

Solution

None.

4.5.548 E726

The transmit packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.549 E727

The transmit retry count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.550 E728

The transmit word count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.551 E729

The receive packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.552 E72A

The receive valid packet count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.553 E72B

The receive CRC error count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.554 E72C

The receive framing error count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.555 E72D

The receive word count register rolled over before it could be read by firmware.

Cause

Solution

None.

4.5.556 E730

Unable to get semaphore for allocating a new bridging transport.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.557 E731

State conflict occurred when deleting a link consumer.

Cause

Link consumer handle.

Solution

None.

4.5.558 E732

State conflict occurred when deleting a link producer.

Cause

Link producer handle.

Solution

None.

4.5.559 E733

State conflict occurred when deleting a link consumer.

Cause

Link consumer handle.

Solution

None.

4.5.560 E734

State conflict occurred when deleting a link producer.

Cause

Link producer handle.

Solution

None.

4.5.561 E735

Time-out on bridged connection, originator to target direction.

Cause

Bridge record handle.

Solution

None.

4.5.562 E736

Error occurred while swapping in-port and out-port buffers, originator to target direction.

Cause

- Bridge record handle.
- Status returned from bcBridgeSwap.

Solution

None.

4.5.563 E737

Error occurred while forwarding a message to the target.

Cause

- Bridge record handle.
- Status returned from Link Producer send routine.

Solution

None.

4.5.564 E738

Time-out on bridged connection, target to originator direction.

Cause

Bridge record handle.

Solution

None.

4.5.565 E739

Error occurred while swapping in-port and out-port buffers, target to originator direction.

Cause

- Bridge record handle.
- Status returned from bcBridgeSwap.

Solution

None.

4.5.566 E73A

Error occurred while forwarding a message to the originator.

Cause

- Bridge record handle.
- Status returned from Link Producer send routine.

Solution

None.

4.5.567 E73C

Error occurred while swapping in-port and out-port buffers, originator to target direction.

Cause

*   Bridge record handle.
*   Status returned from bcBridgeSwap.

Solution

None.

4.5.568 E73D

Error occurred while forwarding a message to the target.

Cause

*   Bridge record handle.
*   Status returned from Link Producer send routine.

Solution

None.

4.5.569 E73F

Error occurred while swapping in-port and out-port buffers, target to originator direction.

Cause

*   Bridge record handle.
*   Status returned from bcBridgeSwap.

Solution

None.

4.5.570 E73G

Error occurred while forwarding a message to the originator.

Cause

*   Bridge record handle.
*   Status returned from Link Producer send routine.

Solution

None.

4.5.571 E73H

Unexpected event received from link producer in transmit done routine.

Cause
- Bridge record handle.
- Event received from link producer.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.572 E73I

Unexpected event received from link producer in transmit done routine.

Cause
- Bridge record handle.
- Event received from link producer.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.573 E740

Unable to get semaphore for allocating a receive descriptor.

Cause
An error value returned from semTake.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.574 E741

Unable to get semaphore for allocating a transmit descriptor.

Cause
An error value returned from semTake.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.575 E742

Unable to get semaphore for allocating a descriptor ID.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.576 E752

Descriptor ID read from transmit channel is 0.

Cause

Solution

None.

4.5.577 E753

The transmit channel returned a transmit error.

Cause

Transmit descriptor ID causing the error.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.578 E754

Unknown transmit status returned by the transmit channel.

Cause

- Transmit descriptor ID containing invalid status.
- Invalid status value

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.579 E755

Unable to send message to the link producer task.

Cause

An error value returned by msgQSend.

Solution

None.

4.5.580 E756

Unable to send message to the unconnected message manager task.

Cause

An error value returned by msgQSend.

Solution

None.

4.5.581 E757

Unknown command code in transmit descriptor.

Cause

- Transmit descriptor ID.
- Invalid command code

Solution

None.

4.5.582 E75A

Descriptor ID read from receive channel is 0.

Cause

Solution

None.

4.5.583 E75B

The receive channel returned a memory access error.

Cause

Receive descriptor ID.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.584 E75C

The receive channel returned an invalid destination error.

Cause

Receive descriptor ID.

Solution

None.

4.5.585 E75D

Unknown received status returned by the receive channel.

Cause

- Receive descriptor ID containing the invalid status.
- Invalid status value

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.586 E75E

Unable to send to the link consumer task.

Cause

An error value returned by msgQSend.

Solution

None.

4.5.587 E75F

Unable to send to the unconnected message manager task.

Cause

An error value returned by msgQSend.

Solution

None.

4.5.588 E75G

Unknown command code in receive descriptor.

Cause

- Receive descriptor ID.
- Invalid command code.

Solution

None.

4.5.589 E75I

A double bit memory error has occurred in local RAM.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.590 E75J

A shared RAM parity error occurred.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.591 E75K

Error occurred while invalidating the data cache for a transmit descriptor.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.592 E75L

Error occurred while invalidating the data cache for a receive descriptor.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.593 E75M

An error occurred while trying to start a watchdog timer to unmask the signal detect interrupt.

Cause
An error value returned by wdStart.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.594 E760

The bcLcFreeReceiveBuffer was called with a NULL buffer pointer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.595 E762

Receive descriptor in use by hardware layer. Not expected unless buffer overwriting is enabled.

Cause

Receive descriptor number.

Solution

None.

4.5.596 E763

Receive descriptor in use by hardware layer. Not expected unless buffer overwriting is enabled.

Cause

Receive descriptor number.

Solution

None.

4.5.597 E764

Unable to get semaphore for allocating a link consumer.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.598 E766

Unexpected message received by the link consumer task.

Cause

Message type received.

Solution

None.

4.5.599 E767

Error reading message from link consumer message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.600 E768

An invalid descriptor ID was received.

Cause

Receive descriptor ID.

Solution

None.

4.5.601 E769

Status of received descriptor is not OK.

Cause

- Receive descriptor ID.
- Status of receive descriptor.

Solution

None.

4.5.602 E76A

Link consumer received a message but is no longer running.

Cause

- Link consumer handle.
- Link consumer state.

Solution

None.

4.5.603 E76C

Receive descriptor in use by hardware layer. Not expected unless buffer overwriting is enabled.

Cause

Receive descriptor ID.

Solution

None.

4.5.604 E76D

Double buffering is enabled but the second buffer is not available.

Cause

Receive descriptor ID.

Solution

None.

4.5.605 E76E

Receive descriptor in use by hardware layer. Not expected unless buffer overwriting is enabled.

Cause

Receive descriptor ID.

Solution

None.

4.5.606 E76F

Double buffering is enabled but the second buffer is not available.

Cause

Receive descriptor ID.

Solution

None.

4.5.607 E770

The selected buffer was not available for the transport layer, the second buffer is being used.

Cause

Transmit descriptor number.

Solution

None.

4.5.608 E771

The selected buffer was not available for the transport layer, the second buffer is being used.

Cause

Transmit descriptor number.

Solution

None.

4.5.609 E772

Unable to get semaphore for allocating a link producer.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.610 E774

A message existed on the pending queue. This means that the hardware is not transmitting messages as fast as they are being submitted by firmware.

Cause

Solution

None.

4.5.611 E777

Error reading message from link producer message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.612 E778

The bcLpSend was called with a NULL buffer pointer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.613 E779

Descriptor being written to the transmit queue has nothing to be transmitted.

Cause

Transmit descriptor number.

Solution

None.

4.5.614 E77A

Descriptor being written to the transmit queue has nothing to be transmitted.

Cause

Transmit descriptor number.

Solution

None.

4.5.615 E77C

The hardware transmit queue is full. Message to be sent will be queued by firmware.

Cause

Transmit descriptor number.

Solution

None.

4.5.616 E77E

A message existed on the pending queue. This means that the hardware is not transmitting messages as fast as they are being submitted by firmware.

Cause

Solution

None.

4.5.617 E77H

Unable to post message to link producer message queue.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.618 E77I

An invalid transmit descriptor was given back by the hardware transmit channel.

Cause

Transmit descriptor ID

Solution

None.

4.5.619 E77J

A transmission has finished for a link producer which is no longer running.

Cause

- Link producer handle.
- Link producer state.

Solution

None.

4.5.620 E77K

Unable to write transmit descriptor to hardware transmit queue or internal firmware transmission queue.

Cause

Solution

None.

4.5.621 E790

Unable to start watchdog used for communication timers.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.622 E791

Unable to send time-out message to link consumer task.

Cause

An error value returned from msgQSend.

Solution

None.

4.5.623 E792

Unable to send time-out message to link consumer task.

Cause

An error value returned from msgQSend.

Solution

None

4.5.624 E7B1

Unable to get semaphore for allocating a client UCMM resource.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.625 E7B2

Unable to get semaphore for allocating a server UCMM resource.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.626 E7B3

Unable to get semaphore when selecting a target resource for sending an unconnected command.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.627 E7B4

Unable to get semaphore when selecting a target resource for sending an unconnected request.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.628 E7B6

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.629 E7B7

An invalid descriptor ID was received.

Cause

Received descriptor ID.

Solution

None.

4.5.630 E7B8

Status of received descriptor is not OK.

Cause

- Received descriptor ID.
- Status of receive descriptor.

Solution

None.

4.5.631 E7B9

Unable to allocate an UCMM server resource when receiving a request.

Cause

Solution

None.

4.5.632 E7BA

Unable to allocate a transmit descriptor when receiving a request.

Cause

Solution

None.

4.5.633 E7BB

Status of received descriptor is not OK.

Cause

- Received descriptor ID.
- Status of receive descriptor.

Solution

None.

4.5.634 E7BC

The message router request to process a received command failed.

Cause

Solution

None.

4.5.635 E7BD

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.636 E7BE

Received a response for an UCMM that is not running.

Cause

UCMM handle.

Solution

None.

4.5.637 E7BF

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.638 E7BG

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.639 E7BH

Unexpected command character in receive descriptor.

Cause

- Receive descriptor ID.
- Command character.

Solution

None.

4.5.640 E7BI

An invalid descriptor ID was received.

Cause

Receive descriptor ID.

Solution

None.

4.5.641 E7BJ

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.642 E7BL

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.643 E7BM

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.644 E7BN

Unable to get semaphore when marking a target resource available.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.645 E7BQ

A message existed on the pending queue. This means that the hardware is not transmitting messages as fast as they are being submitted by firmware.

Cause

Solution

None.

4.5.646 E7BT

Error reading message from unconnected message manager queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.647 E7BU

Unexpected command character in transmit descriptor.

Cause

- Transmit descriptor ID.
- Command character.

Solution

None.

4.5.648 E800

Attempted to free a combuf which was already free.

Cause

Combuf pointer.

Solution

None.

4.5.649 E801

Tries to free a NULL combuf pointer.

Cause

Solution

None.

4.5.650 E810

The ICP ASIC fault line did not go inactive within expected time limit.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.651 E811

The ICP ASIC loop back test failed and a supervisor control could not be submitted to the ASIC to turn off the receiver circuitry.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.652 E812

The ICP ASIC loop back test failed.

Cause

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.653 E813

An invalid control block pointer is trying to be passed to the ICP ASIC.

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.654 E814

An invalid control block pointer came from the control block host free list.

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.655 E815

An invalid control block pointer is trying to be put onto the control block host free list.

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.656 E816

An invalid control block pointer is trying to be passed to the ICP ASIC (for a flow controlled connection).

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.657 E817

An invalid control block pointer is trying to be passed to the ICP ASIC (for a supervisory request).

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.658 E818

A control block pointer is trying to be passed to the ICP ASIC, but the ICP ASIC queuing link is already non-zero.

Cause

Invalid control block pointer.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.659 E819

An invalid control block pointer is trying to be passed to the ICP ASIC (for a notify CB).

Cause

Control block pointer.

Solution

None.

4.5.660 E81A

A control block is going onto the host free list with a non-zero value in the ICP ASIC queuing link.

Cause

Control block pointer.

Solution

None.

4.5.661 E81B

A control block came from the host free list with a non-zero value in the ICP ASIC queuing link.

Cause

Control block pointer.

Solution

None.

4.5.662 E81C

A control block is trying to be passed to the ICP ASIC, but the ICP ASIC queuing link is already non-zero (for a flow controlled connection).

Cause

Control block pointer.

Solution

None.

4.5.663 E81D

A control block is trying to be passed to the ICP ASIC, but the ICP ASIC queuing link is already non-zero (for a supervisory request).

Cause

Control block pointer.

Solution

None.

4.5.664 E81E

A control block is trying to be passed to the ICP ASIC, but the ICP ASIC queuing link is already non-zero (for a notify CB).

Secondary RM encounters a minor recoverable fault during powerup. The **E81E** fault code indicates that the RM encountered a communication failure. Note that as a consequence of this defect, modules within the secondary chassis may not have transitioned to the secondary redundancy role (for example,. CNIs in DUPL node, CPM not in BKUP state). However, this does not affect primary controller chassis operation.

Cause

Control block pointer.

Solution

Cycle power to the secondary chassis.

4.5.665 E820

The dynamic class registration table could not be initialized.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.666 E821

Part of the general initialization failed.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.667 E830

Unable to create semaphore for the UCMM Resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.668 E831

Unable to take semaphore for the UCMM Resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.669 E832

Unable to take semaphore for the UCMM Resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.670 E833

Unable to take semaphore for the UCMM Resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.671 E834

Unable to take semaphore for the UCMM Resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.672 E835

Unable to take semaphore for the UCMM Resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.673 E836

Unable to take semaphore for the UCMM Resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.674 E840

Unable to initialize semaphore for the server transport resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.675 E841

Unable to initialize semaphore for the client transport resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.676 E850

Unable to take semaphore for the server transport resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.677 E851

Unable to give semaphore for the server transport resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.678 E852

Unable to give semaphore for the server transport resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.679 E860

Unable to take semaphore for the client transport resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.680 E861

Unable to give semaphore for the client transport resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.681 E862

Unable to give semaphore for the client transport resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.682 E870

Unable to initialize semaphore for the link consumer resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.683 E871

Unable to take semaphore for the link consumer resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.684 E872

Unable to give semaphore for the link consumer resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.685 E873

Unable to give semaphore for the link consumer resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.686 E876

Tried to free a NULL link consumer receive buffer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.687 E880

Unable to initialize semaphore for the link producer resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.688 E881

Unable to take semaphore for the link producer resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.689 E882

Unable to give semaphore for the link producer resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.690 E883

Unable to give semaphore for the link producer resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.691 E884

Unable to create buffer used for queuing link producers which need to be resent.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.692 E885

Unable to create watchdog timer for monitoring queue of link producers which need to be resent.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.693 E886

Unable to start the watchdog timer used for monitoring queue of link producers which need to be resent.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.694 E887

Unable to restart the watchdog timer used for monitoring queue of link producers which need to be resent

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.695 E888

Tried to do a link producer send with a NULL transmit buffer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.696 E889

Unable to create buffer used for queuing link producers which need to be resent.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.697 E88A

A link producer CB is being processed on return from the ICP ASIC and a new send is already pending. This is unexpected.

Cause
• Pointer to control block allocated by link producer.

- State of control block.

Solution

None.

4.5.698 E88B

Double buffering code is running unexpectedly on a link producer send.

Cause
- Link producer handle.
- Pointer to control block allocated by link producer.

Solution

None.

4.5.699 E88C

Trying a new send when the previous send is still pending in the ICP ASIC.

Cause
- Link producer handle.
- Pointer to control block allocated by link producer.

Solution

None.

4.5.700 E88D

A control block was returned by the ICP ASIC in the CB_STS_INIT state.

Cause
- State of control block.
- Pointer to control block allocated by link producer.

Solution

None.

4.5.701 E88E

A control block was returned by the ICP ASIC in an error state.

Cause
- State of control block.
- Pointer to control block allocated by link producer.

Solution

None.

4.5.702 E891

Unable to take semaphore for the connection manager resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.703 E892

Unable to give semaphore for the connection manager resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.704 E893

Unable to give semaphore for the connection manager resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.705 E894

Unable to create semaphore for the connection manager resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.706 E895

Unable to set device state to CONNECTED_ACTIVE when the first connection is created.

Cause
An error value returned from devSetState().

Solution
None.

4.5.707 E896

Unable to set device state to UNKEYED_AWAITING_CONNECTION when last connection is closed.

Cause

An error value returned from devSetState().

Solution

None.

4.5.708 E8A0

Received Fault interrupt from ICP ASIC.

Cause

Solution

None.

4.5.709 E8A1

Received bad data on loop back test.

Cause

• Data received.
• Data expected.

Solution

Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.710 E8A2

Received a control block from the ICP ASIC with the queuing value still non-zero.

Cause

Control block pointer.

Solution

None.

4.5.711 E8A3

ICP ASIC reported a watchdog error.

Cause

Error register value read from ICP ASIC.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.712 E8A4

ICP ASIC reported a shared RAM parity error.

Cause

Error register value read from ICP ASIC.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.713 E8A5

ICP ASIC reported a host parity error.

Cause

Error register value read from ICP ASIC.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.714 E8B0

Unable to allocate combuf for error response.

Cause

Error register value read from ICP ASIC.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.715 EA00

Error opening LED.

Cause

An error value returned from open.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.716 EA01

Error opening relay.

Cause

An error value returned from open.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.717 EA02

Duplicate RM.

Cause

Solution

Remove the RM.

4.5.718 EA03

Error starting timer for starting state determination.

Cause

An error value returned from wdStart.

Solution

None.

4.5.719 EA04

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.720 EA05

Error reading message from main queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.721 EA10

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.722 EA11

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.723 EA12

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.724 EA13

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.725 EA14

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.726 EA15

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.727 EA16

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.728 EA17

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.729 EA18

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.730 EA19

Unexpected redundancy state from partner.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.731 EA1B

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.732 EA1C

Error completing the state change.

Cause

An error returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.733 EA1D

Event received in wrong state.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.734 EA1E

Unexpected event for powerup.

Cause

Event.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.735 EA1F

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.736 EA1G

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.737 EA1H

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.738 EA1I

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.739 EA1J

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.740 EA1K

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.741 EA1L

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.742 EA1M

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.743 EA1N

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.744 EA1P

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.745 EA1Q

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.746 EA1R

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.747 EA1T

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.748 EA1U

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.749 EA1V

Primary capability checks with a module that is not communicating has maxed out the number of retries. The state cannot be determined without primary capability results.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.750 EA1W

Primary capability checks with a module is not working. The state cannot be determined without primary capability results.

Cause

- State.
- Error or undefined status from primary capability checks.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.751 EA20

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.752 EA21

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.753 EA22

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.754 EA23

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.755 EA24

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.756 EA25

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.757 EA26

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.758 EA27

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.759 EA28

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.760 EA29

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.761 EA2A

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.762 EA2B

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.763 EA2C

Switchover complete event with wrong switchover phase.

Cause

• Switchover phase.

• State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.764 EA2E

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.765 EA2F

Error completing the state change.

Cause

An error returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.766 EA2G

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.767 EA2H

Event received in wrong state.

Cause

• State.

• Redundancy state stored.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.768 EA2I

Unexpected event for primary with qualified secondary.

Cause

Event.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.769 EA2J

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.770 EA2K

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.771 EA2L

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.772 EA2M

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.773 EA30

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.774 EA31

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.775 EA32

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.776 EA33

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.777 EA34

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.778 EA35

Qualification complete event with wrong qualification phase.

Cause

- Qualification phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.779 EA36

Unknown extended error for module requested qualification abort.

Cause

- Extended error.
- Module slot number.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.780 EA37

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.781 EA38

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.782 EA39

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.783 EA3A

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.784 EA3B

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.785 EA3C

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.786 EA3D

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.787 EA3E

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.788 EA3F

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.789 EA3G

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.790 EA3H

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.791 EA3I

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.792 EA3J

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.793 EA3K

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.794 EA3L

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.795 EA3N

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.796 EA3P

Event received in wrong state. Primary RM encounters a major unrecoverable fault during (power-cycle) switchover.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.797 EA3Q

Event received in wrong state.

Cause

- State.
- Redundancy state stored.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.798 EA3R

Unexpected event for primary with disqualified secondary..

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.799 EA3T

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.800 EA3U

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.801 EA3V

Error completing the state change.

Cause

An error returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.802 EA40

Event received in wrong state.

Cause

State

Solution

None. Disconnect and connect the redundancy cable.

4.5.803 EA41

Event received in wrong state.

Cause

State

Solution

None. Disconnect and connect the redundancy cable.

4.5.804 EA42

Event received in wrong state.

Cause

State

Solution

None. Disconnect and connect the redundancy cable.

4.5.805 EA43

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.806 EA44

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.807 EA45

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.808 EA46

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.809 EA47

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.810 EA48

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.811 EA49

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.812 EA4A

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.813 EA4B

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.814 EA4C

Unexpected redundancy state from partner.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.815 EA4E

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.816 EA4F

Error completing the state change.

Cause

An error value returned jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.817 EA4G

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.818 EA4H

Unexpected event for primary with no secondary.

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.819 EA4I

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.820 EA4J

Error completing the state change.

Cause

An error value returned jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.821 EA4K

Error completing the state change.

Cause

An error value returned jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.822 EA4L

Error completing the state change.

Cause

An error value returned jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.823 EA4M

Error completing the state change.

Cause

An error value returned jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.824 EA50

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.825 EA51

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.826 EA52

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.827 EA53

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.828 EA54

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.829 EA55

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.830 EA56

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.831 EA57

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.832 EA58

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.833 EA59

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.834 EA5A

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.835 EA5B

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.836 EA5D

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.837 EA5E

Error completing the state change.

Cause

An error returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.838 EA5F

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.839 EA5G

Unexpected event for primary with standby secondary.

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.840 EA5H

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.841 EA5I

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.842 EA5J

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.843 EA5K

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.844 EA80

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.845 EA81

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.846 EA82

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.847 EA83

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.848 EA84

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.849 EA85

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.850 EA86

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.851 EA87

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.852 EA88

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.853 EA89

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.854 EA8A

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.855 EA8B

Unexpected event for qualified secondary with primary.

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.856 EA8C

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.857 EA90

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.858 EA91

Event received in wrong state. Secondary RM encounters a major unrecoverable fault during initial synchronization.

Cause

State

Solution

Reset the RM ("RM_CA02" on page 507) or cycle power to the secondary chassis.

4.5.859 EA92

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.860 EA93

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.861 EA94

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.862 EA95

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.863 EA96

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.864 EA97

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.865 EA98

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.866 EA99

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.867 EA9A

Unexpected event for primary with standby secondary.

Cause

Event.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.868 EA9B

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.869 EAA0

Event received in wrong state.

Cause

State

Solution

None. Disconnect and connect the redundancy cable.

4.5.870 EAA1

Event received in wrong state.

Cause

State

Solution

None. Disconnect and connect the redundancy cable.

4.5.871 EAA2

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.872 EAA3

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.873 EAA4

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.874 EAA5

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.875 EAA6

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.876 EAA7

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.877 EAA8

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.878 EAA9

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.879 EAAA

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.880 EAAB

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.881 EAAC

Switchover complete event with wrong switchover phase.

Cause

- Switchover phase.
- State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.882 EAAD

Unexpected redundancy state from partner.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.883 EAAF

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.884 EAAG

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.885 EAAH

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.886 EAAI

Unexpected event for disqualified secondary with no primary.

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.887 EAAJ

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.888 EAAK

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.889 EAAL

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.890 EAAM

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.891 EAAN

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.892 EAB0

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.893 EAB1

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.894 EAB2

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.895 EAB3

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.896 EAB4

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.897 EAB5

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.898 EAB6

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.899 EAB7

Event received in wrong state.

Cause

State

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.900 EAB8

Switchover complete event with wrong switchover phase.

Cause

* Switchover phase.
* State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.901 EAB9

Unexpected redundancy state.

Cause

Redundancy state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.902 EABA

Error completing the state change.

Cause

An error value returned from jbaStateChangeComplete.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.903 EABB

Unexpected event for standby secondary with primary.

Cause

Event

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.904 EABC

Error entering event into transition queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.905 EAC0

Error posting event.

Cause

An error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.906 EAC1

Error posting urgent event priority.

Cause

An error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.907 EAC2

Error posting undefined event priority.

Cause

An error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.908 EAC3

Error posting event.

Cause

An error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.909 EAC4

Error entering event into main queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.910 EADO

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.911 EAD1

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.912 EAD2

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.913 EAD3

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.914 EAD4

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.915 EAD5

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.916 EAD6

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.917 EAD7

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.918 EAD8

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.919 EAD9

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.920 EADA

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.921 EADB

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.922 EADC

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.923 EADD

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.924 EADE

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.925 EADF

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.926 EADG

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.927 EAE0

RM's have the same serial number. The state cannot be determined.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.928 EAE1

RM's have the same serial number. The state cannot be determined.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.929 EAE2

RM's have the same serial number. The state cannot be determined.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.930 EAE3

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.931 EAE4

Unexpected event for rules.

Cause

Event.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.932 EAE5

Primary capability checks with a module that is not communicating has maxed out the number of retries. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.933 EAE6

Primary capability checks with a module that is not communicating has maxed out the number of retries. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.934 EAE7

Primary capability checks with a module that is not communicating has maxed out the number of retries. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.935 EAE8

Primary capability checks with a module that is not communicating has maxed out the number of retries. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.936 EAE9

Primary capability checks with a module is not working. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.937 EAEA

Primary capability checks with a module is not working. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.938 EAEB

Primary capability checks with a module is not working. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.939 EAEC

Primary capability checks with a module is not working. The state cannot be determined without primary capability results.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.940 EAF0

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.941 EAF1

Unknown rule interruption reason.

Cause

Rule interruption reason.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.942 EAF2

Unknown rule interruption reason.

Cause

Rule interruption reason.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.943 EAF3

Unknown rule interruption reason.

Cause

Rule interruption reason.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.944 EAF4

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.945 EAF5

Rule failed to complete. At Startup, the RM encountered a Redundancy state resolution rule failure.

Cause

State.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.946 EAG0

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.947 EAG1

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.948 EAG2

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.949 EAG3

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.950 EAH0

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.951 EAH1

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.952 EAH2

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.953 EAH3

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.954 EAI0

Unknown rule determined state.

Cause

Rule determined state.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.955 EAI1

Unknown redundancy state handle.

Cause

Redundancy state handle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.956 EAJ0

Error writing to relay.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.957 EAJ1

Error writing to LED.

Cause

An error value returned from write.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.958 EB00

The configuration log is empty (and ICP_TEST_L is NOT asserted).

Cause

Solution

Assert ICP_TEST_L and reset the RM in order to have the RM auto-program the configuration log with default values.

4.5.959 EB01

The last entry in the configuration log was corrupt, and the previous two entries could also not be read.

Cause

Solution

Assert ICP_TEST_L and reset the RM in order to have the RM auto-program the configuration log with default values.

4.5.960 EB02

The last entry in the configuration log was corrupt, and the previous two entries could also not be read.

Cause

Solution

Assert ICP_TEST_L and reset the RM in order to have the RM auto-program the configuration log with default values.

4.5.961 EB03

The last entry in the configuration log was corrupt, and the previous two entries could also not be read.

Cause

Solution

Assert ICP_TEST_L and reset the RM in order to have the RM auto-program the configuration log with default values.

4.5.962 EB05

Problems recovering a corrupted configuration log (trying to erase corrupted log).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.963 EB06

Problems recovering a corrupted configuration log (trying to write valid entry to replace corrupted log).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.964 EB10

Unable to take semaphore for the FLASH device. "RM_CA02" on page 507.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.965 EB11

Unable to take semaphore for event log.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.966 EB12

Unable to take semaphore for configuration log.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.967 EB13

Unable to take semaphore for event log.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.968 EB14

Unable to take semaphore for configuration log.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.969 EB15

Unable to write new entry to configuration log.

Cause

Solution

Try to write a new configuration entry (by making a configuration change), or assert ICP_TEST_L and reset the RM ("RM_CA02" on page 507). Replacing the RM ("RM_CA01" on page 506) may be necessary.

4.5.970 EB16

Unable to erase the next sector for the configuration log.

Cause

Solution

Try to write a new configuration entry (by making a configuration change), or assert ICP_TEST_L and reset the RM ("RM_CA02" on page 507). Replacing the RM ("RM_CA01" on page 506) may be necessary.

4.5.971 EC00

Unable to create semaphore for application resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.972 EC01

Unable to create semaphore for the request forwarding array.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.973 EC02

Unable to take semaphore for the application resource table.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.974 EC03

Unable to give semaphore for the application resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.975 EC04

Unable to give semaphore for the application resource table.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.976 EC05

A send was requested for an invalid port.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.977 EC06

Unable to take semaphore for the request forwarding array.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.978 EC07

Unable to create link consumer for the multicast connection.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.979 ED00

Unable to start watchdog used for updating the partner's current time.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.980 ED10

Unable to allocate a combuf for sending new offset from CST.

Cause

Solution

None.

4.5.981 ED11

Unable to allocate an UCMM resource for sending time update to partner.

Cause

Solution

None.

4.5.982 ED12

Invalid response handle received.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.983 ED13

Unable to start watchdog used for updating the partner's current time.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.984 ED14

Unable to allocate a combuf for sending new time to partner WCT object.

Cause

Solution

None.

4.5.985 ED20

Unable to take semaphore used synchronize the wall clock time task.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.986 ED21

Unable to allocate combuf for sending GET_ATTRIBUTES_ALL request to partner WCT object.

Cause

An error value returned from semTake.

Solution

None.

4.5.987 ED22

Unable to allocate an UCMM resource for sending GET_ATTRIBUTES_ALL request to partner WCT object.

Cause

Solution

None.

4.5.988 ED23

Unable to start watchdog used for updating the partner's current time.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.989 ED30

Unable to read application revision from configuration log.

Cause

An error value returned from cfgReadAppRevision.

Solution

None.

4.5.990 ED31

Unable to write application revision to configuration log.

Cause

An error value returned from cfgWriteAppRevision.

Solution

None.

4.5.991 EE00

DC_FAIL Interrupt has occured.

Cause

- Value of the hardware watchdog timer register.
- RM watchdog count value.

Solution

If the chassis did not actually power down, reset the RM. Go to "RM_CA02" on page 507.

4.5.992 EF00

Unable to post event to the NVS Object.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.993 EF10

Received unhandled event.

Cause

Event type received.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.994 EF11

Error when receiving messages from message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.995 EF20

Unable to read message from NVS Task message queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.996 EF21

Unable to prepare response buffer for an update service request.

Cause

Solution

None.

4.5.997 EF22

The pointer to the response routine was NULL.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.998 EF23

Unable to prepare response buffer for a transfer service request.

Cause

Solution

None.

4.5.999 EF24

The pointer to the response routine was NULL. Unable to send response to transfer service request.

Cause

Solution

None.

4.5.1000 EF30

Received unknown event.

Cause

Event received.

Solution

None.

4.5.1001 EG02

A second major unrecoverable fault has been declared.

Cause

- Fault code of second major fault declared.
- First argument of second major fault declared.

Solution

Follow the action of the first major fault declared (probably reset the RM).

4.5.1002 EG10

The default exception handler was called by the OS.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1003 EG11

The reboot handler was called by the OS.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1004 EH01

Unable to create a message queue for Self Test Object events.

Cause

An error value returned from msgQCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1005 EH02

Unable to spawn the Self Test Object event handling task.

Cause

An error value returned from taskSpawn.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1006 EH03

Unable to create a watchdog timer for use in timing Self Test Object operations.

Cause

An error value returned from wdCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1007 EH04

Unable to create a semaphore for use in Self Test Object scheduling.

Cause

An error value returned from semBCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1008 EH05

Unable to create a semaphore for use in coordinating Self Test Object operations with Switchovers.

Cause

An error value returned from semBCreate.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1009 EH06

Unable to spawn the Self Test Object test scheduling task.

Cause

An error value returned from taskSpawn.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1010 EH07

Unable to register the Self Test Object with the ICP Toolkit (Backplane comm).

Cause

An error value returned from classRegister.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1011 EH0A

A failure occurred in a Self Test Object attempt to take a semaphore which blocks self tests during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1012 EH10

Error occurred in reception of an event message.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1013 EH11

Failed in attempt to forward events to partner RM.

Cause

Status (no zero) value returned from stoForwardFaultEvent.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1014 EH12

An invalid event type accompanied a request to forward an event to the partner RM.

Cause

- Event type which accompanied request.
- Current error value.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1015 EH20

Failed attempt to allocate a comm buffer.

Cause

An error value returned from ComBuf_Malloc.

Solution

None.

4.5.1016 EH21

Failed attempt to open a connection to the partner RM.

Cause

An error value returned from bcUcmmOpen.

Solution

None.

4.5.1017 EH22

Failed attempt to send a request to the partner RM.

Cause

An error value returned from bcUcmmSendRequest.

Solution

None.

4.5.1018 EH23

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1019 EH24

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1020 EH25

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1021 EH26

Failed attempt to recycle connection with the partner RM.

Cause

An error value returned from bcUcmmRecycle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1022 EH27

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1023 EH28

Invalid or false Secondary Device Status collection state encountered while awaiting response from the partner RM.

Cause

State enumeration.

Solution

None.

4.5.1024 EH29

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1025 EH2A

A failure occurred in a Self Test Object's preliminary attempt to take a semaphore which blocks this function during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1026 EH2B

A failure occurred in a Self Test Object's final (just prior to sending a request message) attempt to take a semaphore which blocks this function during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1027 EH30

Failed attempt to allocate a comm buffer.

Cause

An error value returned from ComBuf_Malloc.

Solution

None.

4.5.1028 EH3A

A failure occurred in a Self Test Object's preliminary attempt to take a semaphore which blocks this function during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1029 EH31

Failed attempt to open a connection to the partner RM.

Cause

An error value returned from bcUcmmOpen.

Solution

None.

4.5.1030 EH32

Failed attempt to send a request to the partner RM.

Cause

An error value returned from bcUcmmSendRequest.

Solution

None.

4.5.1031 EH33

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1032 EH34

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1033 EH35

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1034 EH36

Failed attempt to recycle connection with the partner RM.

Cause

An error value returned from bcUcmmRecycle.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1035 EH37

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1036 EH38

Invalid or false Secondary SYS_FAIL_L Subsystem Status collection state encountered while awaiting response from the partner RM.

Cause

State enumeration.

Solution

None.

4.5.1037 EH39

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1038 EH40

Failed attempt to allocate a comm buffer.

Cause

An error value returned from ComBuf_Malloc.

Solution

None.

4.5.1039 EH41

Failed attempt to open a connection to the partner RM.

Cause

An error value returned from bcUcmmOpen.

Solution

None.

4.5.1040 EH42

Failed attempt to send a request to the partner RM.

Cause

An error value returned from bcUcmmSendRequest.

Solution

None.

4.5.1041 EH43

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1042 EH44

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1043 EH45

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1044 EH46

Failed attempt to recycle connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1045 EH47

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1046 EH48

Invalid or false Forward Fault Event collection state encountered while awaiting response from the partner RM.

Cause

State enumeration.

Solution

None.

4.5.1047 EH49

Failed (BAD HANDLE) attempt to close connection with the partner RM.

Cause

An error value returned from bcUcmmClose.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1048 EH4A

A failure occurred in a Self Test Object's preliminary attempt to take a semaphore which blocks this function during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1049 EH50

Failed attempt to allocate a comm buffer.

Cause

An error value returned from ComBuf_Malloc.

Solution

None.

4.5.1050 EH5A

A failure occurred in a Self Test Object's preliminary attempt to take a semaphore which blocks this function during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1051 EH51

Failed attempt to open a connection to the partner RM.

Cause
- Status value returned from bcUcmmOpen.
- An error value returned from bcUcmmOpen.

Solution
None.

4.5.1052 EH52

Failed attempt to send a request to the partner RM.

Cause
- Status value returned from bcUcmmSendRequest.
- An error value returned from bcUcmmSendRequest.

Solution
None.

4.5.1053 EH53

Status of test response not SUCCESS.

Cause
- Status value returned.
- An error value returned.

Solution
None.

4.5.1054 EH60

Failed attempt to post an event in the Self Test Object Event Queue.

Cause
- Event type.
- An error value returned from msgQSend.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1055 EH70

Device Status Read - Problem encountered in preparing a response buffer.

Cause

Solution

None.

4.5.1056 EH71

Device Status Read - Routine handling a prepared response encountered a fault.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1057 EH72

SYS_FAIL Results Read - Problem encountered in preparing a response buffer

Cause

Solution

None.

4.5.1058 EH73

SYS_FAIL Results Read - Routine handling a prepared response encountered a fault.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1059 EH74

Reset Test Stats - Problem encountered in preparing a response buffer.

Cause

Solution

None.

4.5.1060 EH75

Reset Test Stats - Routine handling a prepared response encountered a fault

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1061 EH76

Set User Relay - Problem encountered in preparing a response buffer

Cause

Solution
None.

4.5.1062 EH77

Set User Relay - Routine handling a prepared response encountered a fault.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507

4.5.1063 EH78

STO Loopback Test - Problem encountered in preparing a response buffer.

Cause

Solution
None.

4.5.1064 EH79

STO Loopback Test - Routine handling a prepared response encountered a fault.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1065 EH7A

Forward Partner Fault - Problem encountered in preparing a response buffer.

Cause

Solution
None.

4.5.1066 EH7B

Forward Partner Fault - Invalid event type.

Cause

Event type.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1067 EH7C

Forward partner Fault - Routine handling a prepared response encountered a fault.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1068 EH7D

A failure occurred in a outside process's attempt to take a semaphore that would block testing during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1069 EHA1

Invalid test pulse state returned after an attempted SYS_FAIL_L test.

Cause

Test pulse state enumeration.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1070 EHA2

Failed attempt to allocate a comm buffer for use in sending a SYS_FAIL_L test request to another module.

Cause

An error value returned from ComBuf_Malloc.

Solution

None.

4.5.1071 EHA3

Failed attempt to open a connection to another module for the sake of sending a test request.

Cause

Solution

None.

4.5.1072 EHA4

Failed attempt to send a test request to another module.

Cause

An error value returned from UCMM_SendRequest.

Solution

None.

4.5.1073 EHA5

Failed attempt to close a connection following the unsuccessful sending of a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1074 EHA6

Failed attempt to close a connection following a NOT READY response to a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1075 EHA7

Failed attempt to close a connection following a READY response to a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1076 EHA8

Failed attempt to close a connection following a COMMS ERROR or NEEDS RETRY response to a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1077 EHA9

Invalid test status response state encountered regarding a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1078 EHAA

Failed attempt to allocate a comm buffer for use in sending a SYS_FAIL_L test status request to another module.

Cause

Solution

None.

4.5.1079 EHAB

Failed attempt to open a connection to another module for the sake of sending a test status request.

Cause

Solution

None.

4.5.1080 EHAC

Failed attempt to send a test status request to another module.

Cause

Solution

None.

4.5.1081 EHAD

Failed attempt to close a connection following the unsuccessful sending of a test status request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1082 EHAE

Failed attempt to close a connection following an UNSUPPORTED, BUSY, or COMPLETE response to a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1083 EHAF

Failed attempt to close a connection following an NEEDS RETRY, WAIT, or COMM ERR, or unrecognized response to a test request to another module.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1084 EHAG

Local SYS_FAIL_L input circuitry has failed local loopback test. Specifics on cause are unknown.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1085 EHAH

Local SYS_FAIL_L input circuitry has failed local loopback test. Interrupt portion was found to be faulty.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1086 EHAJ

Local SYS_FAIL_L input circuitry has failed local loopback test. Status read portion was found to be faulty.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1087 EHAK

Local SYS_FAIL_L input circuitry has failed local loopback test. Local driver portion was found to be faulty.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1088 EHAL

Local SYS_FAIL_L input circuitry has failed local loopback test. Status read portion was found to be faulty.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1089 EHAM

Local SYS_FAIL_L input circuitry has failed local loopback test. Status read occurred, but interrupt did not.

Cause

Solution

Replace RM ("RM_CA01" on page 506) at earliest opportunity. This RM will not support Synchronization if in a Secondary.

4.5.1090 EHAN

Local SYS_FAIL_L input circuitry has failed local loopback test. Invalid test results.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507. If error persists, contact Honeywell TAC.

4.5.1091 EHAP

A failure occurred in a Self Test Object's attempt to take a semaphore which would block scanning for new modules during a switchover.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1092 EHAR

A failure occurred in a Self Test Object's attempt to take a semaphore which would block SYS_FAIL_L assertion testing during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1093 EHAT

A failure occurred in a Self Test Object's preliminary attempt to take a semaphore which blocks the sending of a test status request to another module during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1094 EHAV

A failure occurred in a Self Test Object's attempt to take a semaphore which would block sending a test request to another module during a switchover.

Cause

An error value returned from semTake.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1095 EI00

During a shutdown, a fault occurred while attempting to unregister Workstation Display Object with backplance communications subsystem.

Cause

Solution

None. A shutdown situation.

4.5.1096 EI01

During a shutdown, a fault occurred while attempting to delete the Workstation Display Object task.

Cause

An error value returned from taskDelete.

Solution

None. A shutdown situation.

4.5.1097 EI02

During a shutdown, a fault occurred while attempting to delete a Workstation Display Object semaphore.

Cause

An error value returned from semDelete.

Solution

None. A shutdown situation.

4.5.1098 EI03

During a shutdown, a fault occurred while attempting to delete a Workstation Display Object watchdog timer.

Cause

An error value returned from wdDelete.

Solution

None. A shutdown situation.

4.5.1099 EI10

A failure occurred in a Workstation Display Object attempt to start a scheduling (watchdog) semaphore.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1100 EI40

A failure occurred in a Workstation Display Object attempt to start a scheduling (watchdog) semaphore.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1101 EI50

A failure occurred in a Workstation Display Object attempt to read all RM Configuration Data (via cfgReadAllData).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1102 EI51

A failure occurred in a Workstation Display Object attempt to write all RM Configuration Data (via cfgWriteNewData).

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1103 EI52

A failure occurred in a Workstation Display Object attempt to prepare a response buffer.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1104 EI53

A failure occurred in a Workstation Display Object call to the response handling routine.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1105 EI60

A failure occurred in a Workstation Display Object attempt to initialize its attributes.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1106 EI61

A failure occurred in a Workstation Display Object attempt to create a scheduling watchdog timer.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1107 EI62

A failure occurred in a Workstation Display Object attempt to create a scheduling semaphore.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1108 EI63

A failure occurred in a Workstation Display Object attempt to spawn itself.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1109 EI64

A failure occurred in a Workstation Display Object attempt to register with the comm ports.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1110 EI70

A failure occurred in a Workstation Display Object attempt to start a scheduling watchdog timer.

Cause
An error value returned from wdStart.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1111 EI71

A failure occurred in a Workstation Display Object attempt to take a scheduling semaphore.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1112 EI72

A failure occurred in a Workstation Display Object request to other RM objects to refresh their stale data.

Cause
An error value returned from semTake.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1113 EI73

A failure occurred in a Workstation Display Object attempt to determine its next refresh delay.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1114 EI74

A failure occurred in a Workstation Display Object attempt to start a scheduling watchdog timer.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1115 EI75

A failure occurred in a Workstation Display Object attempt to take a scheduling semaphore.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1116 EI80

A failure occurred in a Workstation Display Object request to BCO to updates stale attributes.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1117 EI81

A failure occurred in a Workstation Display Object request to Device Object to updates stale attributes.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1118 EI90

A failure occurred in a Workstation Display Object attempt to read RM Revision (cfgReadRevision).

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1119 EIZ0

A failure occurred in a Workstation Display Object attempt to take a scheduling (watchdog) semaphore.

Cause
An error value returned from wdCreate.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1120 EJ00

Unable to read serial number from configuration log.

Cause

Solution
Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.1121 EJ01

Unable to read the vendor ID from the configuration log.

Cause

Solution
Reset ("RM_CA02" on page 507) or replace the RM ("RM_CA01" on page 506).

4.5.1122 EJ02

Unable to register the ICP Object with the ICP Toolkit.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1123 EJ10

Unable to register the ICP Object with the ICP Toolkit.

Cause

Solution
None.

4.5.1124 EJ11

Response routine for the SET_ATTRIBUTES_ALL request is NULL.

Cause

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1125 EJ12

Unable to prepare a response buffer for a RESET request.

Cause

Solution
None.

4.5.1126 EJ13

Response routine for the RESET request is NULL.

Cause

Solution

None.

4.5.1127 EJ20

A supervisory request to the ICP ASIC failed.

Cause

State of supervisory control block.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1128 EK10

Error sending event to main watchdog manager queue.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1129 EK21

RM hardware watchdog timer test failed. The watchdog timer was disabled after being enabled.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1130 EK22

RM hardware watchdog timer test failed. The watchdog timer was not counting.

Cause

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1131 EK23

Error receiving event from main watchdog manager queue.

Cause

An error value returned from msgQReceive.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1132 EK24

All of the asynchronous tasks being checked did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Asynchronous tasks reporting.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1133 EK25

The timer clock task did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Synchronous tasks reporting.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1134 EK26

The self-test object task did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Synchronous tasks reporting.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1135 EK27

The collect attributes task did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Synchronous tasks reporting.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1136 EK28

The wall clock time object task did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Asynchronous tasks reporting.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1137 EK29

The workstation display object task did not report to the watchdog manager on time.

Cause
- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Asynchronous tasks reporting.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1138 EK2A

Unknown task index.

Cause
Task index.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1139 EK2B

Unknown event for watchdog manager to process.

Cause
Event.

Solution
Reset the RM, go to "RM_CA02" on page 507.

4.5.1140 EK2C

The event log object task did not report to the watchdog manager on time. Primary RM encounters a major shutdown fault during (power-cycle) switchover.

Cause

- Task number (upper 16 bits); number of watchdog kicks (lower 16 bits).
- Asynchronous tasks reporting.

Solution

Reset the RM, go to "RM_CA02" on page 507. If problem persists, go to "GEN_CA01" on page 499.

4.5.1141 EK40

Error starting the watchdog for checking tasks.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1142 EK70

Error starting the watchdog for kicking the hardware watchdog.

Cause

An error value returned from wdStart.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1143 EKA0

Error sending watchdog 'report in' event to backup communications unconnected message manager receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1144 EKC0

Error sending watchdog 'report in' event to backup communications link producer receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1145 EKD0

Error sending watchdog 'report in' event to ICP link producer receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1146 EKE0

Error sending watchdog 'report in' event to ICP link consumer receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1147 EKF0

Error sending watchdog 'report in' event to ICP link consumer receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1148 EKG0

Error sending watchdog 'report in' event to ICP unconnected message manager receive task.

Cause

An error value returned from msgQSend.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1149 EKT1

Unknown task index.

Cause

Task index.

Solution

Reset the RM, go to "RM_CA02" on page 507.

4.5.1150 EKU0

Unknown task index.

Cause

Task index.

Solution

Reset the RM, go to "RM_CA02" on page 507.

5 Experion Notifications

Related topics

5.1 CPM FB Generated Notifications

Related topics

5.1.1 Backup State

State Change Event generated by the secondary CPM to indicate the CPM is executing in the secondary redundancy role.

Cause

Startup or role change (e.g. switchover) into the secondary redundancy role.

Solution

N/A

5.1.2 Battery Not OK

There are two types of batteries used for CPM memory retention: {1} the lithium battery in the front of the CPM and {2} the Ni-Cad Battery Extension Module (BEM) residing in the chassis. This Diagnostic Alarm indicates either that {1} neither type of battery is present nor of proper voltage or {2} both batteries are present and of proper voltage. Note that having two batteries (of proper voltage) present is a minor fault condition.

Cause

Defective battery or invalid battery configuration.

Solution

Replace defective battery or correct invalid battery configuration "CPM_CA07" on page 503.

5.1.3 Not Synchronized

The primary and/or secondary CPM generates the Not Synchronized Diagnostic Alarm notification either upon redundancy startup (i.e. detection of RM) or detection of loss-of-synchronization. The primary and secondary CPM generates the Not Synchronized return-to-normal notification once synchronization is achieved.

Cause

Many causes that are scrutinized within the corrective action.

Solution

Isolate reason for loss-of-synchronization "CPM_CA03" on page 502.

5.1.4 RAM Sweep Error(s)

Diagnostic Alarm to indicate that a CPM run-time diagnostic was unable to correct a DRAM single bit error.

Cause

Defective CPM memory.

Solution

Restart the CPM "CPM_CA05" on page 502.

If problem persists, replace the CPM "CPM_CA06" on page 502.

5.1.5 RAM Scrub Errors

Diagnostic Alarm to indicate that the CPM encountered more than 10 single bit errors in one pass of the entire DRAM.

Cause

Defective CPM memory and/or high temperatures.

Solution

Restart the CPM "CPM_CA05" on page 502.

If problem persists, replace the CPM "CPM_CA06" on page 502.

5.1.6 REDUN Chassis ID Unknown

System Info Event to inform the user that the RM has not yet notified the CPM in which physical chassis it resides.

Cause

This CPM generation of this notification indicates {1} a transient condition during RM startup or {2} an abnormal condition whereby the RM was visible to the CPM but has failed to broadcast its physical chassis ID setting.

Solution

Check the RM resident in the CPM chassis "CPM_CA08" on page 503.

5.1.7 REDUN Chassis ID A

System Info Event to inform the user that the CPM resides in redundancy chassis A.

Cause

The RM broadcasts its physical chassis ID setting to the CPM either {1} upon completion of startup or {2} when the user changes the physical chassis ID designation.

Solution

N/A

5.1.8 REDUN Chassis ID B

System Info Event to inform the user that the CPM resides in redundancy chassis B.

Cause

The RM broadcasts its physical chassis ID setting to the CPM either {1} upon completion of startup or {2} when the user changes the physical chassis ID designation.

Solution

N/A

5.1.9 Switchover

System Info Event to indicate a redundancy switchover role change operation has occurred. Since the Not Synchronized alarm notification is also generated as a consequence of the switchover operation, it is sufficient for the Switchover notification to only be a System Info Event (i.e. detail as to the cause of loss-of-synchronization).

Cause

Redundancy role change due to a fault in the primary chassis or the receipt of the Switchover command.

Solution

N/A

5.1.10 Sync Checksum Fail

Diagnostic Alarm to indicate the secondary CPM has detected Synchronization Checksum comparison failure. The Synchronization Checksum is a synchronization maintenance integrity verification whereby the synchronized secondary CPM computes a local database checksum for verification with one calculated on the primary CPM. This represents a specific cause for persistent loss-of-synchronization which requires the secondary CPM to be restarted and/or replaced.

Cause

Data corruption during transmission from primary to secondary CPM (across redundancy cable) or Secondary CPM memory corruption.

Solution

Restart the CPM "CPM_CA05" on page 502.

If problem persists, replace the CPM "CPM_CA06" on page 502.

5.1.11 Sync HW Failure

Diagnostic Alarm to indicate that the primary CPM or secondary CPM has detected synchronization hardware failure. Moreover, problem detected either due to use of the synchronization hardware or during execution of the run-time synchronization hardware diagnostic. The corrective action for this persistent loss-of-synchronization depends on the CPM redundancy role as follows.

Cause

Synchronization hardware (i.e. Tracker mechanism) failure.

Solution

If the CPM is being used in a non-redundant configuration, replace the CPM "CPM_CA06" on page 502 at the user's earliest convenience.

If the CPM is currently in the primary redundancy role, attempt switchover to better primary "CPM_CA15" on page 504. Note that commanded initial synchronization causes the CPM to internally reset this failure condition, and if the synchronization hardware failure occurs infrequently, this provides the user a potential avenue from which to replace bad CPM HW that is currently in the primary role without loss of control.

If the CPM is currently in the secondary redundancy role, first restart the CPM "CPM_CA05" on page 502 If problem persists, replace the CPM "CPM_CA06" on page 502.

5.2 Network Diagnostic Manager (NDM) Detected Notifications

NDM detects various Critical Communication Failures and stops the Control Data Access (CDA) Server service to allow for redundant server failover. Prior to stopping the CDA Server service, an indication of the specific communication fault detected is both appended to the Error Log and posted as a diagnostic alarm. Since the NDM cannot tell whether or not it is running in a primary synchronized server, stopping the CDA Server service applies equally to a non-redundant server, the primary server (synchronized or not), and the backup server (synchronized or not). The rationale being that at least this consistent behavior results in user notification of the problem.

Attention

If CDA Server service stops as a result of a critical communication failure, the user must manually restart the CDA Server service.

NDM interprets the following conditions as critical communication failures:

Related topics

"PCIC/KTC Reports Major Fault Status" on page 378
"Lost Communication With PCIC/KTC" on page 378
"Unable to communicate through configured RSLinx driver" on page 378
"Lost communication with RSLinx" on page 379
"PCIC/KTC Lonely on ControlNet" on page 379
"C200/C200E has PCIC Lonely" on page 379

5.2.1 PCIC/KTC Reports Major Fault Status

Error Log	'<PCIC/KTC> reported MajorFault'
Detection	NDM immediately begins processing to stop the CDA Server service.
	When scanning a PCIC/KTC device, the attributes of the device's Device Object are obtained. A NDM Critical Communication Fault has occurred if the PCIC/KTC Device Object Status attribute indicates a Major Recoverable/Unrecoverable Fault.

5.2.2 Lost Communication With PCIC/KTC

Error Log	'Lost comms with <PCIC/KTC>'
Detection	NDM is unable to communicate with the PCIC/KTC after 6 consecutive attempts.
	In general, a device is removed from the scan list if NDM is unable to communicate with the particular device 7 times in a row. However, a NDM Critical Communication Fault has occurred if the device is a PCIC/KTC.

5.2.3 Unable to communicate through configured RSLinx driver

Error Log	'No comms through <driver>'
Detection	NDM is unable to communicate with the PCIC/KTC after 6 consecutive attempts.
	Similar to trigger 2 in that NDM cannot communicate with the PCIC/KTC, but this trigger covers the rare scenario for which NDM cannot communicate with a PCIC/KTC for the first time (i.e. after NDM has detected a new ControlNet RSLinx driver).

5.2.4 Lost communication with RSLinx

Error Log	'Lost comms with RSLinx'
Detection	After NDM verifies that the RSLinx process is not running, NDM immediately begins processing to stop the CDA Server service. After every unsuccessful attempt to perform either an Unconnected Send or a Driver List Query to RSLinx, NDM checks to ensure that the RSLinx process is still running.

5.2.5 PCIC/KTC Lonely on ControlNet

Error Log	'<PCIC/KTC> lonely on CNet'
Detection	NDM detects PCIC/KTC lonely condition after 6 consecutive attempts. When scanning a PCIC/KTC device, the attributes of the device's ControlNet Object are obtained. A NDM Critical Communication Fault has occurred if the PCIC/KTC indicates a lonely on ControlNet condition after 3 attempts.

5.2.6 C200/C200E has PCIC Lonely

Diagnostic Check:	C200/C200E reports Peripheral Component Interconnect Communication (PCIC) Lonely error.
Cause 1:	• Cables not connected correctly. • Cables not terminated correctly.
Solution 1:	1. Check if cables are connected properly on the A & B or just the A ControlNet Supervisory segments. 2. Check if the terminators of the correct value are installed on both ends of the segment.
Cause 2:	• C200/C200E not powered ON. • A and B cables both not healthy.
Solution 2:	Check supervisory CNI for A and B network LEDs
Cause 3:	MAC ID assigned to the PCIC card is incorrect.
Solution 3:	Check the MAC ID and assign it per guidelines in KB.

5.3 Network Diagnostic Manager Generated Notifications

The Network Diagnostic Manager (NDM) monitors the devices physically present that are not explicitly configured as part of the user's control strategy. NDM perodically updates the scan list to add and remove device of interest and monitors the devices on the scan list. It searches the Supervisory network for devices of interest, including all slots within supervisory chassis, all downlinks, and all slots within remote chassis. It monitors the devices on the scan list and generates notifications for noteworthy events. For example, the status of a connecting cable and the fault status of a device.

The NDM uses an auto-identification scheme that generates unique names for each device based on the path used to communicate with the device. First, the list of devices of interest to NDM is as follows:

CNI	ControlNet Interface module
ENET	Ethernet Interface module
KTC	(ISA Bus) PC to ControlNet interface card.
PCIC	(PCI Bus) PC to ControlNet interface card.
GW	ControlNet Gateway for either Non-Hazardous Rail I/O or Hazardous Rail I/O.
LD	Fieldbus Linking Device
PLC	Family of programmable logic controllers
CL	Control Logix 5550 controller
RM	Redundancy Module
FIM	Fieldbus Interface Module
FTEB	Fault Tolerant Ethernet Bridge module

Refer to *Reference -> Control Hardware Notifications Theory* for information about the NDM tag-coding scheme used to identify physical devices.

Note that for all of the device and Ethernet or ControlNet driver notifications, the actual user-configured RSLinx driver name string or Control Builder tag name is embedded as a prefix of the notification source to provide association to the RSLinx driver ID, if applicable. For FIM related 'los of sync' events the user-configured RSLinx driver name appears with the device/driver notification Point ID (Source). This lets additional information be given in the notification description column. Also, these alarms are reported against the RM, not the FIM, which is the actual source of the alarm. The following subsections describe possible RSLinx driver notification descriptions generated by the NDM.

Related topics

5.3.1 BOOTP Enabled

Diagnostic Alarm to indicate that the BootP setting of the specified ENET module is enabled.

Cause

User forgot to disable BootP after updating the ENET module's IP address.

Solution

Utilize the Network Tools application to disable the BootP setting of the specified ENET module.

5.3.2 Cable Failure

Diagnostic Alarm to indicate ControlNet cable failure. Note that the faulted cable (i.e. Cable A or Cable B) is specified to remove ambiguity in dual media systems.

Cause

ControlNet cable disconnected and/or defective.

Solution

Use the NDM generated Point ID (e.g. CNI0007) with the specified cable as the starting point to begin network fault isolation.

5.3.3 Card Added

System Info Event to indicate that the NDM detected the presence of a device of interest.

Cause

Module inserted in the chassis while power still applied (IUP), power applied to the chassis, or redundant controller chassis switchover has occurred.

Solution

N/A

5.3.4 Card Failure

Diagnostic Alarm to indicate that the specified device has explicitly returned a not healthy status.

Cause

Module faulted.

Solution

Restart and/or replace module based on fault code.

5.3.5 Card Removed

System Info Event to indicate that the NDM detected the absence of the specified device which was previously present.

Cause

Module removed in the chassis while power still applied (RUP), power removed to the chassis, or redundant controller chassis switchover has occurred.

Solution

N/A

5.3.6 Comm Failure

System Info Event to indicate that the NDM was not able to communicate with the specified device.

Cause

NDM is not able to communicate to the specified device because either {1} the specified device is removed or {2} as a consequence of an intermittent communication problem. The former may occur as a consequence of redundant controller chassis switchover. The latter may be due to diminished unconnected communication bandwidth somewhere in between the PC (i.e. on which the NDM runs) and the specified device.

Solution

Not applicable, if this notification precedes device removal. Otherwise, use the Network Tools application to investigate diminished communication bandwidth between the PC and the specified device.

5.3.7 Driver Added

System Info Event to indicate that the NDM detected the presence of a new ControlNet or Ethernet RSLinx driver.

Cause

New RSLinx driver configured.

Solution

N/A

5.3.8 Driver Removed

System Info Event to indicate that the NDM detected the absence of a previously configured ControlNet or Ethernet RSLinx driver.

Cause

RSLinx driver deleted.

Solution

N/A

5.3.9 Fieldbus devices not communicating or intermittent

Diagnostic check

Check noise levels and voltage levels using a handheld voltmeter (Relcom fieldbus monitor) that can give health of fieldbus link

Cause

- Noise
- Voltage
- Power supply

Solution

Route field signal cables through conduit and at a distance from power cables.

Check the power supply. Use a conditioned power supply; ordinary power supply is not suitable.

5.3.10 Fieldbus Interface Module (FIM) does not respond

Diagnostic check

FIM does not accept downloads. FIM does not show previous configuration.

Cause

Multiple downloads; downloads not completed. Typically occurs when experimenting prior to site deployment.

Solution

Clear FIM memory by temporarily placing FIM on a different slot. The change will be detected and the memory reset.

Limit trial downloads to as few as possible.

5.3.11 FIM CABLE DISCONNECT, RTP SLOT: XX

Diagnostic Alarm to indicate the RTP cable has been disconnected.

Cause

Disconnected RTP cable.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the FIM slot number in the description field to find the FIM with the disconnected RTP cable.

5.3.12 FIM CABLE FAILURE, FIM OR RTP SLOT: XX

Diagnostic Alarm to indicate the FIM or RTP cable has failed.

Cause

The primary and secondary FIMs see a different amount of devices. This indicates a failure of a FIM module or RTP cable.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description field as the starting point to begin network fault isolation.

5.3.13 FIM DAUGHTER FAIL SLOT : XX

Diagnostic Alarm to indicate a daughter board failure.

Cause

The FIM daughter board has failed.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure. Restart the module. If the problem persists, replace FIM hardware

5.3.14 FIM DAUGHTER BOARD DIAGNOSTIC FAIL SLOT: XX

Diagnostic Alarm to indicate a run time diagnostic failure on the daughter board.

Cause

Run time diagnostic failure of the daughter board.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure. Restart the module. If the problem persists, replace FIM hardware

5.3.15 FIM FIRMWARE ERROR, BUFFERS NOT ALLOCATED SLOT: XX

Diagnostic Alarm to indicate a firmware error.

Cause

Buffers not allocated.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure. Restart module.

5.3.16 FIM FIRMWARE ERROR, OUT OF SYNC BUFFERS: XX

Diagnostic Alarm to indicate a firmware error.

Cause

ControlNet cable disconnected and/or defective.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure. Restart module.

5.3.17 FIM SCHEDULE ERROR, NOT EXECUTING SLOT: XX

Diagnostic Alarm to indicate function block schedule not executing

Cause

Function block schedule not executing.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure. Restart module.

5.3.18 FIM LOST SYNC SLOT: XX

Diagnostic Alarm to indicate FIM lost sync.

Cause

FIM los of sync.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203) and the given slot number in the description field as the starting point to begin network fault isolation.

5.3.19 FIM SLOT: XX { Tag Identifier } (Err XX)

Diagnostic Alarm to indicate FIM lost sync due to an offending device. A Tag ID indicating the device causing the problem is included. An error code in also included. This is for Technical Support only.

Cause

Problem with the device listed in the Tag ID.

Solution

Use the NDM generated Point ID (e.g. Driver Name : RM0203), the given slot number in the description field, and the Tag ID as the starting point to begin network fault isolation.

5.3.20 Intermittent Comm Failure

The NDM executes as a continuous loop performing two phases of operation: {1} single topology scan to find any new devices and/or drivers, and {2} multiple iterations of querying status from the list of known devices.

This generic Diagnostic Alarm indicates that the NDM was not able to communicate with one or more devices in two consecutive device-query iterations.

Cause

NDM is not able to communicate to one or more devices because either {1} the specified device is removed or {2} as a consequence of an intermittent communication problem. The former may occur as a consequence of redundant controller chassis switchover. The latter may be due to diminished unconnected communication bandwidth somewhere in between the PC (i.e. on which the NDM runs) and the device(s).

Solution

Refer to the Event Journal in search of any recent Comm Failure and/or Card Removed System Info Events to determine what specific device(s) with which the NDM has trouble communicating. Be aware that removal of a device (e.g. PCIC) required for communication with other 'downstream' devices results in NDM reporting communication errors against the other 'downstream' devices. Repair/replace any device that was unexpectedly removed, and/or use the Network Tools application to investigate communication bandwidth between the PC and the specified device(s).

5.3.21 Invalid Keeper

Diagnostic Alarm to indicate that a Keeper capable ControlNet resident device does not indicate the Master Keeper Status or Backup Keeper Status.

Cause

Either {1} there is no Master Keeper on the affected ControlNet segment or {2} the specified device's programmed ControlNet parameters disagree with the ControlNet parameters being asserted by the Master Keeper.

Solution

Utilize the Network Tools application to reprogram the ControlNet parameters for the either {1} the entire ControlNet segment or {2} just the specified device.

5.3.22 KTC Failure

Either as part of NDM startup initialization or as a consequence of being unable to communicate with any devices during a portion of the topology scan, the NDM searches the NT Event Log in search of KTC related events. This Diagnostic Alarm indicates that the most recent encountered KTC related event was a KTC 'tombstone' event (as opposed to a KTC 'started successfully' event).

Cause

The presence of a KTC 'tombstone' event implicitly indicates KTC card failure.

Solution

Restart RSLinx, which indirectly resets the KTC.

5.3.23 KTC Normal

Diagnostic Alarm return-to-normal to indicate either KTC card failure recovery or that the KTC is healthy as part of NDM startup initialization. More specifically, the NDM searches the NT Event Log in search of KTC related events and encounters the 'started successfully' event.

Cause

KTC device started successfully.

Solution

N/A

5.3.24 Missing Keeper

Diagnostic Alarm to indicate that a ControlNet segment does not have a Master Keeper.

Cause

Either {1} all Keeper capable devices are in a Keeper Status other than Master or Backup (e.g. Faulted Keeper Status) or {2} there are no Keeper capable devices present on the affected ControlNet segment.

Solution

Either {1} Utilize the Network Tools application to reprogram the ControlNet parameters for the affected ControlNet segment to appropriate values (e.g. NUT 10000, UMAX 24, and SMAX 1) or {2} add a Keeper capable device to the affected ControlNet segment.

5.3.25 PCIC Failure

Either as part of NDM startup initialization or as a consequence of being unable to communicate with any devices during a portion of the topology scan, the NDM searches the NT Event Log in search of PCIC related events. This Diagnostic Alarm indicates that the most recent encountered PCIC related event was a PCIC 'tombstone' event (as opposed to a PCIC 'started successfully' event).

Cause

The presence of a PCIC 'tombstone' event implicitly indicates PCIC card failure.

Solution

Restart RSLinx, which indirectly resets the PCIC.

5.3.26 PCIC Normal

Diagnostic Alarm return-to-normal to indicate either PCIC card failure recovery or that the PCIC is healthy as part of NDM startup initialization. More specifically, the NDM searches the NT Event Log in search of PCIC related events and encounters the 'started successfully' event.

Cause

PCIC device started successfully.

Solution

N/A

5.3.27 RSLinx Initialization Failure

Diagnostic Alarm to indicate that the NDM is unable to initialize a RSLinx session.

Cause

Either {1} incompatible version of RSLinx software or {2} RSLinx not running.

Solution

{1} Verify that the appropriate version of RSLinx software is installed for the specific software release in use or {2} restart the RSLinx service.

5.3.28 RSLinx Initialized

Diagnostic Alarm return-to-normal to indicate that the NDM successfully initialized a RSLinx session.

Cause

N/A

Solution

N/A

5.3.29 RSLinx Failure

Diagnostic Alarm to indicate RSLinx service failure.

Cause

RSLinx service failure.

Solution

Restart RSLinx service.

5.3.30 RSLinx Normal

Diagnostic Alarm return-to-normal to indicate RSLinx service failure recovery.

Cause

N/A

Solution

N/A

5.3.31 UMAX Exceeded

Diagnostic Alarm to indicate that a ControlNet segment has strayed from the expected UMAX ControlNet network parameter.

Cause

Either {1} there is no Master Keeper on the affected ControlNet segment or {2} the ControlNet parameters being asserted by the Master Keeper are not valid.

Solution

Utilize the Network Tools application to reprogram the ControlNet parameters for the affected ControlNet segment to appropriate values (e.g. NUT 10000, UMAX 20 or 24, and SMAX 1).

> **Attention**
> - The UMAX must be set to 20 for downlink CNIs.
> - The UMAX must be set to 24 (or 32) for uplink CNIs.

6 C200/C200E Redundancy Module (RM) Events

Related topics

6.1 About RM Log

An individual RM log entry specifies the following information:

This Field:	Means:
Entry Number	Sequential number, unique to each entry.
Module	Type of module that submitted the event based on its Product Type and Product Code attributes.
Slot Number	Slot number of module that submitted the event.
Serial Number	Serial Number of module that submitted the event.
Source	In addition to viewing the RM's log the Network Tools utility allows the user to the RM's copy of its partner RMs log. To distinguish which RM log is being displayed the Network Tools utility specifies the RM log source as 'T' or 'O' for **T**his RM or the **O**ther RM respectively.
Event Class	Represents the event classification.
Event ID	Module-specific event.
Extended Event Info.	Module-specific extended event data.
Event Time-stamp	Time that event was observed on module that submitted the event.
Logging Time-stamp	RM time that event was stored into the event log.

6.2 CNI Generated C200/C200E RM Events

Related topics

6.2.1 ControlNet Lonely

CNI is lonely on ControlNet.

Error ID

0x0000

Cause

Cable disconnected or network related problem.

Solution

Connect the appropriate ControlNet cables so that the CNI may join the intended network and/or apply power to other nodes on the network.

6.2.2 ControlNet Not Lonely

CNI recovered from ControlNet lonely condition.

Error ID

0x0001

Cause

ControlNet cables attached, or recovery from network problem.

Solution

N/A.

6.2.3 NetWork Entity Gone

The primary CNI lost the connection with its redundant partner across the RM private-path (i.e. the redundancy cable).

Error ID

0x0002

Cause

Secondary CNI faulted/removed, one or both of the RMs faulted/removed or the redundancy cable is faulted/disconnected.

Solution

If the secondary CNI or secondary RM is faulted, power-cycle the secondary chassis.

If the primary RM is faulted, remove and reinsert the primary RM with chassis-power applied (or power-cycle the primary chassis if not performing control).

Reattach the redundancy cable if it is disconnected.

6.2.4 MacID Switches Changed to Bad

MAC switches changed from setting captured during CNI powerup state.

Error ID

0x0003

Cause

Deficient CNI hardware or user inadvertently changed the MAC switches with power applied to the CNI.

Solution

If the user was not changing the CNI MAC switch setting, replace the CNI. Otherwise, if the user was changing the CNI MAC switch setting, restore to original value or power-cycle the CNI for the new value to take effect.

6.2.5 MacID Switches Changed to OK

MAC switches returned to setting captured during CNI powerup state.

Error ID

0x0004

Cause

User restored the MAC switches to original setting.

Solution

If the user was not changing the CNI MAC switch setting, replace the CNI.

6.2.6 Bad CNet Ping for Sec Connection

The primary CNI encountered a ping error response while attempting to communicate with its redundant partner across the ControlNet path.

Error ID

0x0005

Cause

Obvious problems include secondary CNI lonely, faulted, or missing. Obscure problems include the case where the ControlNet trunk cable is broken in between the primary and secondary CNI but each CNI is not lonely.

Solution

If one of the CNIs is lonely, connect the appropriate ControlNet cables so that the CNI may join the intended network.

Use the Network Tools utility to verify that the CNI redundant pair is visible on the same ControlNet subnet.

6.2.7 ControlNet Duplicate Node

CNI encountered Duplicate Node condition.

Error ID

0x0006

Cause

CNI with duplicate MAC switch settings exists on the same ControlNet subnet.

Solution

User must determine which CNI has the improperly configured MAC switch settings and reconfigure it with the appropriate (i.e. not in use MAC ID) setting. Affected CNIs must be power-cycled to go to proper MAC ID settings.

6.2.8 ControlNet Unduplicate Node

CNI recovered from Duplicate Node condition.

Error ID
0x0007

Cause
CNI with duplicate MAC switch settings removed from the network.

Solution
N/A

6.2.9 Revision Not Compatible

The primary CNI module compatibility test failed because the redundant partner has incompatible firmware.

Error ID
0x0008

Cause
The secondary CNI has incompatible firmware.

Solution
Update the CNI firmware.

6.2.10 Node Number Not Identical

The primary CNI module compatibility test failed because the redundant partner CNI MAC Switch setting is not identical to that of the primary CNI.

Error ID
0x0009

Cause
Incorrect redundant CNI installation or attempt to use spare-CNI without setting the appropriate MAC ID.

Solution
Adjust secondary CNI MAC Switch setting to be identical to that of the primary partner CNI.

6.2.11 Unrecognized Product Code

The primary CNI has detected that the redundancy compliant partner in the same slot of the secondary chassis is not a CNI.

Error ID
0x000D

Cause

Incorrect module type in the same slot number of the secondary chassis.

Solution

Replace module in same slot of the secondary chassis with a redundancy compliant CNI (with the same single/ dual media capability and same MAC ID switch setting as the primary CNI).

6.2.12 False ControlNet Partner

The primary CNI does not reside on the same ControlNet subnet, as does the secondary CNI.

Error ID

0x000E

Cause

ControlNet trunk broken in between the redundant pair of CNIs or invalid installation.

Solution

The redundant CNI pair must reside on the same ControlNet subnet. Perform network fault isolation to ensure this requirement is satisfied.

6.2.13 Keeper Info Not Identical

The primary CNI keeper information not identical to the secondary CNI.

Error ID

0x000F

Cause

Incorrect CNI installation or attempt to use spare-CNI (previously programmed with different keeper parameters).

Solution

Use the Network Tools utility to correct whichever CNI does not specify either the Honeywell default or the user network specific keeper parameters.

6.2.14 Incompatible Product Code

The primary CNI has detected that the redundancy compliant partner in the same slot of the secondary chassis is not a compatible CNI.

Error ID

0x0010

Cause

One CNI is dual media and the other CNI is single media.

Solution

Replace CNI that does not agree with the intended single or dual network configuration.

6.2.15 ControlNet Ping Transmit Problem

The CNI (primary or secondary) encountered a problem sending ControlNet ping to the secondary partner.

Error ID

0x0011

Cause

ControlNet trunk broken in between the redundant pair of CNIs or invalid installation.

Solution

The redundant CNI pair must reside on the same ControlNet subnet. Perform network fault isolation to ensure this requirement is satisfied.

6.2.16 ControlNet Ping Transmit Success

The CNI (primary or secondary) recovered from inability to send ControlNet ping to the secondary partner.

Error ID

0x0012

Cause

The redundant CNI pair now resides on the same ControlNet subnet.

Solution

N/A

6.2.17 ICP debug - NoIcpCbFree

Event used during CNI development to indicate no free ICP CBs. This event is generated prior to the CNI entering the faulted state.

Error ID

0x0013

Cause

Software defect or defective CNI hardware.

Solution

If a secondary CNI is faulted, power-cycle the secondary chassis.

If a primary CNI is faulted, remove and reinsert the CNI with chassis-power applied (or power-cycle the primary chassis if not performing control).

If the problem persists, replace the CNI.

6.2.18 ICP debug - BadIcpFreeCbId

Event used during CNI development to indicate invalid ICP CB ID. This event is generated prior to the CNI entering the faulted state.

Error ID

0x0014

Cause

N/A

Solution

If a secondary CNI is faulted, power-cycle the secondary chassis.

If a primary CNI is faulted, remove and reinsert the CNI with chassis-power applied (or power-cycle the primary chassis if not performing control).

If the problem persists, replace the CNI.

6.2.19 ICP debug - IcpCbFree0

Event used during CNI development to indicate down to last free ICP CB. This event is generated prior to the CNI entering the faulted state.

Error ID

0x0015

Cause

N/A

Solution

If a secondary CNI is faulted, power-cycle the secondary chassis.

If a primary CNI is faulted, remove and reinsert the CNI with chassis-power applied (or power-cycle the primary chassis if not performing control).

If the problem persists, replace the CNI.

6.2.20 Smac Spontaneous ListenOnly_Mute

The CNI's ControlNet interface (SMAC) chip can no longer transmit. Code has been added to prevent this from happening during redundancy role change (e.g. switchover). However, it can still happen at powerup. The CNI restarts its SMAC chip as a consequence.

Error ID

0x0016

Cause

N/A

Solution

N/A

6.2.21 Keeper Write

The CNI that posted this event has determined that its Keeper parameters have been corrupted.

Error ID

0x0017

Cause

Defective flash ROM.

Solution

Attempt to reprogram the Keeper parameters using the Network Tools utility.

If that doesn't work, replace the CNI.

6.2.22 Partner Detected

The primary CNI has attempted to trigger initial synchronization due to successful attempt to connect to secondary partner after prior attempts failed.

Error ID

0x0018

Cause

Secondary CNI insertion with chassis power applied.

Solution

N/A

6.2.23 Smac Fail

The CNI has detected that its ControlNet interface (SMAC) chip has failed its powerup or run-time diagnostics. This event is generated prior to the CNI entering the faulted state.

Error ID

0x0019

Cause

CNI SMAC chip diagnostic failure.

Solution

If a secondary CNI is faulted, power-cycle the secondary chassis.

If a primary CNI is faulted, remove and reinsert the CNI with chassis-power applied (or power-cycle the primary chassis if not performing control).

If the problem persists, replace the CNI.

6.2.24 Illegal Partner Compat. Status

The primary CNI has aborted an initial synchronization attempt due to wrong partner compatibility status.

Error ID

0x001A

Cause

Incorrect secondary CNI compatibility status.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.25 Partner In Wrong Module State

The primary CNI has aborted an initial synchronization attempt due to wrong partner module state.

Error ID

0x001B

Cause

Incorrect secondary CNI state.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.26 Partner Not Changed - Qualifying

The primary CNI has aborted an initial synchronization attempt because partner CNI failed to transition to the internal Qualifying Redundancy State.

Error ID

0x001C

Cause

Secondary CNI failed to transition to the internal Qualifying Redundancy State.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.27 Qualifying Notification Not Sent

The primary CNI has aborted an initial synchronization attempt because it was unable to issue the Qualifying Notification service to its partner CNI.

Error ID

0x001D

Cause

Primary CNI unable to issue the Qualifying Notification service.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.28 Not Compatible

The primary CNI has aborted an initial synchronization attempt because it unexpectedly received the Qualification service with phase 1 parameter (from the RM) before its partner compatibility status permits initial synchronization.

Error ID

0x001E

Cause

Race condition whereby the RM commences initial synchronization before the secondary CNI is ready.

Solution

None. The primary CNI remembers the rejected attempt to commence initial-synchronization and triggers initial-synchronization after the secondary CNI completes its partner compatibility analysis.

6.2.29 Xload Unsuccessful

The primary CNI has aborted an initial synchronization attempt because it was unable to successfully crossload connection information to its secondary partner.

Error ID

0x001F

Cause

Secondary CNI faulted/removed, one or both of the RMs faulted/removed, the redundancy cable is faulted/disconnected, or redundant connection could not be established.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.30 Partner Not Changed to Qualified

The primary CNI has aborted an initial synchronization attempt because partner CNI failed to transition to the internal Qualified Redundancy State.

Error ID

0x0020

Cause

Secondary CNI failed to transition to the internal Qualified Redundancy State.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.31 Qualified Notification Not Sent

The primary CNI has aborted an initial synchronization attempt because it was unable to issue the Qualified Notification service to its partner CNI.

Error ID

0x0021

Cause

Primary CNI unable to issue the Qualified Notification service.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.32 Qual Phase2 Req Out Of Sequence

The primary CNI has aborted an initial synchronization attempt because it unexpectedly received the Qualification service with phase 2 parameter (from the RM).

Error ID

0x0022

Cause

Primary CNI received Qualification service out of sequence.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.33 Qual Phase3 Req Out Of Sequence

The primary CNI has aborted an initial synchronization attempt because it unexpectedly received the Qualification service with phase 3 parameter (from the RM).

Error ID

0x0023

Cause

Primary CNI received Qualification service out of sequence.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.34 Qual Phase4 Req Out Of Sequence

The primary CNI has aborted an initial synchronization attempt because it unexpectedly received the Qualification service with phase 4 parameter (from the RM).

Error ID

0x0024

Cause

Primary CNI received Qualification service out of sequence.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.35 ICP ASIC Still timing

CNI encountered condition whereby the ICP Midrange ASIC is still processing data even though it didn't process a request in time.

Error ID

0x0025

Cause

N/A

Solution

N/A

6.2.36 ICP ASIC Recovered

CNI encountered condition whereby the ICP Midrange ASIC completed a request but not within the expected time frame.

Error ID

0x0026

Cause

N/A

Solution

N/A

6.2.37 Qualify Fail Due to DISQ_EVENT

The primary CNI has aborted an initial synchronization attempt because it unexpectedly received the Qualification service (from the RM) while a disqualification was still in progress.

Error ID

0x0027

Cause

Primary CNI received Qualification service out of sequence.

Solution

Power-cycle the secondary chassis or disconnect-and-reconnect the redundancy cable.

6.2.38 Spurious Buffer Pointer Error

Event used during CNI development to indicate a buffer pointer corruption problem.

Error ID

0x0028

Cause

A pointer to a connection buffer was corrupted.

Solution

If a secondary CNI is faulted, power-cycle the secondary chassis. If a primary CNI is faulted, remove and reinsert the CNI with chassis-power applied (or power-cycle the primary chassis if not performing control). If the problem persists, replace the CNI.

6.2.39 Keeper Error

Under Construction.

Error ID

0x0029

Cause

Solution

6.2.40 Combuf Pool ID Invalid

Under Construction.

Error ID

0x002A

Cause

Solution

6.2.41 Module Cmpt Disq Detected #2

Under Construction.

Error ID

0x002B

Cause

Solution

6.2.42 Partner Offline And Not Lonely

Under Construction.

Error ID
0x002C

Cause

Solution

6.2.43 Bad UMAX

Under Construction.

Error ID
0x002D

Cause

Solution

6.2.44 Good UMAX

Under Construction.

Error ID
0x002E

Cause

Solution

6.2.45 Keeper Info Updated

Under Construction.

Error ID
0x002F

Cause

Solution

6.2.46 Process Disqualification

Under Construction.

Error ID
0x0030

Cause

Solution

6.2.47 Partner Connection Closed

Under Construction.

Error ID
0x0031

Cause

Solution

6.2.48 Partner Connection Exists

Under Construction.

Error ID
0x0032

Cause

Solution

6.2.49 Failed To Create Partner Conn

Under Construction.

Error ID
0x0033

Cause

Solution

6.2.50 Create Partner Conn Retry

Under Construction.

Error ID
0x0034

Cause

Solution

6.2.51 <replace with troubleshooting topic title> error message

<replace with short description>
<replace with a context that provides further clarification of the error message and when it may occur>

Error ID
<replace with error message id, if there is one>

Error name
<replace with the short name for the error message, if there is one>

Cause
<replace with a description of the underlying cause of the error>

Solution
<replace with the solution or workaround to the error>

6.2.52 Retry Partner SMAC Not Stable

Under Construction.

Error ID
0x0036

Cause

Solution

6.2.53 Module Not Cmpt

Under Construction.

Error ID
0x0037

Cause

Solution

6.2.54 Retry Xmit Failure

Under Construction.

Error ID
0x0038

Cause

Solution

6.2.55 Entered Qual Phase1

Under Construction.

Error ID
0x0039

Cause

Solution

6.2.56 Qualified Disq-Detected #2

Under Construction.

Error ID
0x003A

Cause

Solution

6.2.57 Partner Not Set To Qualifying

Under Construction.

Error ID
0x003B

Cause

Solution

6.2.58 Qualifying Not Sent To Partner

Under Construction.

Error ID
0x003C

Cause

Solution

6.2.59 Qual Phase1 OutOfSequence Error

Under Construction.

Error ID
0x003D

Cause

Solution

6.2.60 Entered Qual Phase2

Under Construction.

Error ID
0x003E

Cause

Solution

6.2.61 Qual Phase2 OutOfSequence Error

Under Construction.

Error ID
0x003F

Cause

Solution

6.2.62 Entered Qual Phase3

Under Construction.

Error ID
0x0046

Cause

Solution

6.2.63 Partner Not Set To Qualified

Under Construction.

Error ID
0x0047

Cause

Solution

6.2.64 Qualified Not Sent To Partner

Under Construction.

Error ID
0x0048

Cause

Solution

6.2.65 Qual Phase3 OutOfSequence Error

Under Construction.

Error ID
0x0049

Cause

Solution

6.2.66 Entered Qual Phase4

Under Construction.

Error ID
0x004A

Cause

Solution

6.2.67 Qual Phase4 OutOfSequence Error

Under Construction.

Error ID
0x004B

Cause

Solution

6.2.68 Qualifying Cant Xmit

Under Construction.

Error ID
0x004C

Cause

Solution

6.2.69 Reply To RSN disqualification

Under Construction.

Error ID
0x004D

Cause

Solution

6.2.70 Module Cmpt No Partner Conn

Under Construction.

Error ID
0x004E

Cause

Solution

6.2.71 Module Cmpt XmitBuff Unavailable

Under Construction.

Error ID
0x004F

Cause

Solution

6.2.72 Module Cmpt No Response

Under Construction.

Error ID
0x0050

Cause

Solution

6.2.73 Module Cmpt Disq Detected #1

Under Construction.

Error ID
0x0051

Cause

Solution

6.2.74 Module Cmpt Cant Xmit

Under Construction.

Error ID

0x0052

Cause

Solution

6.2.75 Qualified Cant Xmit

Under Construction.

Error ID

0x0053

Cause

Solution

6.2.76 Qualifying Disq-Detected #1

Under Construction.

Error ID

0x0054

Cause

Solution

6.2.77 Qualified Disq-Detected #1

Under Construction.

Error ID

0x0055

Cause

Solution

6.2.78 Qualifying No Response

Under Construction.

Error ID

0x0056

Cause

Solution

6.2.79 Qualified No Response

Under Construction.

Error ID

0x0057

Cause

Solution

6.2.80 Qualifying Xmit Buff Unavailable

Under Construction.

Error ID

0x0058

Cause

Solution

6.2.81 Qualified Xmit Buff Unavailable

Under Construction.

Error ID

0x0059

Cause

Solution

6.2.82 Qualifying No Partner Conn

Under Construction.

Error ID
0x005A

Cause

Solution

6.2.83 Qualified No Partner Conn

Under Construction.

Error ID
0x005B

Cause

Solution

6.3 CPM Generated C200/C200E RM Events

The CPM reports the following redundancy related events to the chassis resident RM. The Network Tools utility can be used to view the RM event log.

Related topics

6.3.1 LOS_CLEANPOINT_BUFFER_OVERFLOW

<replace with short description>

Loss-of-synchronization occurred due to primary CPM detection of buffer-overflow condition while creating cleanpoint notification message for the secondary CPM.

Error ID

0x0001

Error name

UINT32) Number of data bytes.

Cause

Pointer corruption occurred due to possible memory error.

Solution

Attempt switchover to better primary "CPM_CA15" on page 504.

6.3.2 LOS_CLEANPOINT_FIFO_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of Tracker-FIFO-overflow condition while creating cleanpoint notification message for the secondary CPM. Note that the Sync HW Failure Experion Notification is also generated upon detecting this condition.

Error ID

0x0002

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Tracker Status register

Cause

Tracker-FIFO-overflow is only possible due to either incorrect revision of Boot firmware or Tracker hardware failure.

Solution

First, check Boot firmware revision "CPM_CA16" on page 504.

If using valid CPM Boot firmware, attempt switchover to better primary "CPM_CA15" on page 504.

6.3.3 LOS_CLEANPOINT_IDLE_TIMEOUT

Loss-of-synchronization occurred due to primary CPM timeout while waiting for the secondary CPM to acknowledge a cleanpoint notification message.

Error ID

0x0003

Error name

(UINT32) Elapsed time

(UINT16) tx/rx/seq

(UINT16) tx/rx/seq

…

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.4 LOS_CLEANPOINT_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out. The loss of view was detected prior to the transmission of a cleanpoint notification message.

Error ID

0x0004

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.5 LOS_CLEANPOINT_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner track-data connection.

Error ID

0x0005

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary"CPM_CA17" on page 504.

6.3.6 LOS_CPM_CONFIG_LOAD_IN_PROGRESS

Synchronization aborted/blocked due to CPM FB creation/deletion or CCL download.

Error ID

0x0006

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT16) Qualification status.

Cause

CPM FB creation/deletion or CCL download.

Solution

N/A

6.3.7 SYN_CPM_CONFIG_LOAD_END

The CPM has attempted to trigger initial synchronization due to completion of CPM FB creation/deletion or CCL download.

Error ID

0x0007

Error name

None.

Cause

CPM FB creation/deletion or CCL download completion.

Solution

N/A

6.3.8 LOS_CROSSLOAD_ERROR

In the current implementation of CPM redundancy, this event is not used.

Error ID

0x0008

Error name

None.

Cause

N/A

Solution

This is an unexpected RM Event log entry.

6.3.9 LOS_EDIT_RESOURCE_LOCKED

Loss-of-synchronization due to primary CPM detection of the presence of an undefined edit-resource being locked.

Error ID

0x0009

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

Cause

Primary CPM detection of the presence of an undefined edit resource being locked.

Solution

This is an unexpected RM Event log entry.

6.3.10 LOS_EXEC_SYNC_TIMEOUT

Loss-of-synchronization due to primary CPM timeout waiting for the secondary CPM's I/O Manager subsystem to complete forming redundant I/O connections. More specifically, initial synchronization is aborted if the

secondary CPM is unable to redundantly form at least the same number of I/O connections (per CNI) already established in the primary within some finite amount of time (e.g. 12 seconds).

Error ID

0x000A

Error name

(UINT32) Elapsed time

(UINT24) slot/actual/expected (x4 for the primary CPM).

(UINT24) slot/actual/expected (x4 for the secondary CPM).

Cause

Secondary CNI faulted and/or lonely.

Solution

Isolate secondary I/O CNI ControlNet communication fault "CPM_CA18" on page 504.

6.3.11 LOS_IOMGR_PURGE_INPROG

Indicates that the primary CPM aborted an initial synchronization attempt because the secondary CPM's I/O Manager subsystem is purging the I/O Map Table. Note that the secondary CPM's I/O Map Table purge is necessary to ensure that the disqualified secondary CPM has no I/O configuration for the I/O Manager to act upon as a consequence of a disqualify-secondary operation.

Error ID

0x000B

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

Cause

Abort initial synchronization or synchronization maintenance.

Solution

None. The primary CPM remembers the rejected attempt to commence initial-synchronization and triggers initial-sync after the secondary I/O Manager completes its I/O Map Table purge.

6.3.12 LOS_ISR_BUFFER_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of buffer-overflow condition while creating redundancy-data message for the secondary CPM.

Error ID

0x000C

Error name

(UINT32) Number of data bytes.

Cause

Pointer corruption occurred due to possible memory error.

Solution

Attempt switchover to better primary "CPM_CA15" on page 504.

6.3.13 LOS_ISR_FIFO_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of Tracker-FIFO-overflow condition while creating redundancy-data message for the secondary CPM. Note that the Sync HW Failure Experion Notification is also generated upon detecting this condition.

Error ID

0x000D

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Tracker Status register

Cause

Tracker-FIFO-overflow is only possible due to either incorrect revision of Boot firmware or Tracker hardware failure.

Solution

First, check Boot firmware revision "CPM_CA16" on page 504.

If using valid CPM Boot firmware, attempt switchover to better primary "CPM_CA15" on page 504.

6.3.14 LOS_ISR_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out.

Error ID

0x000E

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.15 LOS_ISR_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner track-data connection.

Error ID

0x000F

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.16 LOS_KEEP_ALIVE_BUFFER_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of buffer overflow condition while creating connection-keep-alive message for the secondary CPM.

Error ID

0x0010

Error name

(UINT32) Number of data bytes.

Cause

Pointer corruption occurred due to possible memory error.

Solution

Attempt switchover to better primary "CPM_CA15" on page 504.

6.3.17 LOS_KEEP_ALIVE_FIFO_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of Tracker-FIFO-overflow condition while creating connection-keep-alive message for the secondary CPM. Note that the Sync HW Failure Experion Notification is also generated upon detecting this condition.

Error ID

0x0011

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Tracker Status register

Cause

Tracker-FIFO-overflow is only possible due to either incorrect revision of Boot firmware or Tracker hardware failure.

Solution

First, check Boot firmware revision "CPM_CA16" on page 504.

If using valid CPM Boot firmware, attempt switchover to better primary "CPM_CA15" on page 504.

6.3.18 LOS_KEEP_ALIVE_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out.

Error ID

0x0012

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.19 LOS_KEEP_ALIVE_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner track-data connection.

Error ID

0x0013

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.20 LOS_PARTNER_ABSENT

In the current implementation of CPM redundancy, this event is not used.

Error ID

0x0014

Error name

None.

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.3.21 LOS_PARTNER_INCOMPATIBLE

Indicates that the primary CPM has ascertained that the redundancy compliant partner module is not compatible.

Error ID

0x0015

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Reason: 0x00000000 = Null 0x00000001 = Message size 0x00000002 = Honeywell ID 0x00000003 = Product Type 0x00000004 = Product Code 0x00000005 = Major Revision 0x00000006 = Minor Revision 0x00000007 = I/O Manager DFV Position 0x00000008 = I/O Manager DFV Size 0x00000009 = Debug LSM Address 0x0000000A = Debug LSM Size 0x0000000B = Debug LSM Revision 0x0000000C = I/O Manager LSM Address 0x0000000D = I/O Manager LSM Size 0x0000000E = I/O Manager LSM Revision 0x0000000F = CEE LSM Address 0x00000010 = CEE LSM Size 0x00000011 = CEE LSM Revision 0x00000012 = CDA LSM Address 0x00000013 = CDA LSM Size 0x00000014 = CDA LSM Revision 0x00000015 = Build ID

Cause

1. The secondary CPM has incompatible firmware (i.e. reasons 0x00000005 through 0x00000015).

1. Incorrect module type in the same slot number of the secondary chassis (i.e. reasons 0x00000001 through 0x00000004).

Solution

First, check CPM Application firmware compatibility "CPM_CA19" on page 505.

If using compatible CPM Application firmware, check CPM hardware compatibility "CPM_CA20" on page 505.

6.3.22 LOS_PARTNER_STARTUP_INCOMPLETE

Indicates that the primary CPM aborted an initial synchronization attempt because the secondary CPM has not completed system startup initialization.

Error ID

0x0016

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

Cause

Secondary CPM startup or reboot (as a consequence of switchover).

Solution

None. The primary CPM remembers the rejected attempt to commence initial-synchronization and triggers initial-sync after the secondary CPM completes system startup initialization.

6.3.23 LOS_MOVE_BUFFER_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of buffer-overflow condition while creating redundancy-data message for the secondary CPM.

Error ID

0x0017

Error name

(UINT32) Number of data bytes.

Cause

Pointer corruption occurred due to possible memory error.

Solution

Attempt switchover to better primary "CPM_CA15" on page 504.

6.3.24 LOS_MOVE_FIFO_OVERFLOW

Loss-of-synchronization occurred due to primary CPM detection of Tracker-FIFO-overflow condition while creating redundancy-data message for the secondary CPM. Note that the Sync HW Failure Experion Notification is also generated upon detecting this condition.

Error ID

0x0018

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Tracker Status register

Cause

Tracker-FIFO-overflow is only possible due to either incorrect revision of Boot firmware or Tracker hardware failure.

Solution

First, check Boot firmware revision "CPM_CA16" on page 504.

If using valid CPM Boot firmware, attempt switchover to better primary "CPM_CA15" on page 504.

6.3.25 LOS_MOVE_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out.

Error ID

0x0019

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.26 LOS_MOVE_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner track-data connection.

Error ID

0x001A

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.27 LOS_RM_CONNECTION_TIMEOUT

The CPM has requested either a switchover operation (on the primary) or a disqualify-secondary operation (on the secondary) as a consequence to the detection of RM removal.

Error ID

0x001B

Error name

None.

Cause

RM fault.

Solution

Check the RM resident in the same chassis as the CPM "CPM_CA08" on page 503.

6.3.28 LOS_SD_IDLE_TIMEOUT

Loss-of-synchronization occurred due to primary CPM timeout while waiting for the secondary CPM to acknowledge an initial sync-data message.

Error ID

0x001C

Error name

(UINT32) Elapsed time

(UINT16) tx/rx/seq

(UINT16) tx/rx/seq

…

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.29 LOS_SEC_CLEANPOINT_SEQ_ERROR

Loss-of-synchronization occurred due to secondary CPM out-of-sequence receipt of redundancy related information on the track-data connection. More specifically, a cleanpoint notification was received out-of-sequence.

Error ID

0x001D

Error name

(UINT16) Actual sequence number

(UINT16) Expected sequence number

Cause

Data corruption, on the primary CPM, during transfer across the RM private-path (i.e. redundancy cable), or on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.30 LOS_SEC_SD_SEQ_ERROR

Loss-of-synchronization occurred due to secondary CPM out-of-sequence receipt of redundancy related information on the sync-data connection. More specifically, initial synchronization data or a synchronization status query was received out-of-sequence.

Error ID

0x001E

Error name

(UINT16) Actual sequence number

(UINT16) Expected sequence number

Cause

Data corruption, on the primary CPM, during transfer across the RM private-path (i.e. redundancy cable), or on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.31 LOS_SEC_TD_ACCUMULATE_FORMAT_ERROR

Loss-of-synchronization occurred due to secondary CPM detection of data corruption within redundancy related information received from the primary CPM. Note that the data corruption was detected during synchronization maintenance.

Error ID

0x001F

Error name

(UINT32) Unsupported tracker format

(UINT32) address

(UINT32) data #1

(UINT32) data #2

Cause

Data corruption, on the primary CPM, during transfer across the RM private-path (i.e. redundancy cable), or on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.32 LOS_SEC_TD_ACCUMULATE_OVERRUN

Loss-of-synchronization occurred due to secondary CPM internal circular list overrun. This private resource accumulates redundancy-related information from the primary CPM until a cleanpoint notification is received.

Error ID

0x0020

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) pCommitBeg

(UINT32) pAccumulate

(UINT32) pCommitEnd

Cause

Secondary CPM memory corruption, or redundancy load exceeds internal secondary CPM resource (i.e. primary control strategy exceeds redundancy capacity). Realistically, control cycle overruns occur before the later case.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.33 LOS_SEC_TD_COMMIT_FORMAT_ERROR

Loss-of-synchronization occurred due to secondary CPM detection of data corruption within redundancy related information already preprocessed by the secondary CPM. Note that the data corruption was detected during synchronization maintenance.

Error ID

0x0021

Error name

(UINT32) Unsupported tracker format

(UINT32) address

(UINT32) data #1

(UINT32) data #2

Cause

Data corruption on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

6.3.34 LOS_SEC_TD_SEQ_ERROR

Loss-of-synchronization occurred due to secondary CPM out-of-sequence receipt of redundancy related information on the track-data connection.

Error ID

0x0022

Error name

(UINT16) Actual sequence number

(UINT16) Expected sequence number

Cause

Data corruption, on the primary CPM, during transfer across the RM private-path (i.e. redundancy cable), or on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.35 LOS_SEC_TD_UNPACK_FORMAT_ERROR

Loss-of-synchronization occurred due to secondary CPM detection of data corruption within redundancy related information received from the primary CPM. Note that the data corruption was detected during initial synchronization.

Error ID

0x0023

Error name

(UINT32) Unsupported tracker format

(UINT32) address

(UINT32) data #1

(UINT32) data #2

Cause

Data corruption, on the primary CPM, during transfer across the RM private-path (i.e. redundancy cable), or on the secondary CPM.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.36 LOS_SWITCHOVER_TEST

Event posted in a development environment when the CPM requests a switchover role change for testing purposes.

Error ID

0x0024

Error name

None.

Cause

Development testing.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.3.37 LOS_SYNC_CHECKSUM_FAILURE

The secondary CPM has detected Synchronization Checksum comparison failure. The Synchronization Checksum is a synchronization maintenance integrity verification whereby the synchronized secondary CPM computes a local database checksum for verification with one calculated on the primary CPM. This represents a specific cause for persistent loss-of-synchronization which requires the secondary CPM to be restarted and/or replaced. Note that the Sync Checksum Fail Experion Notification is also generated by the secondary CPM upon detecting this condition.

Error ID

0x0025

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) pMemCurrent

Cause

Data corruption during transmission from primary to secondary CPM (across redundancy cable) or Secondary CPM memory corruption.

Solution

Restart the secondary CPM "CPM_CA05" on page 502.

If the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

6.3.38 LOS_SYNC_HW_FAILURE_PRIMARY

The primary CPM posts this RM Event to indicate that it has detected synchronization hardware failure during execution of the run-time synchronization hardware diagnostic. Note that the primary CPM also generates the Sync HW Failure Experion Notification upon detecting this condition.

Error ID

0x0026

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Hardware status

(UINT32) Hardware address

(UINT32) Tracker Status register

(UINT32) Caller ID

Cause

Primary CPM synchronization hardware (i.e. Tracker mechanism) failure.

Solution

Attempt switchover to better primary CPM "CPM_CA15" on page 504.

6.3.39 LOS_SYNC_HW_FAILURE_SECONDARY

The primary and secondary CPM posts this RM Event to indicate that the secondary CPM has detected synchronization hardware failure during execution of the run-time synchronization hardware diagnostic. Note that the Sync HW Failure Experion Notification is also generated by the secondary CPM upon detecting this condition.

Error ID

0x0027

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

(UINT32) Hardware status

(UINT32) Hardware address

(UINT32) Tracker Status register

(UINT32) Caller ID

Cause

Secondary CPM synchronization hardware (i.e. Tracker mechanism) failure.

Solution

Restart the secondary CPM "CPM_CA05" on page 502.

If the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

6.3.40 LOS_TD_BUFFER_TIMEOUT

Timeout occurred while waiting for a track-data buffer to become available for use.

Error ID

0x0028

Error name

(UINT32) Elapsed time

(UINT16) tx/rx/seq

(UINT16) tx/rx/seq

…

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.41 LOS_TD_PENDING_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out.

Error ID

0x0029

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.42 LOS_TD_PENDING_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner track-data connection.

Error ID

0x002A

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.43 SYN_IOMGR_PURGE_COMPLETE

The primary CPM has attempted to trigger initial synchronization due to completion of the secondary CPM I/O Manager subsystem I/O Map Table purge operation (that occurs as a consequence of the disqualify secondary operation).

Error ID

0x002B

Error name

None.

Cause

Secondary CPM I/O Map Table purge completion.

Solution

N/A

6.3.44 SYN_PARTNER_STARTUP_COMPLETE

The CPM has attempted to trigger initial synchronization due to completion of the secondary CPM system startup.

Error ID

0x002C

Error name

None.

Cause

Secondary CPM system startup completion.

Solution

N/A

6.3.45 DBG_PSEUDO_DATABASE_WRITES

Developer event to declare that a pseudo database-write redundancy load is configured.

Error ID

0x002D

Error name

(UINT16) pseudo database-write load

Cause

CPM memory corruption or development testing.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.3.46 LOS_SD_CONN_OPEN_FAILURE

The primary CPM was unable to open the partner sync-data connection.

Error ID

0x002E

Error name

None.

Cause

Secondary CPM missing, faulted, or rebooting (as a consequence of switchover).

Solution

If the secondary CPM is not rebooting as a consequence of switchover, isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.47 LOS_SD_CONN_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the sync-data connection unexpectedly busy or timed-out.

Error ID

0x002F

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.48 LOS_SD_CONN_TX_FAILURE

Loss-of-synchronization occurred due to primary CPM inability to transmit on the partner sync-data connection.

Error ID

0x0030

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.49 LOS_TD_CONN_OPEN_FAILURE

The primary CPM was unable to open the partner track-data connection.

Error ID

0x0031

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.50 LOS_TD_CONN_RX_FAILURE

Loss-of-synchronization occurred due to primary CPM loss of view to the secondary CPM across the RM redundancy cable. More specifically, encountered the track-data connection unexpectedly busy or timed-out.

Error ID

0x0032

Error name

None.

Cause

Secondary CPM has failed or has been removed. Otherwise, if secondary CPM is present and healthy, CPM to CPM communication fault occurred across the RM redundancy cable.

Solution

Isolate communication fault with secondary "CPM_CA17" on page 504.

6.3.51 LOS_SEC_CLEANPOINT_COMMIT_TIMEOUT

Loss-of-synchronization occurred due to secondary CPM timeout during commit to memory operation (as a consequence of cleanpoint notification).

Error ID

0x0033

Error name

(UINT16) Actual sequence number

(UINT16) Expected sequence number

(UINT32) Elapsed time

Cause

Secondary CPM memory corruption, or redundancy load exceeds internal secondary CPM resource (i.e. primary control strategy exceeds redundancy capacity). Realistically, control cycle overruns occur before the later case.

Solution

First, restart the secondary CPM "CPM_CA05" on page 502.

Second, if the problem persists, replace the secondary CPM "CPM_CA06" on page 502.

Third, if the problem still persists, must reduce the primary CPM capacity consumed by the current control strategy.

6.3.52 LOS_EDIT_RESOURCE_CLEAR_INPROG

Upon issuing the Sync Secondary command, the primary CPM requests that the secondary CPM clear any persistent redundancy faults (internally known as edit resources) so that initial synchronization may be re-attempted.

Error ID

0x0034

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

Cause

The primary CPM posts this RM Event when the secondary CPM has redundancy faults that need to be cleared prior to commencing initial synchronization.

Solution

None. The primary CPM remembers the rejected attempt to commence initial-synchronization and triggers initial-sync after the secondary CPM completes edit resource initialization.

6.3.53 SYN_EDIT_RESOURCE_CLEAR_COMPLETE

The primary CPM has attempted to trigger initial synchronization due to completion of the secondary CPM initialization of all persistent redundancy faults, (which occurs upon receipt of the Sync Secondary command).

Error ID

0x0035

Error name

None.

Cause

Secondary CPM cleared all persistent redundancy faults.

Solution

N/A

6.3.54 LOS_UNKNOWN_SECONDARY_LOS

Loss-of-synchronization due to primary CPM receipt of feedback from its secondary partner. A more specific event is not used because the primary CPM is unable to interpret the reason to drop synchronization specified by the secondary CPM.

Error ID

0x0036

Error name

(UINT16) Partner Connections state machine step

(UINT16) Sync state machine step

(UINT32) Edit Resources vector

Cause

Primary CPM receipt of an undefined reason to drop synchronization from its secondary partner.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4 C200/C200E RM Generated Events

6.4.1 Communication resource error

A communication resource error occurred on the RM. The port was not or could not be determined.

Error ID

0x0001

Error name

Fault Information

Cause

Communication resource errors could be due to inadequate resources or problems accessing resources.

Solution

6.4.2 Operating system error

An operating system error occurred on the RM.

Error ID

0x0002

Error name

Fault Information

Cause

Operation on operating system resource (queues, semaphores) fails.

Solution

6.4.3 Port1 Communication resource err

A communication resource error occurred on the RM ICP port.

Error ID

0x0003

Error name

Fault Information

Cause

Communication resource errors could be due to inadequate resources or problems accessing resources.

Solution

6.4.4 Port2 Communication resource err

A communication resource error occurred on the RM inter-RM port.

Error ID

0x0004

Error name

Fault Information

Cause

Communication resource errors could be due to inadequate resources or problems accessing resources.

Solution

6.4.5 Watchdog time-out

N/A

Error ID

0x0005

Error name

Fault Information

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.6 Hardware failure

An unexpected condition or event occurred and the RM has determined the defect to exist in hardware.

Error ID

0x0006

Error name

Fault Information

Cause

Hardware failure.

Solution

Go to "RM_CA01" on page 506.

6.4.7 Firmware error

An unexpected condition or event occurred and the RM has determined the defect to exist in firmware.

Error ID

0x0007

Error name

Fault Information

Cause

Firmware defect.

Solution

6.4.8 Configuration log error

An error occurred in reading or writing to the RM configuration log.

Error ID

0x0008

Error name

Fault Information

Cause

Configuration log corrupt.

Solution

6.4.9 Dup. RM, This one not in control

Another RM has been detected and that RM is or will be in control of the chassis.

Error ID

0x0009

Error name

Fault Information

Cause

Multiple RM modules in a single chassis.

Solution

6.4.10 RM Power Down

The RM is powering down.

Error ID

0x000A

Error name

Fault Information

Cause

RM removed from chassis or chassis lost power.

Solution

None. Event posted for information purposes only.

6.4.11 Port1 Communication Error

A communication error occurred on the RM ICP port.

Error ID

0x000B

Error name

Fault Information

Cause

Communication errors could be due to many causes. The RM may not be seated properly in the chassis. The redundancy cable may not be properly attached. A module may be taking too long to process a request thus causing timeouts.

Solution

6.4.12 Port2 Communication Error

A communication error occurred on the RM inter-RM port.

Error ID

0x000C

Error name

Fault Information

Cause

Communication errors could be due to many causes. The RM may not be seated properly in the chassis. The redundancy cable may not be properly attached. A module may be taking too long to process a request thus causing timeouts.

Solution

6.4.13 Communication Error

A communication error occurred on the RM. The port was not or could not be determined.

Error ID

0x000D

Error name

Fault Information

Cause

Communication errors could be due to many causes. The RM may not be seated properly in the chassis. The redundancy cable may not be properly attached. A module may be taking too long to process a request thus causing timeouts.

Solution

6.4.14 Event Log Error

An event log error occurred. The error was a read failure, connection failure, or a resource failure.

Error ID

0x000E

Error name

Fault Information

Cause

Event log corrupt or event log partner connection lost due to redundancy cable break or removal.

Solution

6.4.15 Autoqual. Option Always

The autoqualification option has been set to always autoqualify. This configures the RM to always attempt qualification when an autoqualification trigger occurs in a disqualified state.

Error ID

0x000F

Error name

None

Cause

The RM received a request to change the autoqualification option to always.

Solution

None. Event posted for information purposes only.

6.4.16 Autoqual. Option Never

The autoqualification option has been set to never autoqualify. This configures the RM to never attempt qualification when an autoqualification trigger occurs in a disqualified state.

Error ID

0x0010

Error name

None

Cause

The RM received a request to change the autoqualification option to never.

Solution

None. Event posted for information purposes only.

6.4.17 Autoqual. Option Conditional

The autoqualification option has been set to conditional autoqualify. This configures the RM to conditionally attempt qualification when an autoqualification trigger occurs in a disqualified state. The autoqualification state is used as the conditional expression. Qualification is attempted when the autoqualification state is enabled and qualification is not attempted when the autoqualification state is disabled.

Error ID

0x0011

Error name

None

Cause

The RM received a request to change the autoqualification option to conditional.

Solution

None. Event posted for information purposes only.

6.4.18 Program Red. Ini. Cmd Disabled

Program-initiated redundancy commands have been disabled. This configures the RM to not accept redundancy commands from user programs.

Error ID

0x0012

Error name

None

Cause

The RM received a request to change the program-initiated redundancy commands option to disabled.

Solution

None. Event posted for information purposes only.

6.4.19 Program Red. Ini. Cmd Enabled

Program-initiated redundancy commands have been enabled. This configures the RM to accept redundancy commands from user programs.

Error ID

0x0013

Error name

None

Cause

The RM received a request to change the program-initiated redundancy commands option to enabled.

Solution

None. Event posted for information purposes only.

6.4.20 Password Scope Neither

The password scope has been set to neither. This configures the RM to require neither a password for access to redundancy configuration parameters or redundancy user commands.

Error ID

0x0014

Error name

None

Cause

The RM received a request to change the password scope to neither.

Solution

None. Event posted for information purposes only.

6.4.21 Password Scope Only Red. Cfg.

The password scope has been set to only redundancy configuration. This configures the RM to require a password for access to redundancy configuration parameters only.

Error ID

0x0015

Error name

None

Cause

The RM received a request to change the password scope to only require a password for redundancy configuration access.

Solution

None. Event posted for information purposes only.

6.4.22 Password Scope Only User Cmd.

The password scope has been set to only redundancy user commands. This configures the RM to require a password for access to redundancy user commands only.

Error ID

0x0016

Error name

None

Cause

The RM received a request to change the password scope to only require a password for redundancy user command access.

Solution

None. Event posted for information purposes only.

6.4.23 Password Scope Both

The password scope has been set to both. This configures the RM to require a password for access to redundancy configuration parameters and redundancy user commands.

Error ID

0x0017

Error name

None

Cause

The RM received a request to change the password scope to require a password for redundancy configuration parameters and redundancy user commands.

Solution

None. Event posted for information purposes only.

6.4.24 Chassis redundancy state PwNS

The chassis redundancy state for this chassis is primary with no secondary.

Error ID

0x0018

Error name

None

Cause

The RM either entered this state from powerup, disconnection with a secondary, or commanded to become primary.

Solution

None. Event posted for information purposes only.

6.4.25 Chassis redundancy state PwDS

The chassis redundancy state for this chassis is primary with disqualified secondary.

Error ID

0x0019

Error name

None

Cause

The RM either entered this state from powerup, disqualification, or commanded to disqualify.

Solution

None. Event posted for information purposes only.

6.4.26 Chassis redundancy state PwQS

The chassis redundancy state for this chassis is primary with qualified secondary.

Error ID

0x001A

Error name

None

Cause

The RM either entered this state from qualification due to an autoqualification trigger or a command.

Solution

None. Event posted for information purposes only.

6.4.27 Chassis redundancy state PwSS

The chassis redundancy state for this chassis is primary with standby secondary.

Error ID

0x001B

Error name

None

Cause

The RM entered this state from a command.

Solution

None. Event posted for information purposes only.

6.4.28 Chassis redundancy state DSwNP

The chassis redundancy state for this chassis is disqualified secondary with no primary.

Error ID

0x001C

Error name

None

Cause

The RM either entered this state from powerup or disconnection with a primary.

Solution

None. Event posted for information purposes only.

6.4.29 Chassis redundancy state DSwP

The chassis redundancy state for this chassis is disqualified secondary with primary.

Error ID

0x001D

Error name

None

Cause

The RM either entered this state from powerup, disqualification, or commanded to disqualify.

Solution

None. Event posted for information purposes only.

6.4.30 Chassis redundancy state QSwP

The chassis redundancy state for this chassis is qualified secondary with primary.

Error ID

0x001E

Error name

None

Cause

The RM either entered this state from qualification due to an autoqualification trigger or a command.

Solution

None. Event posted for information purposes only.

6.4.31 Chassis redundancy state SSwP

The chassis redundancy state for this chassis is standby secondary with primary.

Error ID

0x001F

Error name

None

Cause

The RM entered this state from a command.

Solution

None. Event posted for information purposes only.

6.4.32 RM Power Up

The RM has been powered on and is in the process or complete with initialization. The RM was previously powered off.

Error ID

0x0020

Error name

None

Cause

Power supplied to the chassis with the RM.

Solution

None. Event posted for information purposes only.

6.4.33 Modules Chassis State Rule

The RM pair has entered rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the modules chassis state rule. The result is found in the extended event info field.

Error ID

0x0021

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

A RM pair powered up at the same time, two primary RM's are connected, or two secondary RM's are connected.

Solution

None. Event posted for information purposes only.

6.4.34 Failed Modules Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the failed modules rule. The result is found in the extended event info field.

Error ID

0x0022

Error name

Rule Result

e.g. [0x01] Rule Loser

Cause

The RM pair progressed to this Rule check after encountering a tie for the Modules Chassis State Rule.

Solution

None. Event posted for information purposes only.

6.4.35 Disqualified Secondaries Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the disqualified secondaries rule. The result is found in the extended event info field.

Error ID

0x0023

Error name

Rule Result

e.g. [0x00] Rule Winner

Cause

The RM pair progressed to this Rule check after encountering a tie for the Failed Modules Rule.

Solution

None. Event posted for information purposes only.

6.4.36 Blank Memories Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the blank memories rule. The result is found in the extended event info field.

Error ID

0x0024

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the Disqualified Secondaries Rule.

Solution

None. Event posted for information purposes only.

6.4.37 Standby Secondaries Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the standby secondaries rule. The result is found in the extended event info field.

Error ID

0x0025

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the Blank Memories Rule.

Solution

None. Event posted for information purposes only.

6.4.38 NRC Modules Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the NRC (non-redundancy compliant) modules rule. The result is found in the extended event info field.

Error ID

0x0026

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the Standby Secondaries Rule.

Solution

None. Event posted for information purposes only.

6.4.39 Powerdown Time Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the powerdown time rule. The result is found in the extended event info field.

Error ID

0x0027

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the NRC Modules Rule.

Solution

None. Event posted for information purposes only.

6.4.40 Chassis Modules Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the chassis modules rule. The result is found in the extended event info field.

Error ID

0x0028

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the Powerdown Time Rule.

Solution

None. Event posted for information purposes only.

6.4.41 RM Serial Number Rule

The RM pair is continuing to process rules for determining primary/secondary chassis redundancy state. This RM has finished its result of the RM serial number rule. The result is found in the extended event info field.

Error ID

0x0029

Error name

Rule Result

e.g. [0x02] Rule Tie

Cause

The RM pair progressed to this Rule check after encountering a tie for the RM Serial Number Rule.

Solution

None. Event posted for information purposes only.

6.4.42 Module Insertion

The RM has detected a module inserted in the chassis. The slot number and redundancy compliance of the inserted module is found in the extended event info field.

Error ID

0x002A

Error name

Slot Number, Redundancy Compliance

e.g. Slot 0x05, Fully Compatible

Cause

Module inserted in chassis or module found during powerup of RM.

Solution

None. Event posted for information purposes only.

6.4.43 Module Removal

The RM has detected a module removed from the chassis. The slot number and redundancy compliance of the removed module is found in the extended event info field.

Error ID

0x002B

Error name

Slot Number, Redundancy Compliance

e.g. Slot 0x05, Fully Compatible

Cause

Module removed from chassis.

Solution

None. Event posted for information purposes only.

6.4.44 Autoqual. Trigger

The RM has detected an autoqualification trigger. The trigger is found in the extended event info field.

Error ID

0x002C

Error name

Trigger

e.g. [0x01] Module Request

Cause

Autoqualification trigger detected. Triggers are listed in extended data.

Solution

None. Event posted for information purposes only.

6.4.45 Qualification Attempted

The RM has made an attempt to initiate qualification for the redundant chassis pair. The reason for the qualification attempt is found in the extended event info field.

Error ID

0x002D

Error name

Qualification Attempt Reason

e.g. [0x01] Commanded Trigger

Cause

The RM either received a command to initiate qualification or an autoqualification trigger was accepted to initiate qualification.

Solution

None. Event posted for information purposes only.

6.4.46 Qualification Complete

The chassis pair has finished qualification.

Error ID

0x002E

Error name

None

Cause

All modules including the RM finished all of the qualification phases without any errors that would cause qualification to abort.

Solution

None. Event posted for information purposes only.

6.4.47 Qualification Abort

The chassis pair has aborted qualification. The reason for the qualification abort is found in the extended event info field.

Error ID

0x002F

Error name

(optional) Slot Number, Qualification Abort Reason

e.g. [0x0C00] Sec Failed Module Exists

e.g. [0x0103] Slot 0x03, Module Configuration Error

Cause

A pre-qualification check failed or an error occurred during qualification. Qualification abort reasons are listed in extended data.

Solution

6.4.48 Switchover Attempted

The RM has made an attempt to initiate switchover. The reason for the switchover attempt is found in the extended event info field.

Error ID

0x0030

Error name

Switchover Attempt Reason

e.g. [0x07] Switchover Command

Cause

The RM either received a command to initiate switchover or an event or failure triggered the switchover. Switchover attempt reasons are listed in the extended data.

Solution

None. Event posted for information purposes only.

6.4.49 Switchover Complete

The chassis has finished switchover.

Error ID

0x0031

Error name

None

Cause

All modules including the RM finished all of the switchover phases.

Solution

None. Event posted for information purposes only.

6.4.50 Autoqual. State Change

The autoqualification state has changed. The new autoqualification state and the reason for the change are found in the extended data info field.

Error ID

0x0032

Error name

Two values.

First value: Autoqualification State (2 hexadecimal digits) 0x00 = Disabled 0x01 = Enabled

Second value: Autoqualification State Change Reason (2 hexadecimal digits) 0x01 = Autoqualification Option Changed to Never 0x02 = Autoqualification Option Change to Always 0x03 = Initiate Qualification Command 0x04 = Disqualify Secondary Command 0x05 = Partner RM's Decision

Cause

The RM or partner RM received and accepted a command to initiate qualification with the autoqualification option set to conditional.

The RM or partner RM received and accepted a command to disqualify secondary with the autoqualification option set to conditional.

The RM or partner RM received and accepted a request to change the autoqualification option to never with the autoqualification state enabled.

The RM or partner RM received and accepted a request to change the autoqualification option to always with the autoqualification state disabled.

The partner RM requested the change due to a configuration mismatch at powerup.

Solution

None. Event posted for information purposes only.

6.4.51 Ini. Qual. Cmd. Accepted

The RM accepted a command to initiate qualification.

Error ID

0x0033

Error name

None

Cause

The RM received a command to initiate qualification.

Solution

None. Event posted for information purposes only.

6.4.52 Ini. Qual. Cmd. Rejected

The RM rejected a command to initiate qualification. The reason for the rejection is found in the extended data info field.

Error ID

0x0034

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

The RM received a command to initiate qualification.

Solution

6.4.53 Ini. Switchover Cmd Accepted

The RM accepted a command to initiate switchover.

Error ID

0x0035

Error name

None

Cause

The RM received a command to initiate switchover.

Solution

None. Event posted for information purposes only.

6.4.54 Ini. Switchover Cmd Rejected

The RM rejected a command to initiate switchover. The reason for the rejection is found in the extended data info field.

Error ID

0x0036

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

The RM received a command to initiate switchover.

Solution

6.4.55 Become Primary Cmd Accepted

The RM accepted a command to become primary.

Error ID

0x0037

Error name

None

Cause

The RM received a command to become primary.

Solution

None. Event posted for information purposes only.

6.4.56 Become Primary Cmd Rejected

The RM rejected a command to become primary. The reason for the rejection is found in the extended data info field.

Error ID

0x0038

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

The RM received a command to become primary.

Solution

6.4.57 Disq. Secondary Cmd Accepted

The RM accepted a command to disqualify secondary.

Error ID

0x0039

Error name

None

Cause

The RM received a command to disqualify secondary.

Solution

None. Event posted for information purposes only.

6.4.58 Disq. Secondary Cmd Rejected

The RM rejected a command to disqualify secondary. The reason for the rejection is found in the extended data info field.

Error ID

0x003A

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

The RM received a command to disqualify secondary.

Solution

6.4.59 Enter Standby Cmd Accepted

N/A

Error ID

0x003B

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.60 Enter Standby Cmd Rejected

N/A

Error ID

0x003C

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.61 Swap Control Cmd Accepted

N/A

Error ID

0x003D

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.62 Swap Control Cmd Rejected

N/A

Error ID

0x003E

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.63 Swap To Standby Cmd Accepted

N/A

Error ID

0x003F

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.64 Swap To Standby Cmd Rejected

N/A

Error ID

0x0040

Error name

CIP General Status

e.g. [0x0b] GS_ALREADY_IN_REQUESTED_MODE

Cause

N/A

Solution

This is an unexpected RM Event log entry.

6.4.65 Firmware Upgrade

N/A

Error ID

0x0041

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

6.4.66 Partner Chassis Connected

N/A

Error ID

0x0042

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

6.4.67 Partner Chassis Disconnected

N/A

Error ID

0x0043

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.68 User Initiated Time Change

N/A

Error ID

0x0044

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.69 SYS_FAIL_L Active

The RM has detected the SYS_FAIL_L signal transition to the active state.

Error ID

0x0045

Error name

None

Cause

A module in the chassis failed.

Solution

6.4.70 SYS_FAIL_L Inactive

The RM has detected the SYS_FAIL_L signal transition to the inactive state.

Error ID

0x0046

Error name

None

Cause

A failed module was removed from the chassis.

Solution

None. Event posted for information purposes only.

6.4.71 Scream Detected

N/A

Error ID

0x0047

Error name

None

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.72 Backup Communication Data Errors

An overflow in transmit or receive statistic counters of backup communication data.

Error ID

0x0048

Error name

Fault Information

Cause

Excessive backup communication data.

Solution

6.4.73 Task Failed It's Status Check

The RM watchdog manager has detected a task that has stopped responding.

Error ID

0x0049

Error name

Fault Information

Cause

An RM task is not operating properly.

Solution

6.4.74 Powerup Startup Time Changed

The RM has changed its stored powerup startup time for the chassis. This powerup time is used to make sure that all modules are given a chance to finish powerup before the RM begins primary/secondary determination.

Error ID

0x004A

Error name

Four values.

First value: Slot Number (2 hexadecimal digits) 0x## = Slot Number

Second value: Module Product Code (4 hexadecimal digits) 0x#### = Module Product Code

Third value: Module Product Type (4 hexadecimal digits) 0x#### = Module Product Type

Fourth value: Startup Time (4 hexadecimal digits) 0x#### = Startup Time

Cause

A module increases its powerup startup time such that the value is greater than the stored RM powerup startup time for the chassis. The RM has finished powerup and has detected a change in the largest powerup startup time for the chassis (a change here meaning greater or lesser than the stored powerup startup time for the chassis).

Solution

None. Event posted for information purposes only.

6.4.75 WCT set to default

The initial wall clock time value was set to the default value.

Error ID

0x004B

Error name

None

Cause

The last time stamp was invalid and the RM is initializing wall clock time object data.

Solution

None. Event posted for information purposes only.

6.4.76 WCT set to last event timestamp

The initial wall clock time value was set to the last time stamp.

Error ID

0x004C

Error name

None

Cause

The last time stamp was valid and the RM is initializing wall clock time object data.

Solution

None. Event posted for information purposes only.

6.4.77 WCT time change (> 1 second)

The time changed greater than one second.

Error ID

0x004D

Error name

None

Cause

The RM received a request to change the time. The request could come from a user or the partner RM when becoming connected.

Solution

None. Event posted for information purposes only.

6.4.78 Rule Failed

The RM encountered a problem with processing a rule. A major non-recoverable fault will occur and give more details concerning the rule failure.

Error ID

0x004E

Error name

None

Cause

Most causes are due to invalid internal RM states during rule processing.

Solution

6.4.79 Rule Interrupted by Ext. Event

The RM received an event that has stopped rule processing. Rule processing will either restart or stop because the event has taken precedence over the processing of rules.

Error ID

0x004F

Error name

None

Cause

The RM pair was disconnected or the partner RM has finished the rules before this RM and has requested this RM to switchover or enter the primary/secondary chassis redundancy state.

Solution

6.4.80 Module Rejected a State Change

A module rejected the chassis redundancy state requested by the RM.

Error ID

0x0050

Error name

Module Slot Number, Rejected Phase

e.g. Slot 0x01, phase/state = 0x0001

Cause

A module in the chassis rejected the redundancy state requested by the RM.

Solution

The RM automatically aborts the state change if the redundancy state was primary with qualified secondary, qualified secondary, primary with standby secondary, or standby secondary. Otherwise, the RM automatically forces the state change.

6.4.81 Module Rejected a Sw. Phase

A module rejected the switchover phase requested by the RM.

Error ID

0x0051

Error name

Module Slot Number, Rejected Phase

e.g. Slot 0x01, phase/state = 0x0001

Cause

A module in the chassis rejected the switchover phase requested by the RM.

Solution

The RM automatically forces the switchover phase.

6.4.82 RM Serial Numbers are the same

The RM pair has the exact same serial number.

Error ID

0x0052

Error name

Fault Information

Cause

RM's were programmed with the same serial number and the RM pair rule result for the last rule, RM serial number rule, was a tie.

Solution

One of the two RM's must be replaced.

Pick one, then go to "RM_CA01" on page 506.

6.4.83 RM application fw has changed

The RM has detected a change in the application firmware revision. This indicates that newer or older application firmware has been loaded into the RM and this is the first time that newer or older application firmware has run.

Error ID

0x0053

Error name

None

Cause

The RM was updated with newer or older application firmware.

Solution

None. Event posted for information purposes only.

6.4.84 DEBUG:: Jabba State Change

Developer event that indicates the RM state machine has transitioned to a new state.

Error ID

0x0054

Error name

State (4 hexadecimal digits) 0x#### = State

Cause

N/A

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.85 A partner RM has been connected

RM has established connection to partner RM.

Error ID

0x0055

Error name

None

Cause

Redundancy cable connecting RM pair was added or partner RM is powering up.

Solution

None. Event posted for information purposes only.

6.4.86 The partner RM screamed.

RM has detected the partner RM screaming. The partner RM has failed or lost power.

Error ID

0x0057

Error name

None

Cause

The partner RM failed or was removed or the chassis power supply failed.

Solution

6.4.87 The Health LED maybe incorrect.

The RM Health LED maybe indicating an incorrect state. The Health LED maybe indicating a connection (solid green) when there is no connection (flash green) or indicating no connection (flash green) when there is a connection (solid green).

Error ID

0x0058

Error name

Fault Information

Cause

The RM had a problem setting the device object state attribute. The RM was setting the state to the connected state or the waiting for connections state.

Solution

6.4.88 Closed Prim. Connection at Sw.

Developer event indicating closure of a primary connection at switchover.

Error ID

0x0059

Error name

Application Connection Table Index

e.g. 0x0103

Cause

Switchover.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.89 Closed Sec. Connection at Sw.

Developer event indicating closure of a secondary connection at switchover.

Error ID

0x005A

Error name

Application Connection Table Index

e.g. 0x0103

Cause

Switchover.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.90 Opened Prim. Connection at Sw.

Developer event indicating opening a primary connection at switchover.

Error ID

0x005B

Error name

Application Connection Table Index

e.g. 0x0103

Cause

Switchover.

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.91 Closed Sec. Connection at Disq.

Developer event indicating closure of a secondary connection at disqualification.

Error ID

0x005C

Error name

Application Connection Table Index

e.g. 0x0103

Cause

Disqualification

Solution

This is an unexpected RM Event log entry.

Go to "GEN_CA01" on page 499.

6.4.92 Module Rejected Qualification

Module rejected the qualification phase requested by the RM.

Error ID

0x005D

Error name

Module Slot Number, Rejected Phase

e.g. Slot 0x01, phase/state = 0x0001

Cause

A module in the chassis rejected the qualification phase requested by the RM.

Solution

The RM automatically aborts qualification.

6.4.93 Module State Change Response Bad

Module responded with an invalid chassis redundancy state.

Error ID

0x005E

Error name

Module Slot Number, Module Phase Response

e.g. Slot 0x01, Invalid Response Parameter = 0x0001

Cause

A module in the chassis responded with an incorrect response to the redundancy state requested by the RM.

Solution

6.4.94 Module Qual Response Bad

Module responded with an invalid qualification phase.

Error ID

0x005F

Error name

Module Slot Number, Module Phase Response

e.g. Slot 0x01, Invalid Response Parameter = 0x0001

Cause

A module in the chassis responded with an incorrect response to the qualification phase requested by the RM.

Solution

6.4.95 Module Switchover Response Bad

Module responded with an invalid switchover phase.

Error ID

0x0060

Error name

Module Slot Number, Module Phase Response

e.g. Slot 0x01, Invalid Response Parameter = 0x0001

Cause

A module in the chassis responded with an incorrect response to the qualification phase requested by the RM.

Solution

6.4.96 The State Change Timed Out

At least one of the chassis resident modules failed to respond to the RM's last broadcast of the chassis redundancy state.

Error ID

0x0061

Error name

[(UINT24) Slot Mask (UINT24) Slot Vector]

Redundancy State

Slots that failed to respond to the RSN

e.g. [0x4F0909 0x00002A] DSwP Slots: 01 03 05

Cause

At least one of the chassis resident modules failed to respond to the RM's last broadcast of the chassis redundancy state.

Solution

6.4.97 Executing Prim. capability check

Indicates that the RM has begun an attempt to transition the disqualified secondary chassis into the primary redundancy role.

Error ID

0x0062

Error name

None.

Cause

Either {1} RM insertion under power to a chassis with at least one module in the secondary state, or {2} receipt of the Become Primary command.

Solution

None. Event posted for information purposes only.

6.4.98 Pri. capability check failed

Indicates that the RM was unsuccessful in its attempt to transition the disqualified secondary chassis into the primary redundancy role.

Error ID

0x0063

Error name

None.

Cause

At least one (chassis resident) modules responded to the RM with an indication of its inability to transition into the primary redundancy role.

Solution

6.4.99 Pri. capability check successful

Indicates that the RM was successful in its attempt to transition the disqualified secondary chassis into the primary redundancy role.

Error ID

0x0064

Error name

None.

Cause

All (chassis resident) modules responded to the RM with an indication of their ability to transition into the primary redundancy role.

Solution

None. Event posted for information purposes only.

6.4.100 Changed vendor ID

Indicates that the RM has manipulated the specified manufacturing information to compensate for an obsolete Honeywell ID. Note that this does not save the modified Honeywell ID into non-volatile memory (i.e. this event shall be regenerated upon every RM release from reset).

Error ID

0x0065

Error name

None.

Cause

RM is one of a batch that was assigned an obsolete Honeywell ID

Solution

None. Event posted for information purposes only.

6.4.101 Changed serial number

Indicates that the RM has manipulated the specified manufacturing information to compensate for an incorrectly formatted serial number. Note that this does not save the modified serial number into non-volatile memory (i.e. this event shall be regenerated upon every RM release from reset).

Error ID

0x0066

Error name

None.

Cause

RM is one of a batch that was assigned an incorrectly formatted serial number.

Solution

None. Event posted for information purposes only.

7 Test Sequence Numbers

Related topics

7.1 C200/C200E CPM

The following table indicates the major tests performed during C200/C200E CPM startup, their test sequence numbers and their order of execution. These tests are basically a linear sequence, which uses very few subroutines and no stack. On any failure, the test loops at that location so the problem can be easily diagnosed. Note that an abnormal condition exists if the CPM remains in a particular test for more than 30 seconds at which time the specified corrective action should be performed.

7.1.1 C200/C200E CPM Test Sequence Numbers

TSN	Description	Corrective Action
0	Alphanumeric Display Test. The alphanumeric display is a write-only device. As such, it is very difficult to test automatically. However, diagnostics scroll vertical and horizontal lines and vary brightness when all segments are lit. In this way an interested user can ascertain whether the display as a whole or any particular segment are functioning properly. Note that this test sequence number is not actually displayed. The firmware version is briefly displayed after this test (e.g. 'FW E').	Replace the CPM "CPM_CA06" on page 502.
1	CPU Type &Version Check. This test is used to detect a bad, obsolete, or unexpected new CPU. The CPU chip version is briefly displayed after this test (e.g. E40+).	Replace the CPM "CPM_CA06" on page 502.
10	Flash ROM parity scan. For each ROM line (8 bytes) of the 1MB Boot Image area, the data is read and the expected parity is computed and compared with the actual parity. The test is timed.	Replace the CPM "CPM_CA06" on page 502.
11	Flash ROM parity scan time. The time needed to perform the above test is checked for reasonability. This test detects CPU Instruction Cache failure and/or ROM wait state problems.	Replace the CPM "CPM_CA06" on page 502.
12	The checksum of the Boot personality is computed and verified.	Replace the CPM "CPM_CA06" on page 502.
13	The checksum of the Boot personality Flash ROM loader is computed and verified.	Replace the CPM "CPM_CA06" on page 502.
15	Verify the DRAM Controller ASIC powered up properly.	< Replace the CPM "CPM_CA06" on page 502.
16	Load the DRAM Controller ASIC configuration file.	Replace the CPM "CPM_CA06" on page 502.
17	Verify the DRAM Controller ASIC configuration was accepted.	Replace the CPM "CPM_CA06" on page 502.
18	Read back the DRAM Controller ASIC configuration and compare with the image embedded in Boot personality.	Replace the CPM "CPM_CA06" on page 502.
20	Verify that RAM can be read/written as 32-bit words. This is the first and simplest way to access RAM. It is also the only way to know if the DRAM Controller ASIC was configured properly.	Replace the CPM "CPM_CA06" on page 502.
21	Verify that the RAM parity/checkbit path is working.	Replace the CPM "CPM_CA06" on page 502.

TSN	Description	Corrective Action
22	Verify RAM word read/write access.	Replace the CPM "CPM_CA06" on page 502.
23	Verify RAM byte read access.	Replace the CPM "CPM_CA06" on page 502.
24	Verify RAM half-word read access.	Replace the CPM "CPM_CA06" on page 502.
25	Verify RAM byte read/write access.	Replace the CPM "CPM_CA06" on page 502.
26	Verify RAM half-word read/write access.	Replace the CPM "CPM_CA06" on page 502.
27	Verify RAM half-word missaligned read/write access.	Replace the CPM "CPM_CA06" on page 502.
28	Verify RAM word misaligned read/write access.	Replace the CPM "CPM_CA06" on page 502.
29	Verify RAM double-word read/write access.	Replace the CPM "CPM_CA06" on page 502.
30	EDAC Correction test to verify that any single-bit error can both be detected and corrected irrespective of whether it occurs in the data or check bits.	Replace the CPM "CPM_CA06" on page 502.
31	EDAC Error Test to verify that a double-bit error can be detected.	Replace the CPM "CPM_CA06" on page 502.
32	After verifying that no machine check interrupt source is active, the exception is unmasked. No interrupt is expected.	Replace the CPM "CPM_CA06" on page 502.
33	Data Parity Interrupt test to verify that the data parity error detection is working by enabling data parity checking and the machine check exception, then walking through an area of ROM which has been intentionally programmed with bad parity.	Replace the CPM "CPM_CA06" on page 502.
34	RAM parity/edac sweep to ensure no multiple-bit errors exists. Single bit errors are counted, and written back for correction. On detection of an error, the memory retention magic number is cleared to force the destructive memory test.	Replace the CPM "CPM_CA06" on page 502.
35	RAM Single-bit Error Threshold Test. If more than 2 single-bit errors occurred in the previous test, force the destructive memory test. High temperatures may cause a number of single-bit errors, so this test is skipped when factory test mode is enabled.	Replace the CPM "CPM_CA06" on page 502.
36	The time required to perform the above RAM parity/edac sweep test is checked for reasonability. This test detects CPU Instruction Cache failure and/or RAM wait state problems. Note that this test is only applicable if a Multi-bit Error was not detected.	Replace the CPM "CPM_CA06" on page 502.
37	Verify that a EDAC double-bit error generates the correct machine check exception.	Replace the CPM "CPM_CA06" on page 502.
40	RAM Memory Retention Test. The magic numbers are checked to determine if the data in RAM may still be valid. In the absence of parity/edac errors, skip RAM destructive test and flush (i.e. skip to test #55).	Replace the CPM "CPM_CA06" on page 502.

TSN	Description	Corrective Action
41	RAM Destructive Pattern Test. Check address and data lines by writing a non-repeating pattern over the whole memory, then verifying it. Data parity is enabled during this test.	Replace the CPM "CPM_CA06" on page 502.
42	Flush RAM Data Zero. Write zeros to all locations and verify. Data parity is enabled during this test.	Replace the CPM "CPM_CA06" on page 502.
43	Verifies that checkbits were correct after DRAM flushed to all zeros. Sets magic number to show memory is initialized.	Replace the CPM "CPM_CA06" on page 502.
55	Enable the Data Cache and execute a RAM write/verify loop. Verify that it runs faster than it would if the cache were broken or disabled. Flush/disable cache and verify that the data was written to RAM correctly. Only uses the memory test area, so just shows that the data cache is enabled and at least partially functional.	Replace the CPM "CPM_CA06" on page 502.
56	Recompute the Boot personality checksum with Data Cache enabled. The test is timed. If either the checksum is incorrect or the test takes too long, the data cache is not working properly.	Replace the CPM "CPM_CA06" on page 502.
60	Verify that Hardware Status Register can be accessed without error.	Replace the CPM "CPM_CA06" on page 502.
61	Verify that Battery Load Applied changes state per the Battery Load Apply/Remove controls. This test is performed early because it is the only test with feedback.	Replace the CPM "CPM_CA06" on page 502.
62	Verify that the DC_FAIL/SRESET status is not asserted.	Replace the CPM "CPM_CA06" on page 502.
63	Verify that the AC_FAIL/BP_LINE_FAIL status is not asserted.	Replace the CPM "CPM_CA06" on page 502.
64	Verify that the ICP ASIC interrupt is not asserted.	Replace the CPM "CPM_CA06" on page 502.
65	Verify that the interrupt from development board is not asserted.	Replace the CPM "CPM_CA06" on page 502.
66	Verify that the interrupt from memory board is not asserted.	Replace the CPM "CPM_CA06" on page 502.
67	If factory test mode is enabled, verify that the SYS_FAIL status is not asserted for longer than a finite period, to account for other module's tests.	Replace the CPM "CPM_CA06" on page 502.
68	Verify that Watchdog Timer Timeout status is not asserted.	Replace the CPM "CPM_CA06" on page 502.
70	Verify that the ICP_FAULT status is not asserted. This would indicate that the ICP ASIC had failed to come out of reset.	Replace the CPM "CPM_CA06" on page 502.
71	ICP ASIC Release and Stuck Interrupt Test. Enables interrupts to make sure that there is no interrupt stuck in the asserted state.	Replace the CPM "CPM_CA06" on page 502.

TSN	Description	Corrective Action
72	If factory test mode is enabled, verify that system controls assert and deassert the SYSFAIL_L condition. Uses timeouts to prevent conflicts with other modules under test on the same backplane. No SYSFAIL_L interrupt test. This test fails if another module leaves SYSFAIL_L asserted.	Replace the CPM "CPM_CA06" on page 502.
73	Watchdog Timer Test. Verify that the WDT does not expire when refreshed over a period of 500 msec. Uses the WDT Test mode to verify that the WDT is capable of interrupt generation on timeout within a fininte expected time range.	Replace the CPM "CPM_CA06" on page 502.
100	ICP Shared RAM Destructive Pattern Test. Check address and data lines by writing a non-repeating pattern over the whole memory, then verifying it.	Replace the CPM "CPM_CA06" on page 502.
102	ICP Shared RAM Initialization.	Replace the CPM "CPM_CA06" on page 502.
111	ICP ASIC Register Access Test.	Replace the CPM "CPM_CA06" on page 502.
112	ICP ASIC Unique Address Echo Test. Correct access to the ICP Shared RAM from the ICP ASIC is verified through the Echo Test, by asking the ASIC to write each location's address at that address. This test is performed once for the address and once for the complement of the address.	Replace the CPM "CPM_CA06" on page 502.
113	Verify that the ICP ASIC can be locked out of ICP Shared RAM.	Replace the CPM "CPM_CA06" on page 502.
114	ICP Clock test to compare the ICP ASIC clock against the CPU clock to make sure they are running at the same relative rates.	Replace the CPM "CPM_CA06" on page 502.
116	ICP ASIC Interrupt Test.	Replace the CPM "CPM_CA06" on page 502.
120	Synchronization Hardware (i.e. Tracker mechanism) test to ensure the controller redundancy specific hardware works as expected.	Replace the CPM "CPM_CA06" on page 502.
130	Perform Application personality parity/edac scan.	Replace the CPM "CPM_CA06" on page 502.
131	Erase the Application personality if the previous test indicated a parity/edac error.	Replace the CPM "CPM_CA06" on page 502.
132	Perform parity/edac scan on the Application personality area, which has been erased.	Replace the CPM "CPM_CA06" on page 502.
133	Compute CPM Application personality checksum and compare with embedded value. A key is written in RAM to indicate whether the personality is invalid or valid depending on whether a checksum error was detected or not respectively. In other words, checksum error detection forces the CPM to execute its Boot personality.	N/A
255	The CPM has completed startup diagnostics. The Alphanumeric Display is updated to display either PASS when starting the operating system in the Boot firmware or BOOT when starting the operating system in the Application firmware.	Replace the CPM "CPM_CA06" on page 502.

7.2 C200/C200E RM

The following table indicates the major tests performed during RM startup, their test sequence numbers and their order of execution.

On any failure, the test loops at that location so the problem can be easily diagnosed.

If the RM displays any 'THxy' code (where 'xy' is any 2 alphanumeric characters) for more than 30 seconds, then a fault has occurred.

7.2.1 C200/C200E RM Corrective Actions

First, take RM Corrective Action "RM_CA02" on page 507.

If the problem persists, take RM Corrective Action "RM_CA01" on page 506.

And if it still persists, take the General Corrective Action "GEN_CA01" on page 499.

7.2.2 C200/C200E RM Test Sequence Numbers

The list of 'THxy' codes below are offered for reference purposes only. The corrective action above is the same for all codes listed.

TH00 - Startup Self Test, Phase 1 Initialization. Phase 1 focuses on CPU and Memory testing, and executes out of RM Flash memory.
TH01 - Arbalest Registers Default Value Test.
TH02 - Arbalest Internal RAM (via Arbalest BIST)
TH05 - Hardware Control/Status Register Verification Test
TH10 - LED and 4-Char Display Verification Test
TH40 - Local RAM, Walking Data Bit Test, Lower half
TH41 - Local RAM, Walking Data Bit Test, Upper half
TH42 - Local RAM, Walking Address Bit Test, Lower half
TH43 - Local RAM, Walking Address Bit Test, Upper half
TH44 - Local RAM, Bus Access Test, Lower half
TH45 - Local RAM, Bus Access Test, Upper half
TH46 - Local RAM, Data Storage Test, Lower half
TH47 - Local RAM, Data Storage Test, Upper half
TH50 - ECC RAM, Walking Data Bit Test, Lower half
TH51 - ECC RAM, Walking Data Bit Test, Upper half
TH52 - ECC RAM, Walking Address Bit Test, Lower half
TH53 - ECC RAM, Walking Address Bit Test, Upper half
TH56 - ECC RAM, Data Storage Test, Lower half
TH57 - ECC RAM, Data Storage Test, Upper half
TH61 - EDAC Code Generation Test
TH62 - EDAC Single Bit Detection/Correction Test
TH63 - EDAC Double Bit Detection Test
TH70 - Shared Bus I/F, Arbitration vs. Wait States
TH71 - Shared Bus I/F, Access vs. Wait States

TH72 - Shared Bus I/F, Parity Checking vs. Wait States
TH73 - Shared Bus I/F, Comm Controller Access vs. Wait States (including a simple Tx to Rx Transfer)
TH80 - Shared RAM, Walking Data Bit Test
TH82 - Shared RAM, Walking Address Bit Test
TH84 - Shared RAM, Bus Access Test
TH86 - Shared RAM, Data Storage Test
TH91 - Parity RAM, Parity Generation and Storage Test
TH99 - Startup Self Test, Phase 1 Termination
TH - During this time, the RM is transferring its application firmware from Flash to RAM, after which it begins execution from RAM.**
THA0 - Startup Self Test, Phase 2 Initialization. Phase 2 testing focuses on RM peripheral testing, and executes out of RAM.
THB0 - Exception Handler Verification Test Initialization
THBE - Arbalest Fault Interrupt (Parity) Test
THBS - SYS_FAIL_L Interrupt Test
THC0 - Arbalest Transmit Comm, Test Initialization
THCA - Arbalest Transmit Comm, Tx Queue Pattern Test
THCB - Arbalest Transmit Comm, Tx Queue Index/Count Test
THCC - Arbalest Transmit Comm, Tx Descriptor ID Port Test
THCH - Arbalest Transmit Comm, Receive ID Queue Test
THCJ - Arbalest Transmit Comm, Rx Queue Index/Count Test
THCK - Arbalest Transmit Comm, Rx Descriptor ID Port Test
THDA - Arbalest Transmit Comm, Local RAM TX Descriptor Processing Test
THDB - Arbalest Transmit Comm, Illegal Descriptor ID Test
THDC - Arbalest Transmit Comm, Bogus Descriptor Address Test
THDD - Arbalest Transmit Comm, Invalid Descriptor Type Test
THDE - Arbalest Transmit Comm, Invalid Destination ID Test
THDF - Arbalest Transmit Comm, Bogus Buffer Address Test
THDG - Arbalest Transmit Comm, Lookup Table Double-Bit Error Test
THDH - Arbalest Transmit Comm, Tx Descriptor Double-Bit Error Test
THDJ - Arbalest Transmit Comm, Tx Lookup Table/Descriptor Single-Bit Error Tests
THDK - Arbalest Transmit Comm, Word and Packet Count Verification
THEA - Arbalest Transmit Comm, Tx Shared Bus Descriptor Tests, Initialization
THEB - Arbalest Transmit Comm, SB Tx Descriptor Processing Tests
THEC - Arbalest Transmit Comm, Bogus Descriptor Address Test
THED - Arbalest Transmit Comm, Invalid Descriptor Type Test
THEE - Arbalest Transmit Comm, Invalid Destination Id Test
THEF - Arbalest Transmit Comm, Bogus Buffer Address Test
THEG - Arbalest Transmit Comm, Lookup Table Parity Error Test
THEH - Arbalest Transmit Comm, Tx Descriptor Parity Error Test
THEJ - Arbalest Transmit Comm, Tx Descriptor Shared Bus Access Test
THEK - Arbalest Transmit Comm, Word And Packet Count Verification Test

THFA - Arbalest Transmit Comm, Local Bus Buffer Access Tests, Initialization
THFB - Arbalest Transmit Comm, Burst = 4, Buffer Size = 1
THFC - Arbalest Transmit Comm, Burst = 4, Buffer Size = 3
THFD - Arbalest Transmit Comm, Burst = 4, Buffer Size = 4
THFE - Arbalest Transmit Comm, Burst = 4, Buffer Size = 5
THFF - Arbalest Transmit Comm, Burst = 4, Buffer Size = 20
THFG - Arbalest Transmit Comm, Burst = 8, Buffer Size = 7
THFH - Arbalest Transmit Comm, Burst = 8, Buffer Size = 8
THFJ - Arbalest Transmit Comm, Burst = 8, Buffer Size = 9
THFK - Arbalest Transmit Comm, Burst = 16, Buffer Size = 15
THFL - Arbalest Transmit Comm, Burst = 16, Buffer Size = 16
THFM - Arbalest Transmit Comm, Burst = 16, Buffer Size = 17
THFN - Arbalest Transmit Comm, Burst = 16, Buffer Size = 20
THFP - Arbalest Transmit Comm, Burst = 16, Buffer Size = 0x8000 (Word Count Rolldown)
THGA - Arbalest Transmit Comm, Shared Bus Buffer Access Tests, Initialization
THGB - Arbalest Transmit Comm, Burst = 4, Buffer Size = 1
THGC - Arbalest Transmit Comm, Burst = 4, Buffer Size = 3
THGD - Arbalest Transmit Comm, Burst = 4, Buffer Size = 4
THGE - Arbalest Transmit Comm, Burst = 4, Buffer Size = 5
THGF - Arbalest Transmit Comm, Burst = 4, Buffer Size = 20
THGG - Arbalest Transmit Comm, Burst = 8, Buffer Size = 7
THGH - Arbalest Transmit Comm, Burst = 8, Buffer Size = 8
THGJ - Arbalest Transmit Comm, Burst = 8, Buffer Size = 9
THGK - Arbalest Transmit Comm, Burst = 16, Buffer Size = 15
THGL - Arbalest Transmit Comm, Burst = 16, Buffer Size = 16
THGM - Arbalest Transmit Comm, Burst = 16, Buffer Size = 17
THGN - Arbalest Transmit Comm, Burst = 16, Buffer Size = 20
THGP - Arbalest Transmit Comm, Burst = HF/4, Buffer Size = 30
THGQ - Arbalest Transmit Comm, Burst = HF/8, Buffer Size = 30
THGR - Arbalest Transmit Comm, Burst = HF/16, Buffer Size = 30
THGS - Arbalest Transmit Comm, Burst = F, Buffer Size = 33
THHA - Arbalest Transmit Comm, Transmit Channel Operational Test, Initialization
THHB - Arbalest Transmit Comm, Transmit Channel Enable/Disable/Busy Tests
THHC - Arbalest Transmit Comm, Enable/Impact Verification Test
THHD - Arbalest Transmit Comm, Transmit Channel Reset/Abort Tests
THHE - Arbalest Transmit Comm, Send ACK When Tx Disabled Test
THHF - Arbalest Transmit Comm, Send ACK When Acknowledge Enabled Test
THHG - Arbalest Transmit Comm, Send ACK When Tx Enabled Test
THHH - Arbalest Transmit Comm, Send ACK With Tx Buffer Full Test
THHJ - Arbalest Transmit Comm, Send ACK With Tx Buffer Full And Tx Channel Enabled Test
THHK - Arbalest Transmit Comm, Tx Descriptor Processing With Tx Buffer Full
THHL - Arbalest Transmit Comm, Tx Buffer Content Validation

THJA - Arbalest Transmit Comm, Tx Acknowledge Tests, Initialization
THJB - Arbalest Transmit Comm, Tx Acknowledge Enable Test
THJC - Arbalest Transmit Comm, Tx ACK/ACK Enabled/Invalid ACK Tests
THJD - Arbalest Transmit Comm, ACK Timer/ACK Enable/TX Disable Test
THJE - Arbalest Transmit Comm, Acknowledge Turn-Off/Turn-On Test
THJF - Arbalest Transmit Comm, ACK Word Error Tests
THJG - Arbalest Transmit Comm, Tx Acknowledge/Tx Enabled Tests - No Rollback
THJH - Arbalest Transmit Comm, Tx Acknowlegde/Tx Enabled - Rollback Test
THJJ - Arbalest Transmit Comm, Tx Acknowledge Timeout Test
THJK - Arbalest Transmit Comm, Tx Acknowledge Tests - Same Slot - Success
THJL - Arbalest Transmit Comm, Tx Acknowledge Tests - Same Slot - No Rollback
THJZ - Arbalest Transmit Comm, Testing Cleanup
THK0 - Arbalest Receive Comm, Test Initialization
THKA - Arbalest Receive Comm, Packet with No Errors Test
THKB - Arbalest Receive Comm, Header with Bad Buffer Address Test
THKC - Arbalest Receive Comm, Header with Bad Descriptor Address Test
THKD - Arbalest Receive Comm, Header with Bad Descriptor Type Test
THKE - Arbalest Receive Comm, Header with Unavailable Descriptor Test
THKF - Arbalest Receive Comm, Packet with Data Block Too Big Test
THKG - Arbalest Receive Comm, Packet Duplicate Test
THLA - Arbalest Receive Comm, Header with No Error Overwrite Available Test
THLB - Arbalest Receive Comm, Header with Overwrite Unavailable Test
THLC - Arbalest Receive Comm, Header with NoError With Noise Test
THLD - Arbalest Receive Comm, Header with Admin2 Walk Parity Errors Test
THLE - Arbalest Receive Comm, Header with Various Parity Errors Test
THLF - Arbalest Receive Comm, Header with Various Special Codes Test
THLG - Arbalest Receive Comm, Header with Sliding EOF Test
THLH - Arbalest Receive Comm, Header with Sliding Packets Test
THLJ - Arbalest Receive Comm, Header with CRC Error Test
THMB - Arbalest Receive Comm, Packet with Sliding EOF Burst Length Test
THMC - Arbalest Receive Comm, Packet with Early SOF Test
THMD - Arbalest Receive Comm, Packet with CRC Error Test
THME - Arbalest Receive Comm, Packet with Parity Errors Test
THMF - Arbalest Receive Comm, Packet with Context Errors Test
THMG - Arbalest Receive Comm, Packet with Ack Word Test
THMJ - Arbalest Receive Comm, Packet with Abort Test
THMM - Arbalest Receive Comm, Packet with No Errors (Again) Test
THMP - Arbalest Receive Comm, Packet with SB Burst Length Wait States Test
THMZ - Arbalest Receive Comm, Testing Cleanup
THP0 - Arbalest HotLink I/F, Tx Bfr Test, Test Initialization
THPA - Arbalest HotLink I/F, Tx Bfr Test, Empty Flag Test
THPB - Arbalest HotLink I/F, Tx Bfr Test, Half-Full Flag Test

THPC - Arbalest HotLink I/F, Tx Bfr Test, Full Flag Test
THPD - Arbalest HotLink I/F, Tx Bfr Test, Walking Ones/Zeros Test
THQA - Arbalest HotLink I/F, Rx Bfr Test, Empty Flag Test
THQB - Arbalest HotLink I/F, Rx Bfr Test, Half-Full Flag Test
THQC - Arbalest HotLink I/F, Rx Bfr Test, Full Flag Test
THQD - Arbalest HotLink I/F, Rx Bfr Test, Walking Ones/Zeros Test
THRA - Arbalest HotLink I/F, Tx/Rx Test, Transmit Buffer Clear Tes
THRB - Arbalest HotLink I/F, Tx/Rx Test, Receive Buffer Clear Test
THRC - Arbalest HotLink I/F, Tx/Rx Test, Transmit Interface Enable/Disable Test
THRE - Arbalest HotLink I/F, Tx/Rx Test, Receive Interface Enable/Disable Test
THRF - Arbalest HotLink I/F, Tx/Rx Test, Transmit/Receive Data Transfer Test
THSA - Arbalest HotLink I/F, HOTLink BIST
THSZ - Arbalest HotLink I/F, Testing Cleanup
THZZ - Phase 2 Cleanup. End of RM Startup Self Testing.

7.3 Serial Interface Module (SIM)

The following table indicates the major tests performed during SIM startup diagnostics, their test sequence numbers and their order of execution.

> **Attention**
>
> This information is offered for reference purposes only. Should the user find that the SIM has failed one of these startup tests, the module should be replaced.

These tests are linear sequence, which uses very few subroutines and no stack. On any failure, the test loops at that location so the problem can be easily diagnosed. Note that an abnormal condition exists if the CPM remains in a particular test for more than 30 seconds at which time the specified corrective action should be performed.

In order that all LED colors can be checked by the factory test technician:

The Health LED (right-hand) will be turned RED to start. It will be turned GREEN upon successful completion of selftest.

The Channel Activity LEDs will be turned RED until completion of the Alphanumeric Display Test. They will be turned GREEN until completion of the ROM test.

Test Sequence Numbers are output first to the Factory Test Port and then to the Alphanumeric Display.

7.3.1 SIM Test Sequence Numbers

TSN	Description	Probable Cause for Error	Action on Error
0	Alphanumeric Display and LED Test -- This test walks horizontal/vertical bars, then flashes all segments of the display through stages of brightness. This test number will be output only to the Test Port, not to the Display. For this test to work, CPU, Flash ROM, address bus, data bus and some of the hardware control logic must be working. The firmware version is briefly displayed after this test.	Hardware control registers are not writable, CPU PLD.	FAULT
1	CPU Type & Version Check. This test is done before the ROM tests because a wrong CPU could appear to succeed but might fail timing tests. The CPU version is also displayed as E40+ or E41+ for 603e Rev 4.0 or 4.1, 100 MHz.	Wrong CPU chip installed.	FAULT
10	Flash ROM parity scan -- For each ROM line (8 bytes) of the 1MB Boot Image area, the data is read and the expected parity is computed and compared with the actual parity. The test is timed.	Flash chip.	FAULT
11	Flash ROM parity scan time -- the time needed to perform the above test is checked for reasonability. This test detects 603 Instruction Cache failure and/or ROM wait state problems.	Instruction Cache, MEM PLD wait states.	FAULT
12	Flash ROM checksum - The checksum of the boot personality in ROM is computed and verified.	Flash chip.	FAULT
13	Flash ROM Loader checksum - The checksum of the boot personality's Flash ROM loader is computed and verified.	Flash chip.	FAULT
15	XILINX DRAM Controller ASIC Ready check (Hardware Status Register [MEM_STATUS]). This bit is asserted if the XILINX did not power up properly.	Hardware Status Register chips, XILINX	FAULT
16	XILINX DRAM Controller ASIC Load -- The XILINX configuration file is written one bit at a time to the chip.	MEM PLD	FAULT
17	XILINX DRAM Controller ASIC Error Check (Hardware Status Register [MEM_STATUS]). This bit is asserted if the XILINX did not configure properly.	Hardware Status Register chips, XILINX, MEM PLD	FAULT

TSN	Description	Probable Cause for Error	Action on Error
18	XILINX DRAM Controller ASIC read-back verify -- The XILINX configuration file is read back 32 bits at a time, and compared to the image in ROM. A read-back mask is used to determine which bits of the stream are not to be compared for one reason or another.	XILINX, MEM PLD	FAULT
20-3x	Various RAM/Parity/Interrupt Tests	For all: RAM, XILINX, buffers, MEM PLD.	
20	RAM path - verifies that RAM can be read/written as 32-bit words. This is the first and simplest way to access RAM. It is also the only way to know if the XILINX was configured properly.		FAULT
21	RAM parity path -- writes two 8-byte patterns and verifies that parity byte was set correctly, even and odd.		FAULT
22	RAM word access - verifies that word patterns can be written and read, including three cases of miss-aligned transfer.		FAULT
23	RAM byte access - verifies that writing a string of 8 bytes can be read back as 2 correct words, and as 8 bytes.		FAULT
24	RAM half access - verifies that half words can be read.		FAULT
25	RAM byte write - verifies that bytes can be written correctly.		FAULT
26	RAM half write - verifies that half-words can be written correctly.		FAULT
27	RAM half align - verifies that half-words can be written and ready when miss-aligned.		FAULT
28	RAM word align - verifies that words can be written and ready when miss-aligned.		FAULT
29	RAM double access - verifies that the floating point unit can write and read a double-word value, and the same value is correctly stored as two words.		FAULT
30	EDAC Correction - Verifies that any single-bit error can both be detected and corrected, in data or check bits, in high or low word. One bit at a time is changed and walked through one line of RAM.		FAULT
31	EDAC Error Test - verifies that a double-bit error can be detected, in both high and low word.		FAULT
32	Stuck Machine Check interrupt - after verifying that no machine check source is active in the Hardware Status Register, unmasks the exception. No interrupt is expected.	Hardware Status Register chips, CPU PLD, MEM PLD	FAULT
33	Data Parity Interrupt -- verify that the data parity error detection is working by enabling data parity checking and the machine check exception, then walking through an area of ROM which has been programmed with bad parity. There are 8, 8-byte lines, each with a parity error in a different byte, such that all byte lanes are covered.	Parity buffers, parity circuit (CPU PLD?)	FAULT
34	RAM parity sweep - The RAM is read 2 words at a time until end or until a multiple-bit error is detected. Single bit errors are counted, and written back for correction. Parity errors (SRAM) or Multi-bit Errors (DRAM) Force destructive testing of RAM. Stress Screen can log the time for this test for profiling. On an error, the memory retention magic number is cleared to force the destructive memory test.		Destructive RAM Test
35	RAM Single-bit Error Threshold test -- The number of single-bit errors is compared against a threshold. High temperatures may cause a number of single-bit errors, so this test is skipped in Factory Test.	RAM self-refresh control, very high temp.	FAULT

TSN	Description	Probable Cause for Error	Action on Error
36	RAM parity sweep time - the time needed to perform the above test is checked for reasonability, using the PPC 603 decrementer. This test detects 603 Instruction Cache failure and/or RAM wait-state problems. Note that the time is not measured (zero) if a parity error / Multi-bit Error is detected and memory is flushed.	Instruction Cache, MEM PLD wait states	FAULT
37	EDAC Interrupt - verifies that a double-bit error will generate the correct machine check exception.	XILINX chip, Hardware Status Register chips, MEM PLD, CPU PLD	FAULT
40	RAM Memory Retention Test - The magic numbers are checked to see if the data in RAM may still be valid. In the absence of parity errors, RAM is considered valid at the boot level. If passes test, bumps power cycle counter and skips destructive test and flush.	Battery low	Fall into Destructive Test.
41	RAM Destructive Pattern Test. Checks address and data lines by writing a non-repeating pattern over the whole memory, then verifying it. Runs with data parity enabled and fatal. Two starting patterns are used for better coverage.	XILINX, RAM chip, MEM PLD	FAULT
42	Flush RAM Data Zeros - Write zeros to all locations and verify. Data parity is enabled during this test. Runs with data parity enabled and fatal.	XILINX, RAM chip, MEM PLD	FAULT
43	Flush RAM Parity Ones - verify that Flush RAM Data Zeros test forced parity byte to ones (check bits to correct value). Data parity disabled during this test, but enabled permanently after the test completes. Runs with data parity disabled. Sets magic number to show memory is initialized.	RAM chip, XILINX, Parity/check bit buffers	FAULT

Attention

Note that after the RAM tests, data parity detection is disabled.

TSN	Description	Probable Cause for Error	Action on Error
50	CPU I-Cache Active Test - Compare how many times a loop runs in one clock tick with I-Cache disabled and enabled. May not need to do this test because ROM timing test may show whether I-Cache is working or not.		FAULT
5x	Other I-Chache Tests.		FAULT
55	CPU D-Cache Active Test - Enable cache and execute a RAM write/verify loop. Verify that it runs faster than it would if the cache were broken or disabled. Flush/disable cache and verify that the data was written to RAM correctly. Only uses the memory test area, so just shows that the data cache is enabled and at least partially functional.	CPU	FAULT
5	CPU D-Cache Function Test - The checksum of the boot code is repeated with Data Cache enabled. The test is timed. If the data cache is not working properly, the checksum will fail or the test will take too long.	CPU	FAULT
5x	Other D-Cache Tests.		FAULT
60-7x	Hardware Status Register and System Controls Tests. Until these status checks are made, interrupts (SMI, INT, DEC) cannot be enabled. Machine Check is enabled and checked separately. Data parity is disabled for each hardware status register read operation.	For all: Hardware Status Register chips, CPU PLD	
60	Hardware Status Register Access Test - Verifies that the Hardware Status Register appears to be readable without generating a machine check exception.		FAULT
61	Hardware Status Register Battery Load Test - Verifies that Battery Load Applied changes state per the Battery Load Apply/Remove controls. This test is performed early because it is the only test with feedback.		FAULT
62	Hardware Status Register DC_FAIL Test - Verifies that the DC_FAIL/SRESET status is not asserted.	Backplane, P/S	FAULT

63	Hardware Status Register FTA_INT Test - Verifies that the FTA DUART interrupt status is not asserted.	CPU card DUART	FAULT
64	Hardware Status Register ICP_INT Test - Verifies that the ICP_INT status is not asserted.	ICP ASIC	FAULT
65	Hardware Status Register DEV_INT Test - Verifies that the DEV_INT (interrupt from development board) status is not asserted.	Dev Card DUART.Dev Card PLD.CPU PLD.	FAULT
66	Hardware Status Register MEM_INT Test - Verifies that the MEM_INT (interrupt from memory board) status is not asserted.	XILINX, MEM PLD	FAULT
67	Hardware Status Register SYS_FAIL Test - Verifies that the SYS_FAIL status is not asserted for longer than a TBD period, to accommodate other module's tests.	CPU PLD, backplane, other modules.	FAULT
68	Hardware Status Watchdog Timer Timeout Pending Test - Verifies that the WDT_PENDING status is not asserted.	PLD, WDT Chip	FAULT
69	Hardware Status DUART Interrupt Pending Test - Verifies that the DUART_INT status is not asserted.	DUART	FAULT
70	Hardware Status Register ICP_FAULT Test - Verifies that the ICP_FAULT status is not asserted. This would indicate that the ICP ASIC had failed to come out of reset.	ICP ASIC	FAULT
71	ICP ASIC Release and Stuck Interrupt Test - Enables interrupts to make sure that there is no interrupt stuck in the asserted state. Because the Hardware Status Register has been tested for potential interrupt sources, no interrupt is expected. Interrupts are disabled after this test. If any interrupt source is stuck, this test will fail to return from the interrupt level. Writes hardware setup parameters (such as odd parity, one wait-state) to the ICP ASIC. The ASIC firmware reinitializes.	ICP ASIC	FAULT
72	SYS_FAIL Assert Test - Verifies that SYS_FAIL system controls assert and deassert the SYS_FAIL condition. Uses timeouts to prevent conflicts with other modules under test on the same backplane. No SYS_FAIL interrupt test. This test will fail if another module leaves STS_FAIL asserted. Only execute when in Factory Test mode.	CPU PLD, backplane, other modules	FAULT
73	Watchdog Timer Test - Verifies that the WDT does not expire when hit for 500 msec, based on Hardware Status Register and interrupt. Uses the WDT Test mode to show that the WDT will time out and generate an SMI interrupt in more than 195 msec but less than 210 msec. The interrupt routine disables WDT Test Mode to clear the interrupt. Disables WDT after test.	CPU PLD, WDT Chip, ICP ASIC, ICP Oscillator	FAULT
80-89	FTA DUART Tests	For all: CPU card DUART	
80	FTA DUART Register Access Test - Verifies that the DUART can be initialized.	CPU PLD	FAULT
81	FTA DUART Clock Compare Test -- Check the DUART clock against the CPU timebase register to make sure they are running at the same relative rates. The test is run for 2048 Duart ticks (8.8888 msec) which corresponds to 55555 CPU ticks +/- 54.	DUART Crystal	FAULT
82	FTA DUART Interrupt Test - Verifies that the DUART can generate an interrupt. The counter which had expired from the previous test is used. The interrupt is verified in the DUART ISR, then enabled through the DUART IMR and verified in the Hardware Status Register; finally exceptions are enabled to make sure that the interrupt occurs.	CPU PLD	FAULT
83	FTA DUART Channel A Transceiver and Loopback Test - verifies that data cannot be transmitted or received if either transceiver is disabled, but data can be transmitted and received when both are enabled.	Transceivers	FAULT

84	FTA DUART Channel B Transceiver and Loopback Test - verifies that data cannot be transmitted or received if either transceiver is disabled, but data can be transmitted and received when both are enabled.	Transceivers	FAULT
100-1xx	ICP Shared RAM Tests	For all: RAMs, buffers, CPU PLD, ICP ASIC	FAULT
100	ICP Shared RAM Destructive Pattern Test. Checks address and data lines by writing a non-repeating pattern over the whole memory, then verifying it. Runs with data parity enabled and fatal. Two starting patterns are used for better coverage.	Shared RAM chip, buffers, arbitration	FAULT
101	ICP Shared RAM Destructive Pattern Parity Interrupt Check - verify that 603 data parity error did not occur during previous test. Runs with data parity enabled and fatal.	Shared RAM chip, buffers, arbitration	FAULT
102	ICP Shared RAM Initialization to force correct odd parity. Verified. This must be done before writing to the ASIC control registers. Runs with data parity enabled and fatal.	Shared RAM chip, buffers, arbitration	FAULT
110-119	ICP ASIC Tests		
110	N/A		
111	ICP ASIC Register Access Test - The hardware setup parameters having been written to the ASIC some time earlier, access to the ICP ASIC registers is verified, and the error register is verified as zero. The ECHO_REV operation is used to make the ASIC write its version register to a designated location in Shared RAM. This value is saved in RAM. The rest of Shared RAM is verified to make sure that only the designated location was written.	ICP ASIC, ASIC-RAM I/F	FAULT
112	ICP ASIC Unique Address Echo Test - Correct access to the ICP shared RAM from the ASIC is verified through the Echo Test, by asking the ASIC to write each location's address at that address. This test is performed once for the address and once for the complement of the address. Coverage is not 100% because only the 17 LS address bits are supported by the ASIC.	ICP ASIC, ASIC-RAM I/F	FAULT
113	ICP Bus Lock Test - Verify that the ICP ASIC can be locked out of it Shared RAM by the 603. This is accomplished with the ASIC Echo_REV Test by: 1) locking the bus 2) telling the ASIC to write to a specified address, 3) looking at the address, 4) unlocking the bus, 5) looking at the address to see that it changed and the correct data was written.	Bus lock or arbitration circuit (CPU PLD) ICP ASIC.	FAULT
114	ICP Clock Compare Test - Check the ASIC clock against the 603 clock to make sure they are running at the same relative rates. The ICP ASIC read timer command is used to write the Internal Timer to shared RAM where it is read by the 603. The test is run for 20 msec, and +/- 0.016 msec error is allowed at this time.	603 Oscillator, ICP ASIC Oscillator	FAULT
115	ICP ASIC Interrupt Test - The ICP ASIC timer interrupt is enabled, along with the CPU external interrupt, to see if the interrupt generation and recognition works and the Hardware Status Register ICP_INT is asserted. The ASIC timer is disabled, and the CPU interrupt inhibited, after the test.	Hardware Status Register chips, ICP ASIC	FAULT
130	Personality Parity Check - A parity interrupt scan is performed of the 3MB personality area.	No personality, bad personality load	Personality is erased.
131	Personality Area Erase - If the previous test indicated a parity error, the 3MB personality area is erased and verified.	Bad flash chip	FAULT
132	Personality checksum -- If the previous test indicated no parity error, and a personality is present, the personality checksum is verified. If no errors, a key is written in RAM to indicate that the personality is valid.	Bad personality load	Personality is ignored.

255	PCM Signals end of selftest. The HEALTH LED is made GREEN. Depending on various state flags and whether RAM was flushed, selftest will exit to the Alive/Fail executive or start the personality. Displays BOOT when starting the personality and PASS when starting the Alive executive.	N/A	N/A

7.4 Corrective Actions

Related topics

7.4.1 General Corrective Actions

7.4.1.1 GEN_CA01

Call TAC for assistance.

7.4.1.2 GEN_CA02

Cycle power to the chassis.

7.4.2 Battery Extension Module (BEM) Corrective Actions

7.4.2.1 BEM_CA01

Check the BEM.

If ...	Then ...
If the BEM front panel indicator is off,	Ensure chassis power is applied and/or BEM is fully inserted into the chassis.
If that doesn't work,	Replace the BEM.

7.4.2.2 BEM_CA02

Recharge the BEM.

If ...	Then ...
If the BEM OK LED is solid red,	1. Verify that the battery-pack has been inserted into the BEM (usually done at time of installation).
	2. Otherwise, if the battery-pack is present, then its capacity is not within spec. Replace the BEM to reinstate the battery-backed protection of the CPM control strategy and perform the following steps to attempt to repair the deficient BEM.
	• Allow the BEM to recharge the battery-pack in a powered chassis for 24 hours. The battery-pack may have originally been drained after the chassis has been powered down for an extended period of time.
	• If the battery pack fails to charge after sitting in a powered chassis for 24 hours, replace the battery-pack.
	• If the BEM LED is not solid green with a new battery-pack, then the BEM circuitry and/or ICP connector is defective. Note that the battery-pack may still be salvaged by recharging (for 24 hours in a powered chassis) using another BEM.

7.4.3 ControlNet Interface (CNI) Corrective Actions

Related topics

"CNI_CA01" on page 500
"CNI_CA02" on page 500

7.4.3.1 CNI_CA01

To replace a CNI,

If ...	Then ...
the CNI resides in a "PRIMARY chassis,	• Initiate a switchover so CNI is in Secondary chassis,
	• remove SECONDARY chassis power,
	• then replace the CNI,
	• then return SECONDARY chassis power,
	• then wait for chassis to synchronize and initiate a switchover,
	• then wait for the PRIMARY CNI to successfully complete startup.
the CNI resides in a SECONDARY or Non-Redundant chassis,	• remove SECONDARY or Non-Redundant chassis power,
	• then replace the SECONDARY or Non-Redundant CNI,
	• then return SECONDARY chassis power.

7.4.3.2 CNI_CA02

To reset a CNI,

If ...	Then ...
the CNI resides in a" PRIMARY chassis,	• Initiate a switchover so CNI is in Secondary chassis,
	• cycle SECONDARY chassis power,
	• then wait for chassis to synchronize and initiate a switchover,
	• then wait for the PRIMARY CNI to successfully complete startup.
the CNI resides in a SECONDARY or Non-Redundant chassis,	Cycle SECONDARY or Non-Redundant chassis power.

7.4.4 C200/C200E Control Processor Module (CPM) Corrective Actions

Related topics

7.4.4.1 CPM_CA01

Check the CPM.

If ...	Then ...
If all the CPM front panel indicators are off,	Ensure chassis power is applied and/or CPM is fully inserted into the chassis.
If that doesn't work,	Replace the CPM "CPM_CA06" on page 502.

7.4.4.2 CPM_CA02

Load the CPM firmware.

If ...	Then ...
If the CPM is in the Alive or Ready State,	Use the NetworkTools utility to load the CPM Boot and/or Application personality firmware.
If the CPM is in the Loading State,	Await CPM Application or Boot personality-download completion. Otherwise, if the current firmware download session terminated abnormally:
	• Ensure downloading the correct personality for the module type.
	• Attempt to reload the CPM personality firmware using the NetworkTools utility.

If ...	Then ...
	• If repeated attempts to load CPM personality firmware are unsuccessful, replace the CPM "CPM_CA06" on page 502.

7.4.4.3 CPM_CA03

Isolate reason for loss-of-synchronization.

If ...	Then ...
If RM COM LED is off,	Ensure redundancy cable is present and attached to both the primary and secondary RM.

7.4.4.4 CPM_CA04

Recover from CPM Fail State.

1 Acquire the CPM crash block using either the NetworkTools or the CPMTools utility. This information is necessary for the generation of an effective defect report. See "Effective Trouble Reporting" on page 607.

2 Interpret the "C200/C200E CPM Fault Codes" on page 70 and perform any additional corrective action specific to the individual CPM Fault Code extracted from the crash block in step #1 or the CPM Alphanumeric Display.

3 Issue the Recover command to the CPM in the Fail State using either the NetworkTools or CPMTools utilities. If the CPM does not reboot into the Alive or Ready States either {1} interpret the new "C200/C200E CPM Fault Codes" on page 70 or {2} replace the CPM "CPM_CA06" on page 502, if the same Fault Code persists.

4 Once the CPM transitions into the Ready State issue the Start command using either the NetworkTools or CPMTools utilities. If the CPM does not reboot into the NotLoaded or Backup States either {1} interpret the new "C200/C200E CPM Fault Codes" on page 70 or {2} replace the CPM "CPM_CA06" on page 502, if the same Fault Code persists.

5 If the CPM is in the Alive State, load the CPM Boot and/or Application personality firmware using the NetworkTools utility.

7.4.4.5 CPM_CA05

Restart the CPM.

If ...	Then ...
If the CPM is in the secondary chassis,	Power-cycle the secondary chassis.
If the CPM is operating, be sure process is in a safe state and CPM is in Idle mode.	Power-cycle the primary/non-redundant chassis.

If restarting the CPM does not resolve the problem replace the CPM "CPM_CA06" on page 502.

7.4.4.6 CPM_CA06

Replace the CPM.

If ...	Then ...
If the CPM is still operating, be sure process is in a safe state and CPM is in Idle mode.	Perform CPM replacement with chassis power removed.

7.4.4.7 CPM_CA07

Replace defective battery or correct invalid battery configuration. There are two types of batteries used for CPM memory retention:

- The lithium battery in the front of the CPM
- The Ni-Cad Battery Extention Module (BEM) residing in the chassis.

If ...	Then ...
If no batteries are present,	Equip the CPM with one type of battery.
If only one battery is present,	Replace the battery because it is drained and/or damaged.
If two batteries of proper voltage are present,	Remove one of the batteries. Note that having two batteries (of proper voltage) present is a minor fault condition.

7.4.4.8 CPM_CA08

Check the RM resident in the CPM chassis.

If ...	Then ...
If the RM faulted,	Interpret the RM fault code.
Otherwise, if the RM appears healthy,	power-cycle the secondary chassis or initiate a switchover first depending on whether the RM is in the secondary or primary redundancy role respectively.
If that doesn't work,	Restart the CPM "CPM_CA05" on page 502.

7.4.4.9 CPM_CA09

Activate the CPM control strategy using Control Builder or the appropriate SCAN display.

7.4.4.10 CPM_CA10

If necessary, create/modify control strategy using Control Builder. Load new/existing control strategy using the Control Builder.

7.4.4.11 CPM_CA11

Reload the CEE FB manually.

7.4.4.12 CPM_CA12

Interpret the *CPM Test Sequence Number* displayed on the Alphanumeric Display.

7.4.4.13 CPM_CA13

Recover from CPM Watchdog Timer timeout. The following recovery procedure assumes the CPM is the only control agent within the chassis. If this is not the case and the CPM must be immediately recovered (i.e. without gathering defect information), simply *restart the CPM*

1 Ensure a battery is present and power-cycle the CPM.
2 The CPM reboots into the Fail State displaying FAIL 0014.
3 Acquire the CPM crash block using either the NetworkTools or the CPMTools utility.

4 Issue the Recover command to the Failed CPM using either the NetworkTools or CPMTools utilities.

5 The CPM reboots into the Ready State.

6 Issue the Start command to the Ready CPM using either the NetworkTools or CPMTools utilities.

7 The CPM reboots into the NotLoaded or Backup State.

8 Replace the CPM if the Watchdog Timer timeout condition reoccurs.

7.4.4.14 CPM_CA14

Isolate cause of ControlNet communication fault.

1 Search the Experion SCAN Alarm Summary display for any revealing indications as to which communication module and/or cable are in distress.

2 Repair CNI slot x (where x is the slot number embedded in the Experion Notification text descriptor) communication fault between primary and secondary chassis.

7.4.4.15 CPM_CA15

Attempt switchover to better primary CPM. The goal of the following procedure is to remove the marginally defective CPM hardware that is currently executing in the primary redundancy role without loss of control. If unable to achieve synchronization, the primary CPM must be replaced, CPM_CA06; however, if the user is comfortable controlling without redundancy for the time being, primary CPM replacement can wait until a more convenient time.

1 Initiate initial synchronization using the Control Builder RM configuration form or the appropriate SCAN display.

2 When initial synchronization is complete, issue the Initiate Switchover command to change redundancy roles.

3 Power down the secondary chassis and replace the marginally defective (original primary) CPM.

7.4.4.16 CPM_CA16

Check Boot FW revision.

1 Using either the NetworkTools or the CPMTools utility verify that the proper Boot firmware is loaded to the CPM.

2 Reload the CPM Boot firmware using the NetworkTools utility if an older Boot firmware exists.

7.4.4.17 CPM_CA17

Isolate communication fault with secondary CPM. Primary CPM aborted initial synchronization or synchronization maintenance due to communication error with the secondary CPM (across the RM redundancy cable).

1 If the secondary CPM is missing and/or faulted

2 Otherwise, if secondary CPM is present and appears healthy, power cycle the secondary chassis, and verify auto-synchronization commences if configured to do so.

7.4.4.18 CPM_CA18

Recover from secondary I/O CNI ControlNet communication fault.

1 If a secondary CNI is faulted, power-cycle the secondary chassis.

2 If a primary CNI is faulted, initiate switchover, if possible, and power cycle secondary chassis or put CPM in Idle mode and power cycle primary chassis.

7.4.4.19 CPM_CA19

Check CPM Application firmware compatibility. See the "Using the Detail Pane in NTools" on page 532 to retrieve current CPM firmware level. Use NTools to upgrade the firmware, if required.

7.4.4.20 CPM_CA20

Check CPM hardware compatibility. See the "Using the Detail Pane in NTools" on page 532 to retrieve current CPM hardware version information. Replace CPM, if required.

7.4.4.21 CPM_CA21

Disconnect the backup battery and restart the CPM.

If …	Then …
If the CPM is in the secondary chassis,	Power-cycle the secondary chassis.
If the CPM is operating, be sure process is in a safe state and CPM is in Idle mode.	Power-cycle the primary/non-redundant chassis.

Re-connect the backup battery.

If restarting the CPM does not resolve the problem, replace the CPM "CPM_CA06" on page 502.

7.4.5 Series A Chassis I/O Module Corrective Actions

Related topics

"IO_CA01" on page 505
"IO_CA02" on page 505

7.4.5.1 IO_CA01

With chassis power removed, replace the I/O module.

7.4.5.2 IO_CA02

With process in safe operating mode, cycle I/O chassis power.

7.4.6 C200/C200E Rack and Supply Corrective Action

Related topics

"CH_CA01" on page 505
"CH_CA02" on page 506

7.4.6.1 CH_CA01

To replace a chassis power supply.

If …	Then …
the supply resides in a" PRIMARY chassis,	• take the controller 'Off Control', • then remove SECONDARY chassis power, • then a few seconds later remove PRIMARY chassis power, • then replace the PRIMARY supply, • then repower the PRIMARY and wait for startup to successfully complete, • then return SECONDARY chassis power.
the supply resides in a SECONDARY chassis,	• remove SECONDARY chassis power, • then replace the SECONDARY supply, • then return SECONDARY chassis power.
the supply resides in a non-redundant controller or in an I/O rack,	• take the controller 'Off Control', • remove chassis power, • then replace the supply, • then return chassis power.

7.4.6.2 CH_CA02

To replace the chassis backplane,

If …	Then …
the backplane resides in a "PRIMARY chassis,	• take the controller 'Off Control', • then remove SECONDARY chassis power, • then a few seconds later remove PRIMARY chassis power, • then replace the PRIMARY backplane, • then repower the PRIMARY and wait for startup to successfully complete, • then return SECONDARY chassis power.
the backplane resides in a SECONDARY chassis,	• remove SECONDARY chassis power, • then replace the SECONDARY backplane, • then return SECONDARY chassis power.
The backplane resides in a non-redundant controller or in an I/O rack,	• take the controller 'Off Control', • remove chassis power, • then replace the backplane, • then return chassis power.

7.4.7 C200/C200E Redundancy Module (RM) Corrective Action

Related topics

7.4.7.1 RM_CA01

To replace an RM,

If ...	Then ...
The RM resides in a" PRIMARY chassis	1. Take the controller 'Off Control'. 2. Remove SECONDARY chassis power. 3. Then a few seconds later remove PRIMARY chassis power. 4. Then replace the PRIMARY RM. 5. Then return PRIMARY chassis power. 6. Then wait for the PRIMARY to successfully complete startup. 7. Then return SECONDARY chassis power.
The RM resides in a SECONDARY	1. Remove SECONDARY chassis power. 2. Then replace the SECONDARY RM. 3. Then return SECONDARY chassis power.

7.4.7.2 RM_CA02

To reset an RM,

If ...	Then ...
the RM resides in a" PRIMARY chassis,	1. Take the controller 'Off Control'. 2. Remove SECONDARY chassis power. 3. Then a few seconds later, remove PRIMARY chassis power. 4. Then return PRIMARY chassis power. 5. Then wait for the PRIMARY to successfully complete startup. 6. Then return SECONDARY chassis power.
the RM resides in a SECONDARY,	Cycle SECONDARY chassis power.

7.4.7.3 RM_CA03

To check and/or replace a Redundancy Cable,

- remove SECONDARY chassis power,
- then detach the Redundancy Cable,
- then verify the ends are clean and polished to the naked eye,
- then verify the cable has no sign of kinks or breaks,
- replacing the cable if suspect,
- checking its replacement in the same manner,
- then return SECONDARY chassis power.

Note: Optical cable is sensitive to mishandling, particularly with regard to a tight bend radius.

8 ControlNet Configurations

Related topics

8.1 ControlNet Addressing

You set the MAC ID (ControlNet address) switches on the partner CNI modules in an RCP to the same ID (address). The software automatically assigns the switch set address to the Primary Controller and increments the set address by one for the Secondary Controller. For example, if you set the switches on the partner CNI modules to 1 for the Supervisory ControlNet, the address of the Primary Controller is always 1 and the address for the Secondary Controller is always 2. You must always allocate two consecutive addresses for partner CNI modules in an RCP.
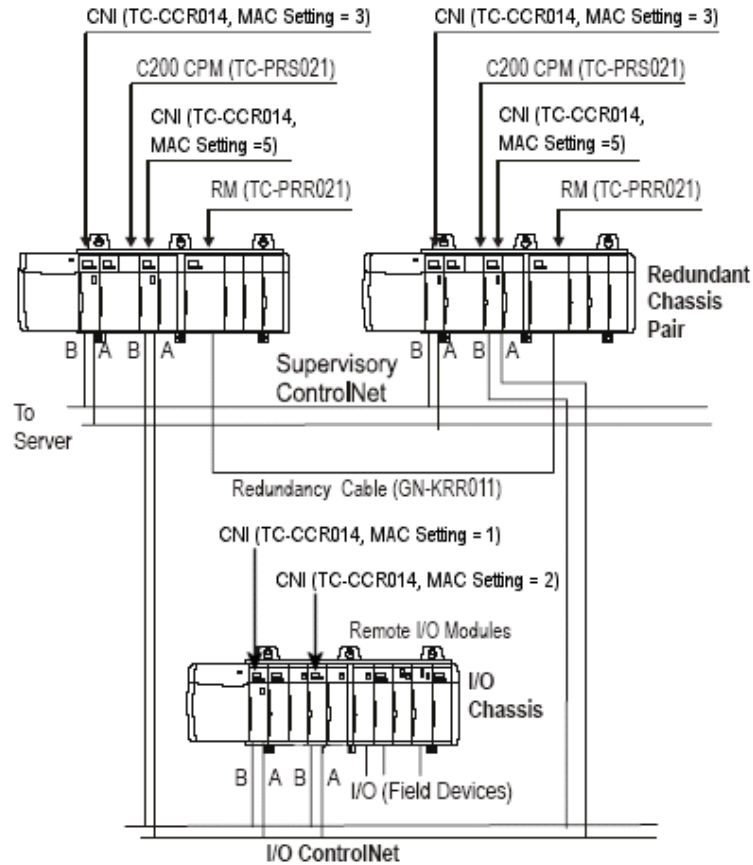
8.2 Redundant C200/C200E ControlNet requirements

Related topics

8.2.1 Conjoined ControlNets with C200/C200E0 redundancy requirements

You must comply with the following system configuration rule, when your Experion system supports C200/C200E controller redundancy.

- Any ControlNet segment that connects to an RCP must have at least two other nodes. A node can be a CNI in another chasssis, KTC, PCIC, Linking Device, Series A/H Gateway, etc.

The following sample system configurations show how you can adapt a given small system architecture to meet minimum redundant controller system requirements.

- If your system only consists of a non-redundant Server or redundant Servers, one RCP, and one I/O chassis, you must link the Supervisory ControlNet with the I/O ControlNet though a trunk cable to form a common ControlNet as shown in the figure below. In this case, the default addresses are as follows.

  - Default address for CNI in slot 0 is 1.
  - Default address for CNI in slot 3 is 5.
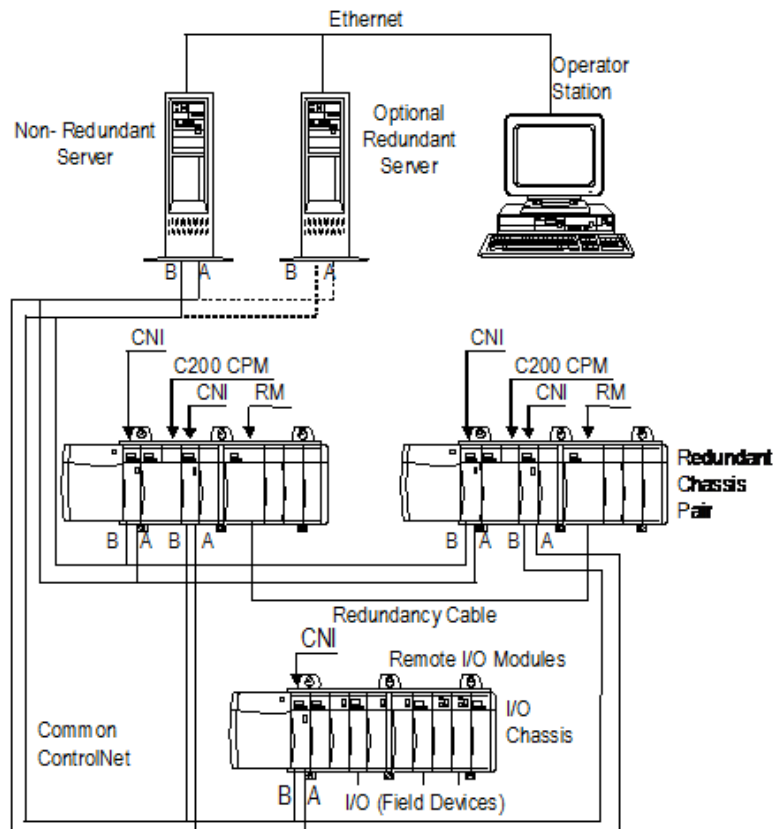 - Note that the default address for the I/O Chassis CNI in slot 0 is 3.

8.2.2 Independent ControlNets with C200/C200E redundancy requirements

You must comply with the following system configuration rule, when your Experion system supports controller redundancy.

- If your system only consists of a non-redundant Server or redundant Servers, two RCPs, and one I/O chassis per RCP, you can add another CNI in the I/O chassis to increase the nodes in the I/O ControlNet to a given RCP as shown in the figure below. In this case, the default MAC ID addresses for CNIs are as follows. (Note that addresses must be incremented accordingly in the other RCP. The default addresses are shown for example purposes only. You are free to set the addresses you want within the constraints of the ControlNet addressing rules.)

  – Default address for CNI in slot 0 is 3.
  – Default address for CNI in slot 3 is 5.
  – Note that the default address for the I/O Chassis CNI in slot 0 is 1.
  – Note that the default address for the I/O Chassis CNI in slot 4 is 2. (Note that the slot 4 location was chosen for example purposes only.)
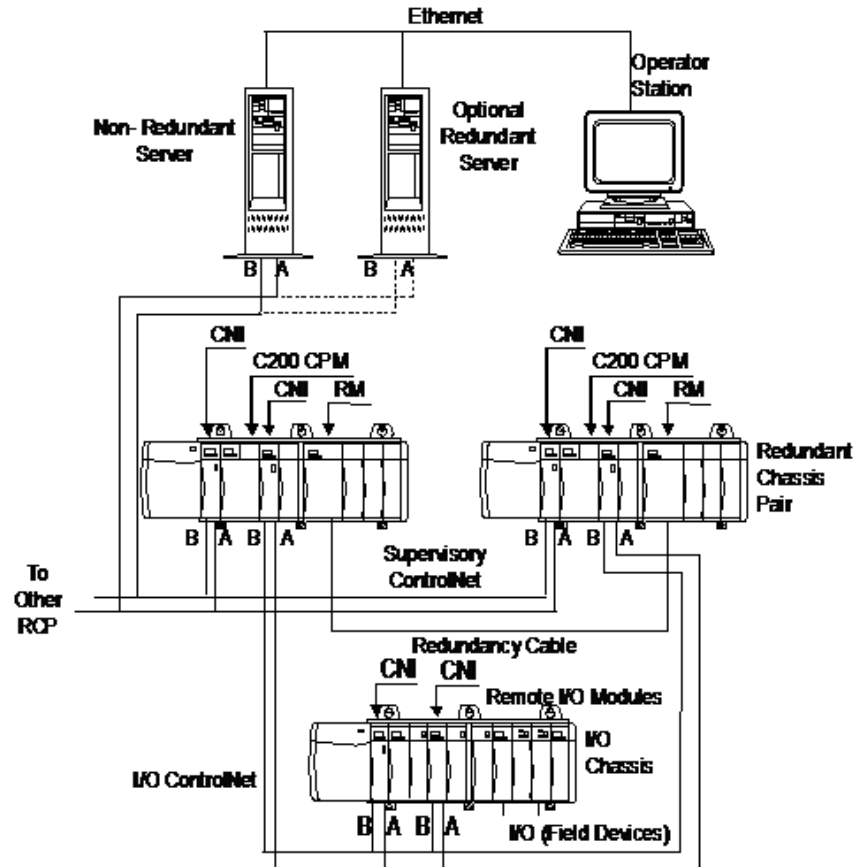
8.3 Invalid ControlNet Configuration

The figure below shows an invalid redundant controller system configuration for reference only. Do not add additional CNIs to an RCP as the means to increase the number of nodes in a ControlNet segment to a single I/O chassis. This does not meet the requirement of having at least two nodes in any ControlNet segment that connects to an RCP.
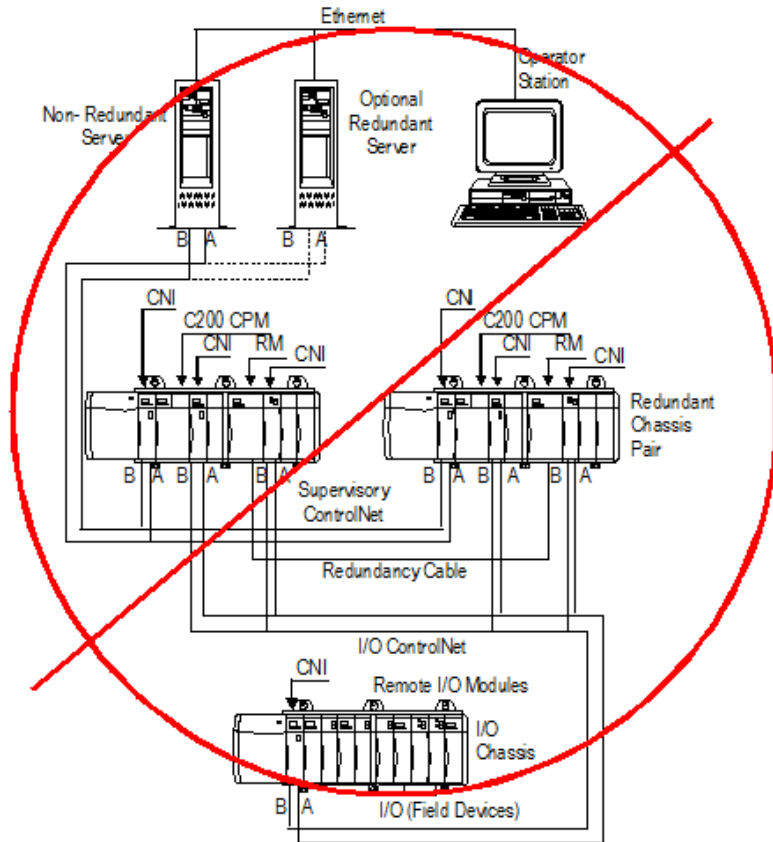
8.4 ControlNet Checklists

Related topics

8.4.1 Guidelines for assigning MAC ID/ControlNet addresses

Be sure your MAC ID assignments conform to these general guidelines.

- Valid Supervisory ControlNet address range is between 1 to 24. Note that 24 can be extended up to 32, if your system has more than 24 nodes present.
- Valid I/O ControlNet address range is between 1 to 20.
- Assign 23 as the address for the Server. This reserves address 24 for an optional redundant partner Server.

> ⚠ **CAUTION**
> When reconfiguring the Server MAC ID from 19/20 to 23/24 for the first time, you must first change the Supervisory ControlNet UMAX parameter to 24. Otherwise, a loss of view occurs.

- ControlNet address 1 is now optional (even though the documentation assumes that it is always present). The CNI node with the lowest MAC ID controls the NUT timing for the CNET segment it is in.
- When you assign the lowest MAC ID to an operating CNI in an RCP, do not assign the next higher used address above 'lowest MAC ID + 1' (in the same physical network) to another CNI in that RCP. You must assign the next higher used address above 'lowest MAC ID + 1' to a CNI in another Controller chassis, a CNI in a remote I/O chassis, or the PCIC card in the Server in the same physical network. (Note that the examples shown in Figures 2, 3, and 4 comply with this rule.)
- Only assign odd numbered addresses to accommodate the logical assignment of odd/even address pairs for RCP applications.
- Assign same odd numbered address to CNI partners in an RCP.

Refer to the *Experion Planning Guide, Supervisory ControlNet Addressing* for more address guidelines.

8.4.2 Confirming redundant C200/C200E controller system requirements

Be sure your redundant controller system architecture includes:

- At least four nodes. This means that there must be at least two other nodes in any ControlNet segment that connects to an RCP.
- Redundant-compliant C200/C200E CPMs and CNIs in RCP.
- CPMs, CNIs, and RMs located in matching slots in RCP.
- Partner CNIs in RCP have same odd numbered address.
- Partner CNIs in RCP have same ControlNet parameter settings.
- RMs connected by a redundancy cable for each RCP.
- No local I/O in any RCP.
- RCP that includes a CNI with the lowest MAC ID of the ControlNet segment does not also include a CNI with the next higher used address above 'lowest MAC ID + 1' in the same physical network.

9 Redundancy Module Displays

Experion offers RM Displays from both Control Builder and Station. The data which feeds these displays is the same. The presentations are similar. References (in tis document) to these displays apply in general to both the CB and Station versions.

The RM Displays provide not only a view to the RM's themselves, but also a means to monitor and control Redundancy within a given redundant chassis pair (RCP).

The displays offer an indication of the general Redundancy state of each chassis of an RCP along with several tabs/categories of detailed Redundancy related data and command features.

This section will discuss these displays with the emphasis on their use as diagnostic tools.

Related topics

9.1 Redundancy Terminology

These definitions are listed in order of complexity, and are given in the context of process and machine control.

Term	Definition
Device (Chassis)	A physical device connected to the trunk, and having a network address. Examples of devices are a EXPERION Server, a Experion Station, and a Controller.
	A single ICP enclosure, with backplane, power supply, communication(s) and (in most cases) controller module(s). Also referred to as a chassis.
Assigned Functions	A function or set of functions assigned to a chassis, e.g., a controller (chassis) within a bottling plant may have an Assigned Function to wash bottles.
On-Line vs. Off-Line	On-line is the state of a chassis where that chassis is performing its Assigned Functions. Off-line, conversely, is the state where the chassis is not performing its Assigned Functions. The chassis may or may not be powered while off-line.
	Off-line is the state where the chassis is not performing its Assigned Functions. On-line, conversely, is the state of a chassis where that chassis is performing its Assigned Functions. The chassis may or may not be powered while off-line.
Availability	The ability of a device to carry out its Assigned Functions based on its probability of failure. Mean Time Between Failure (MTBF) is a measure of availability.
Redundancy	The use of multiple similar devices such that if one fails, the remaining unit(s) will take over the Assigned Functions (the set of functions assigned to the device) thereby improving the device's availability (the ability of the device to carry out its Assigned Functions based on its probability of failure).
Dual Redundancy	A form of redundancy involving a pair of devices that operate with one device performing the Assigned Functions (the set of functions assigned to that device) while the other remains in some state of readiness to assume responsibility for the Assigned Functions should the first experience a failure.
RCP (supported at the chassis level only)	Redundant Chassis Pair
	A pair of chassis (single ICP enclosures with backplane, power supply, communication(s), and in most cases controller module(s)) configured for redundant operation. The RCP may or may not have 'control' as its Assigned Function (it may not have any Controllers in its Chassis Complement).
	This RCP may or may not have 'control' as its Assigned Function, i.e., it may have only communications modules in its chassis complement.
Redundancy State Primary Secondary	The state of a Redundant Chassis Pair (RCP) with regard to redundancy and specifically with regard to which chassis is handling the Assigned Functions (the set of functions assigned to that device). In a dual redundant system, such as ICP Redundancy, two basic redundancy states exist:
	• Primary - Refers to the chassis carrying out the Assigned Functions.
	• Secondary - Refers to the chassis which is in some degree of readiness to assume responsibility for the Assigned Functions.
	The ability of the secondary to carry out the Assigned Functions in the event of a Primary failure is referred to as Secondary Readiness.

Term	Definition
Secondary Readiness	The ability of the secondary of a Redundant Chassis Pair in a dual redundant system to carry out the Assigned Functions in the event of a Primary failure.
	Two states (of Secondary Readiness) are available:
	Disqualified - In this state, a Secondary can not assume the Primary state.
	Synchronized - In this state, the Secondary can assume the Primary state. In order for a Secondary to assume responsibility for the Assigned Functions (from a Primary), with minimal impact to the Assigned Functions, that Secondary must closely track the variables and states of the Primary. The process of aligning the databases of two devices is called Synchronization. Once two devices are synchronized, they must continue to track database changes, or else the Secondary will revert to a Disqualified state of readiness.
Switchover	An immediate (possibly bumpy) exchange of control.
	In a Redundant Chassis Pair (RCP), it is the act of transferring the responsibility for the Assigned Functions from a primary chassis to a synchronized or standby secondary chassis due to the occurrence of either a failure, a fault, or the 'Initiate Switchover' command.
	The resulting state of readiness, should the switchover not be due to a failure, and depending on the reason for the switchover, could be either Synchronized or Disqualified. A Switchover will take place immediately upon detection of a fault or upon reception of a Switchover command (vs. at the end of a control scan).
Chassis ID	Given a Redundant Chassis Pair, this is a need to reference an individual chassis logically (i.e., Redundancy State: Primary, Secondary) or physically (i.e., Chassis ID: Chassis A or Chassis B). Chassis A and Chassis B are used as generic references to the physical chassis, assuming that most systems will label their chassis pairs with an A/B suffix.
	Since chassis placement (upper/lower; right/left; etc.) is optional, a position-dependent reference is unsuitable.

9.2 Accessing C200/C200E RM Displays

Related topics

9.2.1 Control Builder RM Displays

In Control Builder, under the Monitor tab, double click on the icon of the target RM, e.g., 'RM0103'.

Once the dialog box appears, select the tab (pane) of interest.

Note the data from both chassis appears on one display.

9.2.2 Station RM Displays

In Station, enter the target RM identifier (e.g., 'RM0103') on the tool bar and hit F12.

Once in the display, select the display of interest using the buttons along the upper edge of the display.

Note that data from only one chassis appears. To see the partner data, hit the 'Show Secondary' or 'Show Primary' button in the lower left corner.

9.3 RM Summary (CB) or Main (Stn) Panes

The Summary display in Control Builder and the Main display in Station serve as a Redundant controller summary. In many instances, this summary is sufficient for operator interaction.

The following table illustrates the diagnostic features.

Feature	Diagnostics
(Visibility)	Is data being retrieved from the target RMs?
Redundancy State	Are states opposing (one PRIMARY, the other SECONDARY)? Are states as expected?
Secondary Readiness	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?
Module	Are modules present and placed as expected?
Compatibility	Do modules consider themselves compatible with their partners? ATTENTION: The RM always displays UNDEFINED.
% Complete	If Secondary Readiness is DISQUALIFIED, is this value 0? Otherwise, is this value approaching (or at) 100% as the modules approach (or reach) Synchronization? ATTENTION: The RM will always report 0.

9.4 RM Profiles (CB and Stn) Panes

A view to check and compare identity, revisions, and states of the RM's.

The following table illustrates the diagnostic features.

Feature	Diagnostics
(Visibility)	Is data being retrieved from the target RMs?
Redundancy State	Are states opposing (one PRIMARY, the other SECONDARY)?
	Are states as expected?
Secondary Readiness	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?
Compatibility	Are module version and revisions compatible (i.e., have the same ver./rev/ numbers?
	Are Product Types 112 and Product Codes 1?
	Do vendor codes match?
	Are Serial Numbers different?
	Are Chassis ID's opposing (one CHASSIS_A, the other CHASSIS_B)?
	ATTENTION: Mismatches may be allowed. Refer to release documentation.
General State	Are both RM's OK?
Auto-Sync Option, Auto-Sync State, Program Command Recognition	Do these 3 items match?
Error Code	Is this field blank (…)?
	If not, does the code remain after 1 minute?
Fault Bits	Are any Major fault bits set?
	ATTENTION: Minor fault bits should not hinder normal operations.

9.5 RM Configuration (CB and Stn) Panes

The following table illustrates the diagnostic features.

Feature	Diagnostics
(Visibility)	Is data being retrieved from the target RMs?
Redundancy State	Are states opposing (one PRIMARY, the other SECONDARY)?
	Are states as expected?
Secondary Readiness	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?
Chassis ID	Are Serial Numbers different?
	Are Chassis ID's opposing (one CHASSIS_A, the other CHASSIS_B)?
(Command writes)	Toggling the Chassis ID is a way to test the ability to issue a command to the RM without impacting the Redundancy State or Secondary Readiness.
	Do the Serial Number/Chassis A vs. B relationships swap as the Chassis ID is toggled?

9.6 RM Synchronization (CB) and Synch (Stn) Panes

This display offers the user the broadest set of features related to controlling and monitoring RCP Synchronization.

The following table illustrates the diagnostic features.

Feature	Diagnostics
(Visibility)	Is data being retrieved from the target RMs?
Redundancy State	Are states opposing (one PRIMARY, the other SECONDARY)?
	Are states as expected?
Secondary Readiness	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?
Auto-Synchronization State	Does this state track the Auto-Sychronization Option as it should?
	e.g.,
	IF Auto-Synchronization Option = ALWAYS,
	Then Auto-Synchronization State should be ENABLED.
	ELSE IF Auto-Synchronization Option = NEVER,
	Then Auto-Synchronization State should be DISABLED.
	ELSE Auto-Synchronization Option = CONDITION,
	Then Auto-Synchronization State can be ENABLED or DISABLED.
Module	Are modules present and placed as expected?
Compatibility	Do modules consider themselves compatible with their partners?
	ATTENTION: The RM always displays UNDEFINED.
% Complete	If Secondary Readiness is DISQUALIFIED, is this value 0?
	Otherwise, is this value approaching (or at) 100% as the modules approach (or reach) Synchronization?
	ATTENTION: The RM will always report 0.

9.7 Redundant Chassis Profiles (CB and Stn) Panes

These displays offer the user the broadest set of feature for diagnosing a problem RCP.

The objective of these displays is to pinpoint the problem slot or module. From there, the user must refer to module specific displays and documentation to further isolate the problem.

The following table illustrates the diagnostic features.

Feature	Diagnostics
(Visibility)	Is data being retrieved from the target RMs?
Redundancy State	Are states opposing (one PRIMARY, the other SECONDARY)? Are states as expected?
Secondary Readiness	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?
Module	Are modules present and placed as expected? Does every module have a partner?
General State	Are both existing modules OK?
Compatibility	Do modules consider themselves compatible with their partners? ATTENTION: The RM always displays UNDEFINED.
% Complete	If Secondary Readiness is DISQUALIFIED, is this value 0? Otherwise, is this value approaching (or at) 100% as the modules approach (or reach) Synchronization? ATTENTION: The RM will always report 0.
Secondary Readiness (module-specific)	Is this state as expected (DISQUALIFIED, SYNCHRONIZED)?

9.8 RM Display (CB) Pane

This display offers no significant diagnostic usefulness.

9.9 RM Server Parameters (CB) Pane

This display offers no significant diagnostic usefulness.

10 Tools and Utilities

Related topics

10.1 NetworkTools (NTools) for Chassis Based Components (C200/C200E)

NetworkTools (Ntools) automatically starts up by scanning all nodes on the ControlNet, Ethernet, or Fault Tolerant Ethernet (FTE) supervisory network segment connected to your computer. Information is presented in three panes - the Tree pane (on the upper left), the List pane (on the upper right) and, below them, the Detail pane. The List pane shows ControlNet message error counters maintained by NetworkTools. Consult the Help file for NetworkTools (from the application's menu bar or hit F1) for on-line Help.

> **CAUTION**
>
> **Honeywell makes the following recommendations:**
>
> • Do not set NetworkTools to run continuously on heavily loaded systems. NTools is a utility that places a load on the communications network. Therefore, running NTools may cause some degradation to the network on systems that are already heavily loaded.
>
> • Do not open more that two instances of NTools on a system simultaneously.

If you are on control, or performing activities such as connecting nodes to the network or monitoring an analog I/O module; consider running NetworkTools with the Pause / Resume mode of operation or using Ping mode. This way you can let NetworkTools remain launched while performing such activities.

10.1.1 NTools Command Line options

NetworkTools supports several command-line options. Start NetworkTools at the command prompt with the command-line options as follows:

> **Attention**
>
> If your system includes Configuration Studio, you set the command line options pg, pit, l, nl, and u through the corresponding check box selections on the **Select options for Network Tools** dialog. On **Configuration Explorer**, click **Control Strategy** > **Set options for maintaining control system firmware** to call up the dialog.

Option	Behavior
ntools -c	Starts the NetworkTools application in the ControlNet mode. This means NetworkTools scans for MAC IDs on a supervisory ControlNet segment through the ControlNet Driver. If there is more than one ControlNet Driver installed, the NetworkTools application uses the first available driver. NetworkTools displays the MAC IDs present in the tree pane.
ntools -e	Starts the NetworkTools application in the Ethernet mode. This means NetworkTools scans for the Ethernet drivers on the supervisory Ethernet or FTE segment. Network Tools gets a list of all installed Ethernet or FTE drivers and scans them periodically.
ntools -pg	Lets you update the ControlNet parameters for selected ControlNet Interface Module (CNI)
ntools -pit	Lets you set any value of Network Update Time (NUT), when used in conjunction with the -pg command line.
ntools -l	NetworkTools executes in the **Log** mode. This mode creates an ASCII text file called **LOG.TXT** in the same directory in which NetworkTools resides *(C:\Honeywell\Experion\Engineering Tools \system\bin)*. This contains a textual record of what modules were found on the last scan.
When running with the **I** command line, the **LOG.TXT** file is written to on every scan. This may generate more hard drive activity than you want. We suggest that you only use the **I** command line when running Network Tools in the **Ping** (manual) scanning mode.	
ntools -nl	Use this command if you not want to get waning messages about Lonely CNI conditions. This is discouraged in normal practice but this warning may become a nuisance in certain commissioning situations.

Option	Behavior
ntools -u	Allows the NetworkTools application to update the firmware in the selected device. See the Update Firmware from File topic for more information. Updating device firmware should not be done on-process.

10.1.2 Launching NTools

Use the following procedure to launch the NetworkTools (NTools) utility.

> **Attention**
> If your system includes Configuration Studio, you launch Network Tools through **Configuration Explorer** by clicking **Control Strategy** > **Maintain control system firmware**. In this case, skip Step 1 and the Tip in the following procedure.

1 Click the **Start** button in the taskbar.

2 Click **Programs-** > **Experion Engineering Tools-** > **NTools** to launch the application.

> **Tip**
> By default, NTools starts in the ControlNet mode. Use the command line **-e** to launch NTools in the Ethernet mode. For example, in the taskbar, click the **Start** Button and click **Run**. In the Run dialog, key in *ntools -e -u* in the **Open** box and click the **OK** button to launch NTools in the Ethernet mode

3 Click **OK** to acknowledge the warning about monitoring through Control Builder.
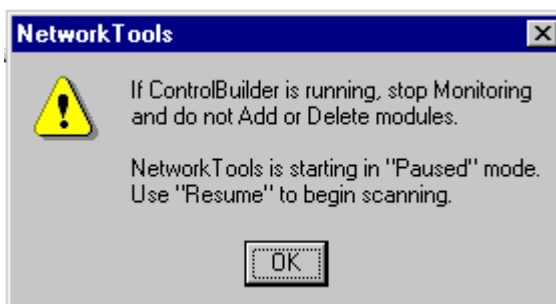
4 Click the Resume button to begin the network scan.

5 If this is the initial launch of NTools, click the **Settings** button to open the **Settings** dialog. Select the desired scanning options. The defaults are:
   - 2 second delay between scans
   - Periodic (automatic) - selected
   - Enable mode version/revision checking - checked
   - Enable ControlNet Parameter checking - checked

   Click the **OK** button to close the dialog.

6 For the initial NTools launch, you must specify some details about your particular network configuration. Click the first CNI/ENET/FTEB icon under the Desktop tree. Fill in the appropriate data in the Settings dialog for the Local and Remote chassis configurations in your network associated with the given CNI/ENET/FTEB. This only applies for the initial use of NTools. Repeat this step for the other CNI/ENET/FTEB icons.
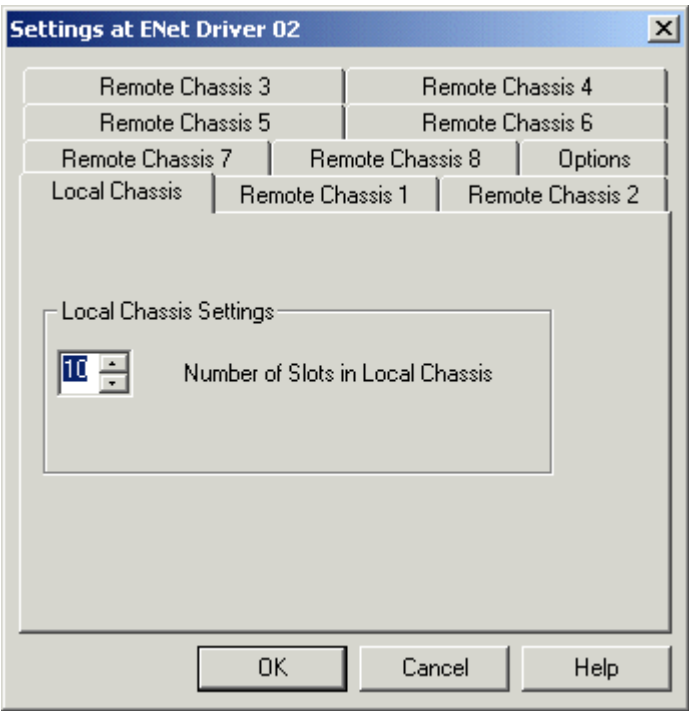
7 Once the graphic representation of the chassis appears in the Detail pane, individual modules can be selected which results in the applicable menu options becomming enabled.
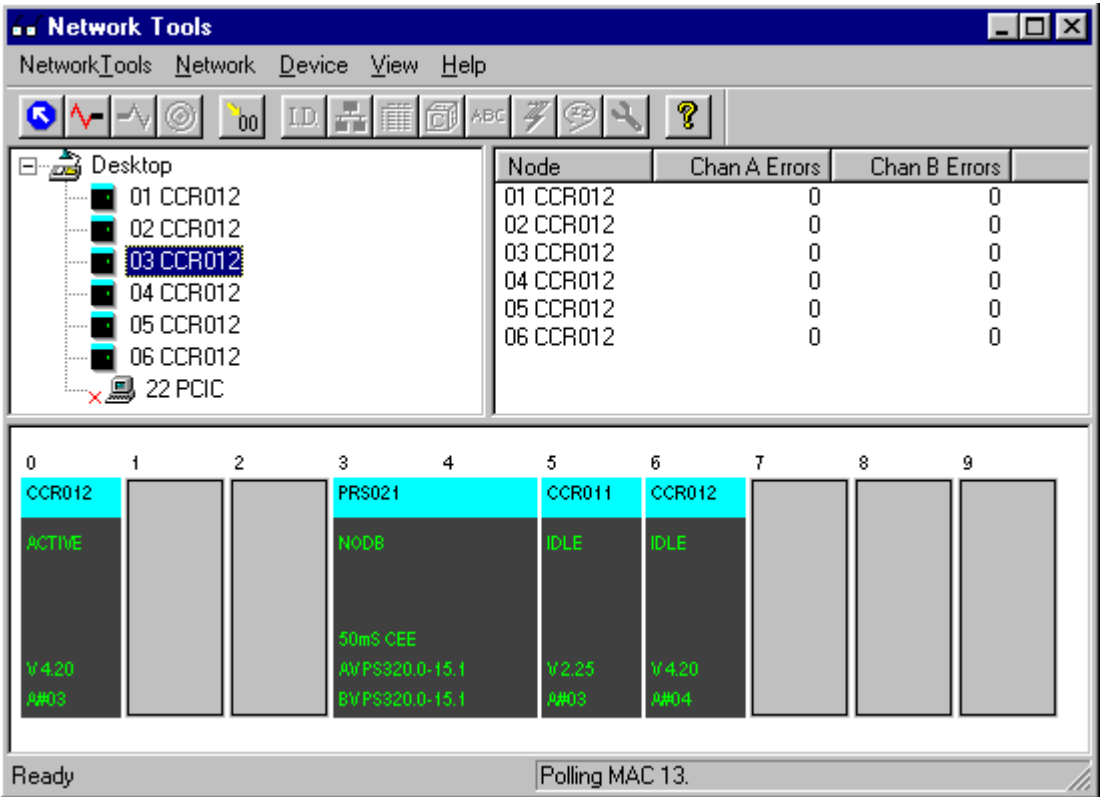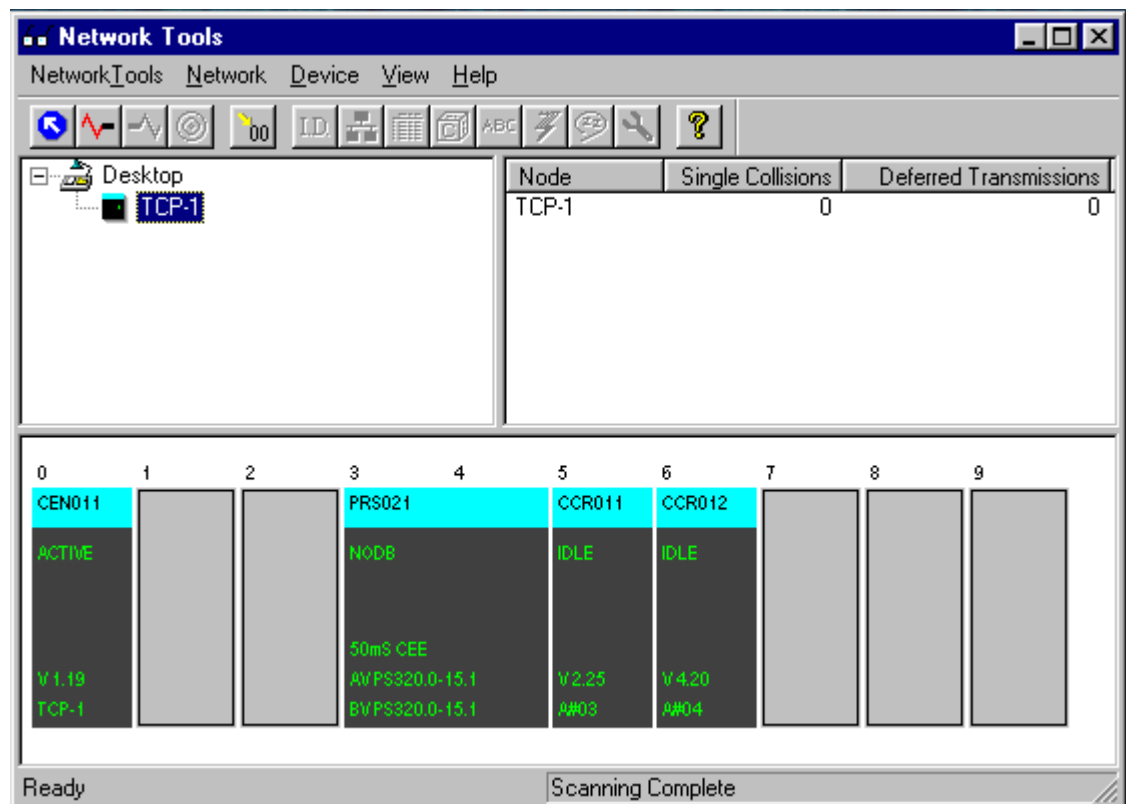
8   This completes the procedure.

10.1.3 Message Meter

When NTools is set to run continuously it scans the control network repeatedly. A popup Message Meter window appears, as shown in the following figure, to remind you that NetworkTools is running.

10.1.4 NTools Display Regions (panes)

By default, NetworkTools starts in the paused mode. Just click **NetworkTools-** > **Resume** to have NTools automatically start scanning all nodes on the Supervisory network segment connected to your computer. Information is presented in three panes - the Tree pane (on the upper left), the List pane (on the upper right) and, below them, the Detail pane. The List pane shows ControlNet/Ethernet/FTE related statistics maintained by NetworkTools.

10.1.5 Using the Detail Pane in NTools

Select one item (either the MAC ID of a CNI or the driver name for an Ethernet module or FTE Bridge module) from the Tree pane to populate the Detail pane with a C200/C200E Controller chassis and any associated remote chassis. You may be asked to provide the details on the Controller (Local) chassis. If so, fill in the details requested by the **Settings** dialog tab - use the applicable remote chassis tab, if you have any remote chassis. Note that you must provide the MAC IDs for the CNIs in any Remote chassis and you must provide chassis slot positions for DownLink CNIs in your Local (Controller) Chassis.

You can display one Local chassis and up to eight Remote chassis at a time. Use the **Settings** selection on the **NetworkTools** menu to make adjustments at any time. Your settings are saved across sessions.

NetworkTools scans per your settings and reports results in a visual manner on each module discovered. NetworkTools can be run in **Periodic** (automatic) mode or **Ping** (manual) mode. If **Periodic** mode is chosen, you can specify a number between 1 and 60 that is the time, in seconds, that NetworkTools pauses between consecutive scans. Adjust this on the **Settings** dialog. You can pause and resume Periodic scanning.

The text in the cyan boxes is the string provided in the Device Identity Object - typically, the Model number with its TC- or TK- prefix suppressed for the sake of readability.

The green text in the black box is the human-readable version of the state information acquired from the module during the scan. The Device Identity Object state is used for all modules except the CPM for which the Extended Device Object state is used.

The **V** string in the box represents the Major (version) and Minor (revision) release identifiers for the module.

The **A** and **B** text at the bottom of CNI modules indicates what ControlNet cable they were using when last scanned. The Cable Redundancy Warning is indicated by a **W** (this may appear if your system is only using a single ControlNet cable).

10.1.6 NTools Device Identity Dialog Box

To view details for a module in a chassis, click on the module's face to highlight it. Click **Device** > **Show Module Details** to open the module's **Module Details** dialog. Double clicking on the module will also launch the dialog.

10.1.7 NTools CNI ControlNet Stats Dialog Box

With a CNI module selected, click **Device** > **Show ControlNet Stats** to open **ControlNet Stats** dialog for the selected CNI. The CN Page1 tab is static data; the CN Page2 and CM0 tabs are dynamic data. When this dialog is showing, the normal scanning is suspended and the scanning for the statistics on the CN Page 2 or CM0 tab occurs every one-half second.

10.1.8 NTools ENET TCP/IP Configuration

With an Ethernet module selected, click **Device** > **TCP/IP Configuration** to open the **TCP/IP configuration** dialog for the selected ENET. This dialog is only active when NTools is started with the -**U** command line and an Ethernet module is selected. When this dialog is showing, the normal scanning is suspended and the scanning for the statistics on the second or third tab occurs every one-half second. This dialog contains the following:

IP Address	The IP Address for the Ethernet module
Subnet Mask	The Subnet Mask for the IP Address of the Ethernet module
Gateway Address	The Gateway Address for the Ethernet module
BOOTP Enable/ Disable flag	On Checking this check box, the BOOTP flag in the module is enabled and on unchecking this, it is disabled.

	If the BOOTP flag is enabled, the module expects a BOOTP server on the Ethernet segment to provide it an IP Address, a Subnet Mask and a Gateway Address after the next power up. The module remains with all these three settings with all 0s until a BOOTP Server replies to the module and successfully gives it an IP Address, Subnet Mask and Gateway Address.
	If the BOOTP flag is disabled, the module remembers its configuration and uses it on next powerup. However, the module also remembers the slot number and chassis where it was configured. Thus, it is currently not possible to set an IP Address in a slot and then shift the module to another slot. In this case, the module enables BOOTP and all other settings are initialized with 0s.

A screenshot of this dialog is shown:
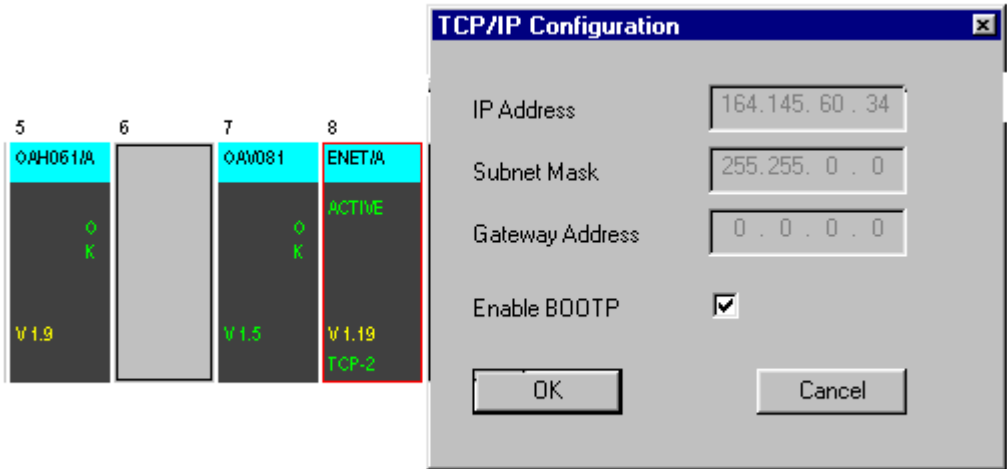
10.1.9 NTools Reset Error Counter Dialog Box

Click **Network** > **Reset Error Counters** to reset Channel A and B error counters (maintained by NetworkTools) for individual nodes on the Supervisory ControlNet segment.

10.1.10 NTools Status Bar

The progress of a scan is reflected in message on the right side of the status bar.

10.1.11 NTools ControlNet Parameters

This section discusses the Keeper Values dialog box and its operation. This powerful feature should only be used by those with a thorough understanding of the operation of ControlNet. This function can only be used if you launched NetworkTools with the **-pg** command line.

The **Change ControlNet Parameters** command is on the **Device** menu because you must select a keeper capable module for NetworkTools to effect the network changes operation. The CNI modules have the Keeper Object that orchestrates the distribution of new network parameters to all segment nodes.

Depending on which keeper capable module is selected, all modules on the corresponding ControlNet segment can be updated (i.e. the Supervisory network or subsidiary I/O networks).

You can view the current ControlNet parameters by double-clicking on any CNI in the network and reviewing the data on the **CN Page1** tab of the **ControlNet Stats** dialog.

With any CNI selected, click **Device** > **Change ControlNet Parameters** to open the **Keeper Values** dialog. You can view the ControlNet parameters that are stored in the Keeper Object on the **Present Keeper** tab. These parameters may not represent the parameters in current use in the network, but would be impressed on the network, if this CNI became the Keeper node and found that the network needed to have ControlNet parameters impressed upon it.

The parameters on the **Future Keeper** tab of the **Keeper Values** dialog for any specific CNI are just a calculation based on the values shown in the **Changes** tab of **the Keeper Values** dialog. These will be the parameters stored in this CNI's Keeper Object when you click the OK button. This is an operation that takes about 10 seconds - at the end you are told of the success and shown the Unique ID value that was impressed on the CNI - See the following section for more information.

10.1.12 NTools ControlNet Unique ID

The Unique ID shown on the **Present Keeper** tab of the **Keeper Values** dialog is important for redundant chassis operation. It is strongly recommended that all CNIs at a site be programmed for the same ControlNet parameters. Each time a CNI is programmed for ControlNet parameters a 'shorthand' code is calculated - the Unique ID - and it too is stored to the CNI. The Experion default values are as follows:

	Supervisory Network	I/O Network
NUT	10000	10000
SMAX	1	1
UMAX	24[1]	20
Repeaters	0	0
Cable Length	1000	1000
Channel Usage	A+B	A+B
Fiber Optics	No	No
Unique ID	0xa0b3b298	0x4687418c

[1]If your system requires more than 24 nodes, you can increase the UMAX to equal the number of nodes above 24 up to a maximum of 32.

If your site needs to be different than the values above (e.g. you use fiber optics) then a different Unique ID will result. Again, we strongly recommend that all CNIs at a site be programmed for the same ControlNet parameters.

If CNIs show '!CPT' in their four character display, it could be because of a Unique ID mis-match. To recover, update the ControlNet parameter settings for the secondary CNI and then power-cycle the secondary chassis, so that the CNIs reattempt their partner compatibility checks.

Flash Upgrades to CNI firmware do not affect the previously-stored ControlNet parameter settings.

10.1.13 Capturing chassis information using NetworkTools

You can use the NTools Capture Chassis Information application to collect information that will be helpful in diagnosing problems in chassis resident components like C200/C200E Controller, Fieldbus Interface Module (FIM), Fault Tolerant Ethernet Bridge module (FTEB), and I/O Link Interface Module (IOLIM).

Use the following procedure to initiate the capture of chassis information in the open NTools window.

1   Click the CNI, Ethernet, or FTEB icon under the Desktop tree for the chassis that contains the component you need to gather information about.

2   In the Detail pane, click the graphic representation of the component of interest in the chassis to select it.

3   On the **Device** menu, click **Capture Chassis Information** to launch the application.

    a   Wait for the **File Save** dialog to appear. This may take from 1 to 2 minutes, depending on chassis size and mix of components in the chassis.

    b   In the **File Save** dialog, navigate to desired file storage location or accept the default and type the desired name for the captured file with a **.ccf** extension.

    c   Click the **Save** button to initiate the chassis information capture.

4   For redundant chassis pair, repeat the previous Steps for each chassis.

5   On the **Networktools** menu, click **Exit** to close the application.

6   Forward the captured file to Honeywell's Technical Assistance Center (TAC) for analysis.

10.1.14 Viewing SIM statistics in NetworkTools

Use the following procedure to view SIM statistics in the open NTools window.

1   Click the CNI icon under the Desktop tree for the chassis that contains a SIM.

2   In the Detail pane, click the graphic representation of the SIM in the chassis to select it.

3   Click **Device-** > **Show SIM Details** to call up the dialog box. Click the Pause 〰 button to stop the network scan, if desired.

4   View the following statistics to determine if the rate of writes needs tuning.

    •   Updates/sec: Shows the number of arrays transferred from the FTA to the SIM per second. Divide this number by the number of arrays to find the per array update rate.

    •   Stores/sec: Shows the number of individual parameter writes per second.

    •   Overruns/sec: Shows the number of parameter writes that were not accepted per second. A non-zero value is signaled as an overrun.

5   Click **OK** to close the dialog box.

6   Click **NetworkTools-** > **Exit** to close the application.

10.1.15 Getting RM Events in NetworkTools

With a Redundancy Module (RM) selected, click **Device** > **Show History** to open **Redundancy Module Events History** dialog.
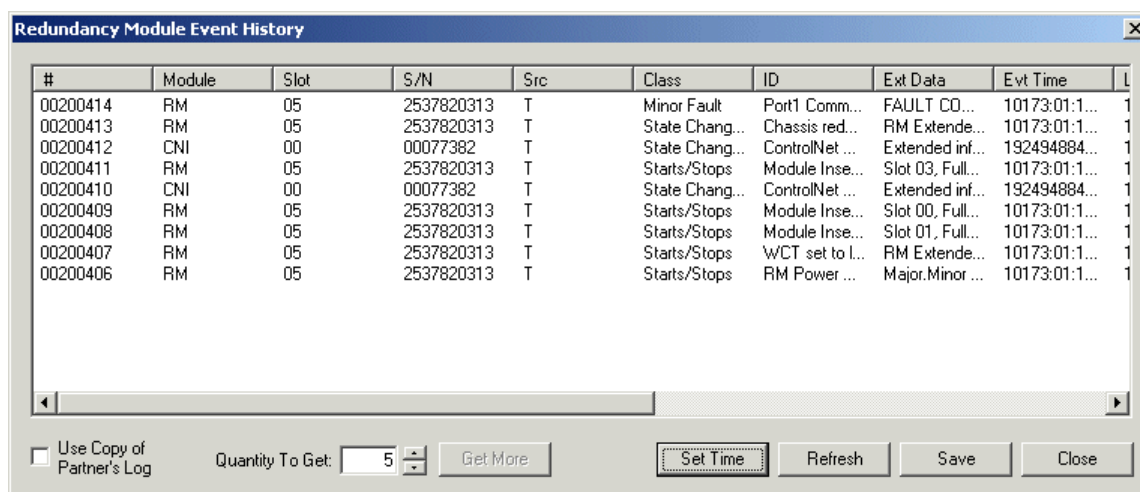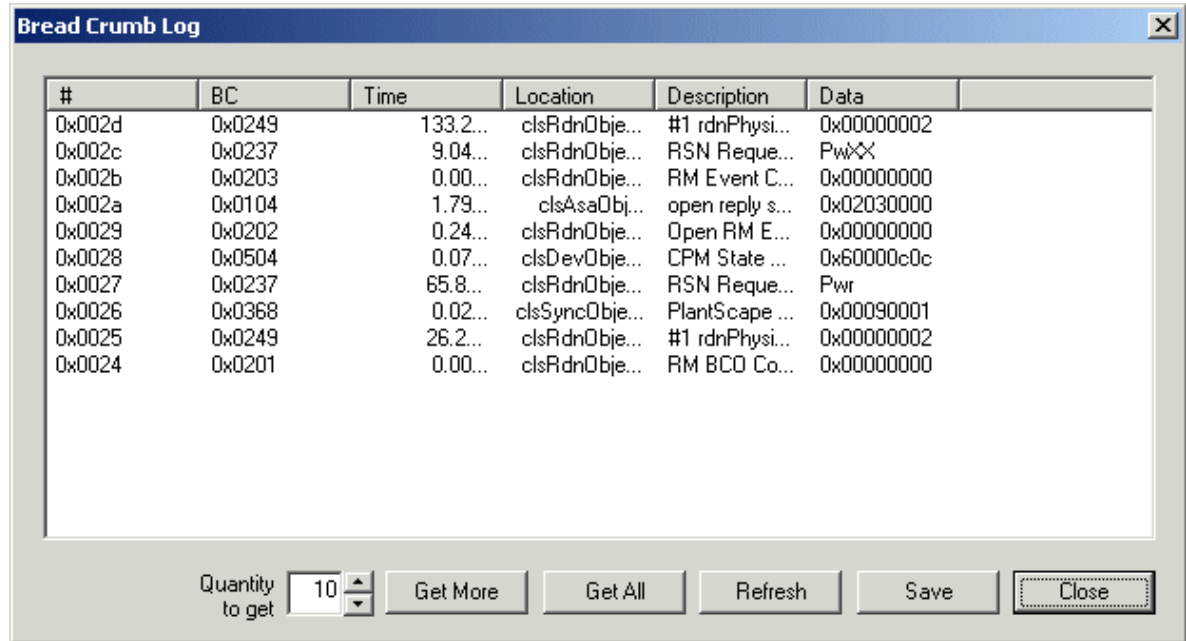

Use this dialog to display the RM's Event Log and set the social time of the RM. You cannot destroy the events - only view them. Use the **Refresh** button to re-fetch the most recent events (this is useful if you think some new events have occurred since you launched the dialog). The **Set Time** affects only the RM and not the other modules in the controller chassis.

RMs contain their own Event Log and a small copy of their partner's Log. Use the **Use Copy of Partner's Log** check box to select which you want. In the Src column the letter **T** means this selected RM and the letter **O** means the other RM (the partner) is the source for the displayed events.

10.1.16 Getting CPM Breadcrumbs in NetworkTools

With CPM selected. Click **Device** > **Show History** to open the **Bread Crumb Log** dialog.

Use this dialog to display the C200/C200E CPM's Bread Crumbs. You cannot destroy the Bread Crumbs - only view them.

> **Attention**
>
> The retreival of Bread Crumbs occurs at a priority higher than control execution - this may adversely affect the control mission.

Use the **Refresh** button to re-fetch the most recent Bread Crumbs (this is useful if you think some new Bread Crumbs have occurred since you launched the dialog).

10.1.17 Firmware Upgrades using NetworkTools

Updating device firmware should **not** be done on-process. The **Update Firmware from file** command can only be used if you launched NetworkTools with the -**u** command line or have selected the **Enable updating device firmware** check box on the **Select options for Network Tools** dialog.

> **Attention**
>
> The firmware development of the C200 Controller (including function blocks) and the Serial Interface Module (SIM) I/O is capped at R311. Therefore, you must use the R311.2 firmware versions of the C200 Controller and the SIM I/O in R400.

> **Tip**
> - You may be able to use the On-Process Migration function to update your firmware. See the *On-Process Migration Planning Guide* for more information
> - See the *Control Hardware and I/O Module Upgrade Guide* for its discussion of this topic.
> - Remove from the chassis all modules except the one to be upgraded. While this is not necessary, it removes distractions and any module interaction that could cause failure of the upgrade.
> - Read the dialog boxes that appear very carefully. If a dialog box appears which is titled 'Warning: Use Extreme Care' be very certain before you click OK. If the text in that dialog says 'The NVS file you have chosen does not contain a reference to the module you selected' you may have selected an inappropriate image to Flash to the target module.

CNI:	Click the CNI in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**.
C200/ C200E:	Click the CPM in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**. If you asked to change the state of the CPM, select OK but realize that this causes the CPM to re-boot. If you proceed too quickly to the actual Flashing operation (firmware upgrade), the operation will fail (but in a graceful, recoverable way). Be sure you wait until the CPM has fully rebooted before proceeding with a firmware upgrade.
	In some situations the Flashing operation starts but goes on and on until a failure is finally declared. This is a graceful, recoverable failure. But it if happens more than once, you are advised to shut down the CDA service and try again. (If you do this, remember to restart the CDA service).
	Note: You can find the C200E file in the path …/system/firmware/Controllers/C200E/<release> directory.
ENET:	Click the ENET in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**.
FTEB	Click the FTEB in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**.
I/O:	Click the applicable I/O Module in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**. Be sure you select the correct firmware for the selected I/O Module model.
PCIC:	Click the PCIC icon in the Tree Pane and click **Device** > **Update Firmware from file**. We suggest that you shut down the CDA Service before starting this operation.
RM:	Click the applicable RM in the chassis shown in the Detail Pane and click **Device** > **Update Firmware from file**. You cannot upgrade a RM that is showing E054 or some other failure code on its 4-character display.

10.2 Series A Chassis and Rail I/O Maintenance Tool

The Series A Chassis and Rail I/O Maintenance Tool allows the user to {1} navigate to a single I/O Module and display Module Information and Status, {2} perform calibration for various Analog Modules, and {3} reset Short/Overload Faults on Diagnostic Output Modules. These operations are separated into 3 tabs on the main I/O Maintenance Tool display: Navigator, Calibration, and Utilities respectively. The Calibration and Utilities tabs are not accessible until the user specifies the appropriate target I/O Module type on the Navigator tab. The terms Rack I/O and Chassis I/O are used interchangeably in this document.

> ❗ **Attention**
> If your system includes Configuration Studio, you launch the I/O Maintenance Tool through **Configuration Explorer** by clicking **Control Strategy** > **Maintain I/O modules**.

10.2.1 Series A Chassis and Rail I/O Maintenance Tool Navigator Tab

The Navigator Tab is used to specify the location of the I/O Module that requires maintenance. The target I/O module can be either a Rack or Rail mount module, and the destination Rack/Rail can reside on either a Local or Remote network.

Select Driver	Used to select an appropriate driver to communicate with the target I/O Module. The IO Maintenance Tool supports the maintenance of IO Modules via both Ethernet and ControlNet networks. With the possibility of having multiple RSLinx drivers, the user must explicitly select the driver needed to communicate with the target I/O module. At startup, the IO Maintenance Tool populates this combo box with a list of configured RSLinx drivers. Please note that RSLinx drivers must be configured before using the IO Maintenance Tool.
Enable Remote	If the target I/O Module resides on a remote network (i.e. not directly connected to the PC), check this Box to expose the Remote Network fields.
Rail I/O	If selecting a Rail I/O Module, check this box to expose the Gateway and Device Information fields. Selecting this box also changes the final 'SLOT' field to 'MODULE #', because Rail I/O modules are referred to by their number position on the Rail vs. Rack I/O modules that are referenced by the slot location in the Rack.
Local Network	If the 'Enable Remote' check box is selected, the Local Network information specifies the communication hub used to reach the remote network. Otherwise, if the Enable Remote check box is not selected, the Local Network information specifies the target Rail/Rack I/O module.
	Local Network information is comprised of up to 2 fields: 'MAC ID' and 'SLOT'. The 'MAC ID' field specifies the ControlNet address directly connected to this PC. Note that this selection is not required and hence not available when an Ethernet driver has been selected.
	The 'SLOT' field specifies the Rack position of either the I/O Module (i.e. no remote network) or the communication interface module (i.e. I/O Module on remote network). Note that if the I/O Module resides on the local network and it is a Rail I/O Module (i.e. 'Enable Remote' is not selected and 'Rail I/O' is selected), the 'SLOT' field is renamed to 'MODULE #'.
Remote Network	The Remote Network entry fields are only exposed when the Enable Remote check box is selected. Remote Network information is comprised of 2 fields: {1} 'MAC ID' and {2} either 'SLOT' in the case of Rack I/O or 'MODULE #' in the case of Rail I/O. The 'MAC ID' field specifies the ControlNet address of the remote Rack/Rail. The 'SLOT' / 'MODULE #' field specifies the Rack / Rail position of the I/O Module. Note that the 'SLOT' field is only renamed to 'MODULE #' if the I/O Module is a Rail I/O Module (i.e. 'Rail I/O' is selected).

The following illustration depicts the Navigator Tab configuration for a Rack I/O Module residing on a local ControlNet network.

The following illustration depicts the Navigator Tab configuration for a Rack I/O Module residing on a local Ethernet network.
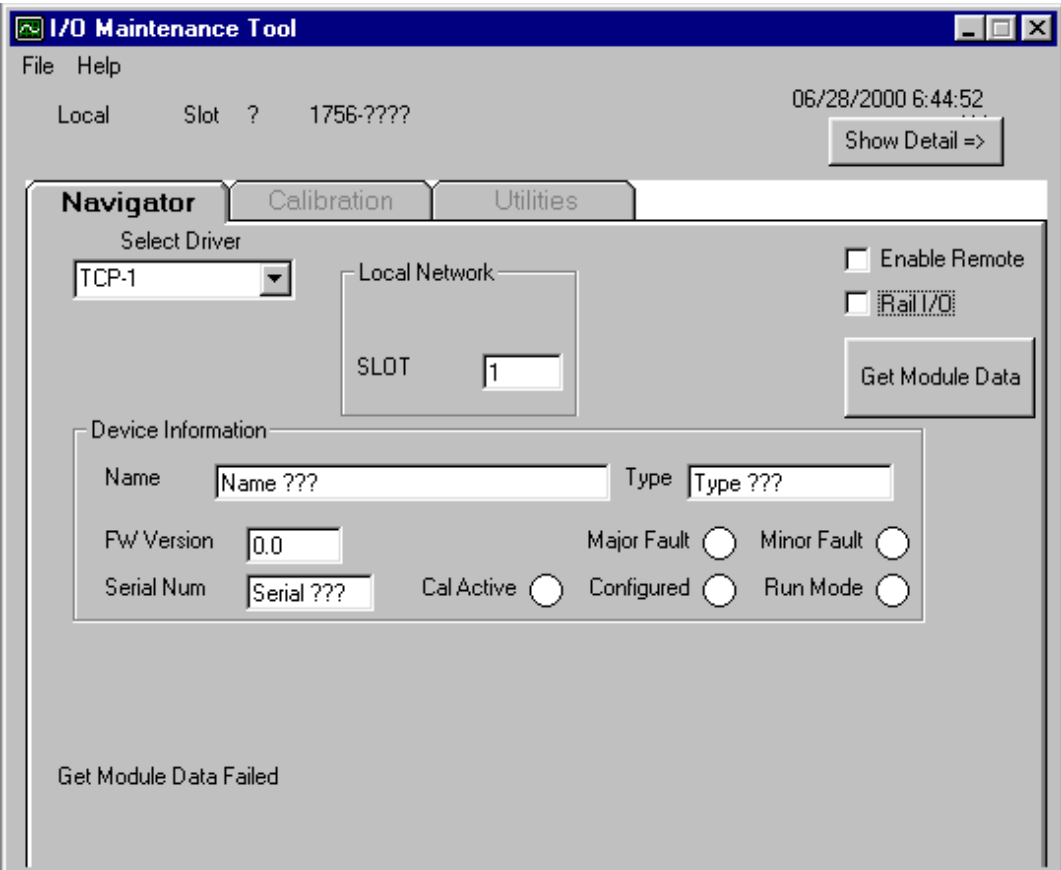
The following illustration depicts the Navigator Tab configuration for a Rail I/O Module residing on a local ControlNet network. Note that although the equivalent selections for a local Ethernet network are allowed by the I/O Maintenance Tool, this is currently a non-supported topology.
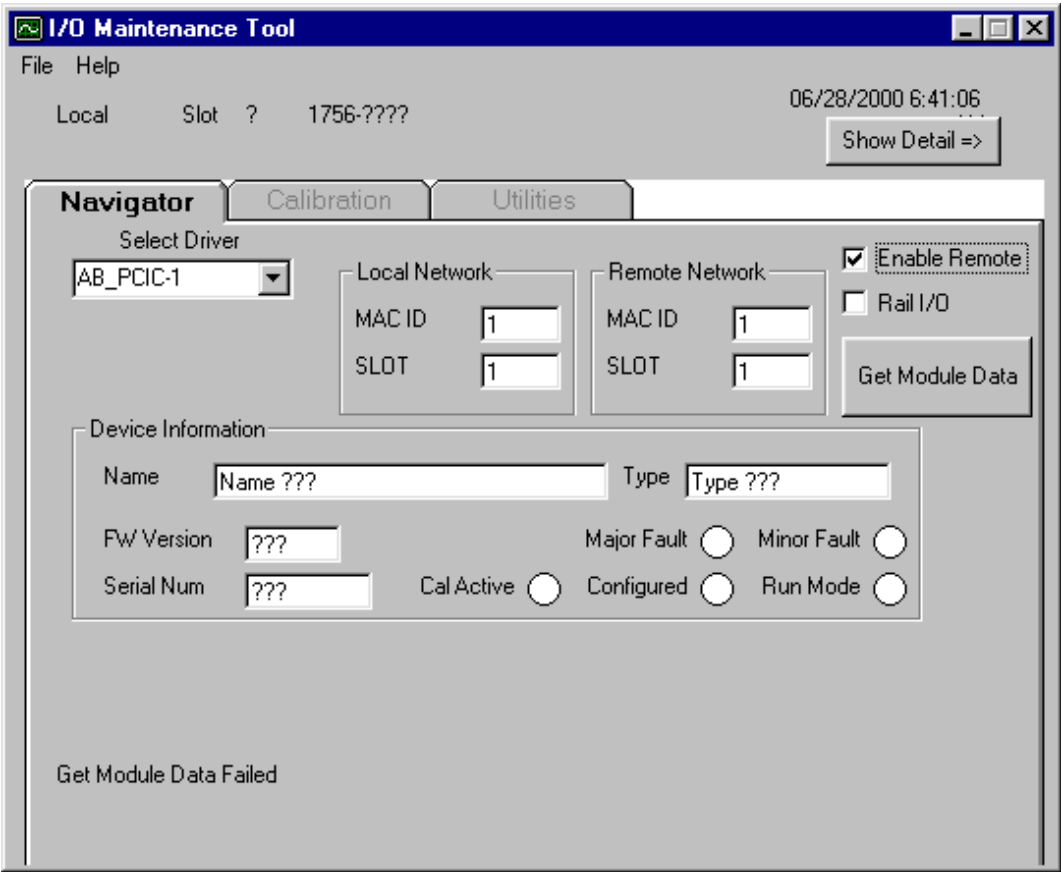
The following illustration depicts the Navigator Tab configuration for a Rack I/O Module residing on a remote ControlNet network with a Supervisory ControlNet network.

The following illustration depicts the Navigator Tab configuration for a Rail I/O Module residing on a remote ControlNet network with a Supervisory Ethernet network.

Selection of the 'GET MODULE DATA' Button causes the I/O Maintenance Tool to acquire information & status for the targeted I/O Module. For Rack I/O, the requested I/O Module information is displayed in the Device Information field. For Rail I/O, the requested I/O Module information is displayed in the ControlNet Gateway Information and Device Information fields.

For Rack I/O

Device Information	
Name	The Catalog name of the I/O Module.
Type	The type of I/O Module.
FW Version	The version number of the I/O Module firmware currently loaded.
Serial Num	The I/O Module's serial number.
LEDs	The I/O Module Operation and Fault Status is displayed by the round 'LED' symbols.

For Rail I/O

ControlNet Gateway Information:	
Name	The Catalog name of the ControlNet Gateway.
Type	The type of ControlNet Gateway.
FW Version	The version number of the ControlNet Gateway firmware currently loaded.

Serial Num	The ControlNet Gateway's serial number.
LEDs	The ControlNet Gateway Operation and Fault Status is displayed by the round 'LED' symbols.
Device Information:	
Name	The Catalog name of the I/O Module.
Type	The type of I/O Module.

If this data reflects the desired I/O Module, proceed to the Calibration or Utilities Tabs.

NOTES:

- Selection of an Analog Module enables the Calibration Tab.
- Selection of a Diagnostic Output Module enables the Utilities Tab.
- If 'GET MODULE DATA' fails, some of the fields display '???' and a STATUS message is displayed at the bottom of the Navigator Tab.
- Possible Messages:
  - 'Get Module Data Succeeded'
  - 'Get Module Data Failed'
  - 'Bad MAC ID for the Remote CNI'
  - 'Bad SLOT # for the Local Rack CNI' 'Selected Analog Module is READY to Calibrate'
  - 'Selected Analog Module is RUNNING. You MUST INACTIVATE and DELETE this Module from the Control Builder Monitoring TAB before Calibrating.'
  - 'The ControlNet Gateway is Connected to one or more Rail I/O Devices. You MUST INACTIVATE and DELETE any such Device(s) from the Control Builder Monitoring TAB before Calibrating.'

10.2.2 Series A I/O Maintenance Tool Calibration Tab

The Calibration Tab is enabled once the Navigator Tab specifies an Analog Module. The following are procedures for performing a Calibration sequence for various Analog Modules. Substitute calibration values from the procedure-subordinate tables based on the particular I/O Module type.

10.2.3 Series A AI (Rack I/O) Module Calibration

Attention

This calibration procedure only applies to the following Rack I/O Modules: TC-IAH061, TC-IAH161, TC-IXL061, TC-IXL062, and TC-IXR061.

1. Select the Channel or Channels to be calibrated with the 'Select' check boxes next to each Channel. For TC-IAH161, the 'Select Channel Group Box' is also used to navigate between the four (4) four-channel groups.
2. Select the 'Optional Cal Range' if the calibration range is 1~20mA for TC-IAH061, or -12~30mV for TC-IXL061 or TC-IXL062. Do not check for the other Analog Input module types.
3. Press 'Start Calibration Mode' Button. Calibration is prohibited if the I/O Module is in RUN Mode. Please inactivate and unload (delete) the I/O Module from the Controller before proceeding with Calibration.
4. Input exactly the Low Cal Value to the screw terminals of the channel(s).
5. Press 'Perform Low Cal' Button. The input is then sampled and the 'L' LED transitions to Yellow. If the Input is out of range the LED transitions to Red and the calibration is unsuccessful. Verify that the input is exactly the Low Cal Value and press 'Perform Low Cal' again.
6. Once the 'L' LED is Yellow, input exactly the High Cal Value to the screw terminals of the channel(s).
7. Press 'Perform High Cal' Button. The input is then sampled and the 'H' LED should transition to Yellow. If the Input is out of range the LED transitions to Red and the calibration is unsuccessful. Verify that the input is exactly the High Cal Value and press 'Perform High Cal' again.

8. Now that the Low signal and High signal are sampled, the calibration should finish and the 'H' and 'L' LEDs transition to Green. The Calibration Status LED on the left also transitions to Green. If either the low or high signal is not sampled correctly, the calibration is unsuccessful. In that case you can stop the calibration by pressing the 'Stop Calibration Mode' button. Note that the Calibration Status LED transitions to Red.

9. When the calibration has succeeded, the calibration mode stops automatically. You do not need to press 'Stop Calibration Mode' button. If you need to continue the calibration for other channels, repeat from step 1) until all channels are calibrated correctly.

10.2.4 Series A AI (Rack I/O) Calibration Value Table

Module	Low Value	Low Tolerance	High Value	High Tolerance
TC-IAH061	0V	+/-0.68mV	+10V	+/-0.6V
(Optional range)	1mA		20mA	
TC-IAH161	0V	+/-0.11V	+10.25	-0.07~0.18V
TC-IXL061 or TC-IXL062	-12mV	-0.89~0.84mV	+78mV	-3.7~4.0mV
(Optional range)	-12 mV		+30 mV	
TC-IXR061	1 Ohm	+/-0.8 Ohm	487 Ohm	+/-17 Ohm

Notes:

- TC-IXL061, TC-IXL062 and TC-IAH061 have two types of Calibration values depending on the configuration.
- The type is selected by the 'Optional Cal Range' check box.
- The tolerance for -12~30mV type is half of the -12~78 type.
- The tolerance means allowable difference counts from the Nominal Counts before the value is rejected with an error.
- The counts are converted to physical value based on the High Cal Nominal counts.
- The accuracy of the devices are typically 0.005%.

10.2.5 Series A AO (Rack I/O) Module Calibration

> **Attention**
>
> This calibration procedure only applies to the following Rack I/O Modules: TC-OAV061, TC-OAH061, and TC-OAV081.

1. Select the Channel or Channels to be calibrated with the 'select' check boxes next to each Channel. For TC-OAV061, the 'Select Channel Group Box' is also used to navigate between the two (2) four-channel groups.

2. For TC-OAV081, the 'optional cal range' selection enables the channel(s) selected to output mA values to the current output pins, for Current Mode calibration.

3. Press 'Start Calibration Mode' Button

4. Press 'Perform Low Cal' Button. The AO module outputs the Low Value. The 'L' LED transitions to Yellow.

5. Measure the value of the screw, and enter the value into the left 'Measurements' text box.

6. Press 'Perform High Cal' Button. The AO module outputs the High Value, and the 'H' LED transitions to Yellow.

7. Measure the value of the screw, and enter the value into the right 'Measurements' text box. The value should be near the High Value.

8. Press 'Finish Calibration' Button. The calibration should finish. If the entered values are out of range, the calibration is unsuccessful. In that case you can stop the calibration by pressing the 'Stop Calibration Mode' button. Note that the Calibration Status LED transitions to Red.

9. When the calibration has succeeded, the calibration mode stops automatically. You do not need to press 'Stop Calibration Mode' button. If you need to continue the calibration for other channels, repeat from step 1).

10.2.6 Series A AO (Rack I/O) Calibration Value Table

Module	Low Value	Low Tolerance	High Value	High Tolerance
TC-OAV061	0.0 V	+/-18 mV	10.0 V	+/-251 mV
TC-OAH061	4.0 mA	+/-0.15 mA	20.0 mA	+/-0.67 mA
TC-OAV081	0.0 V	+/-18 mV	10.0 V	+/-251 mV
(Optional current range)	4.0 mA	+/-0.15 mA	20.0 mA	+/-0.67 mA

Notes:

When the calibration has finished, the 'Last Cal Date' in the module is updated to Today's date.

10.2.7 Series A Current Input (Rail I/O) Module Calibration

> **Attention**
> This procedure only applies to TC-PIA082. The TC-FIAH81 does not allow calibration.

1. Select a Channel to be calibrated with the 'Select' check boxes next to the Channel Number. You can also select 'Sel All' to calibrate all channels at the same time.

2. Press 'Start Calibration Mode' Button. Calibration is prohibited if the Module is in RUN Mode. Please inactivate and unload (delete) the Module from the Controller before proceeding with Calibration. If the calibration can proceed, the 'Cal Active' LED on the top left corner transitions to Green.

3. Create an open circuit between the 'sig' (+) terminal and '-' (-) terminal(s) of selected channel(s).

4. Press 'Offset Cal' Button. The Input is then sampled and the 'Offset' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that there is an open circuit between 'sig' (+) terminal and '-' (-) terminal(s) of selected channel(s) and press 'Offset Cal' again.

5. Once the 'Offset' LED(s) transition to Green, input exactly the Gain Calibration Value of 20.000 mA to the screw terminals of the channel(s).

6. Press 'Gain Cal' Button. The Input is then sampled and the 'Gain' LED(s) should transition to Green. If the Input is out of range the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the current source connection is correct and that the input is exactly the Gain Calibration Value and press 'Gain Cal' again.

7. Once the Offset and Gain signals are sampled, the calibration should finish and the 'Offset' and 'Gain' LEDs should be Green.

8. If you need to continue the calibration for other channels, repeat from step 1) until all channels are calibrated correctly.

9. When the calibration has succeeded, press 'Stop Calibration Mode' button. All LEDs transition to White and the Navigator Tab is enabled.

10.2.8 Series A Current Output (Rail I/O) Module Calibration

Attention

This procedure only applies to TC-POA082. The TC-FOA041 does not allow calibration.

1. Select a Channel to be calibrated with the 'Select' check box next to the Channel Number. You can also select 'Sel All' to calibrate all channels at the same time.

2. Press 'Start Calibration Mode' Button. Calibration is prohibited if the Module is in RUN Mode. Please inactivate and unload (delete) the Module from the Controller before proceeding with Calibration. If the calibration can proceed, the 'Cal Active' LED on the top left corner transitions to Green.

3. Press 'Min Scale Cal' Button. The AO module outputs the Min Scale Cal Ref value of 1.000 mA. The 'Min' LED transitions to Yellow.

4. Connect the '+' lead(s) of the current meter(s) to the '+' terminal(s) of selected Channel(s). Connect the '-' lead(s) of the current meter(s) to 250 Ohm resistor(s). Connect the other end(s) of the 250 Ohm resistor(s) to the '-' terminal(s) of selected Channel(s).

5. Measure the value(s) at the screw(s), and enter the value(s) into the left 'Measurements' text box to a precision of 0.001 mA.

6. Press 'Finish Calibration' Button. The Minimum Scale calibration should finish and the 'Min' Calibration Status LED(s) transition to Green. If the entered value(s) are out of range, the calibration is unsuccessful and the 'Min' Calibration Status LED(s) transition to Red. Verify that the current meter(s) are properly connected and press 'Min Scale Cal' Button again.

7. Press 'Max Scale Cal' Button. The AO module outputs the Max Scale Cal Ref value of 21.000 mA. The 'Max' LED transitions to Yellow.

8. Connect the '+' lead(s) of the current meter(s) to the '+' terminal(s) of selected Channel(s). Connect the '-' lead(s) of the current meter(s) to 250 Ohm resistor(s). Connect the other end(s) of the 250 Ohm resistor(s) to the '-' terminal(s) of selected Channel(s).

9. Measure the value(s) of the screw(s), and enter the value(s) into the left 'Measurements' text box to a precision of 0.001 mA.

10. Press 'Finish Calibration' Button. The Maximum Scale calibration should finish and the 'Max' Calibration Status LED(s) transition to Green. If the entered value(s) are out of range, the calibration is unsuccessful and the 'Max' Calibration Status LED(s) transition to Red. Verify that the current meter(s) are properly connected and press 'MaxScale Cal' Button again.

11. If you need to continue the calibration for other channels, repeat from step 1) until all channels are calibrated correctly.

12. When the calibration has succeeded, press 'Stop Calibration Mode' button.

10.2.9 Series A Temperature Input (Rail I/O) Module Calibration #1

Attention

There are two Temperature Input (Rail I/O) Module calibration procedures. This procedure only applies to TC-PIL081. There is a separate procedure (following this one) for TC-FIL081.

1. Select a Channel to be calibrated with the 'Select' check box next to the Channel Number. You can also select 'Sel All' to calibrate all channels at the same time.

2. Press 'Start Calibration Mode' Button. Calibration is prohibited if the Module is in RUN Mode. Please inactivate and unload (delete) the Module from the Controller before proceeding with Calibration. If the calibration can proceed, the 'Cal Active' LED on the top left corner transitions to Green.

3. Press 'Offset Cal' Button. This enables Offset calibration for ALL Programmable Gain Amplifier (PGA) Selections.

4. Connect the voltage source to the millivolt-input terminals of the selected Channel(s).

5. To the screw terminals of the selected channel(s), input exactly the Offset Calibration Value for a particular PGA Selection for which a button is currently Enabled. (Note: Refer to the table below for Offset Calibration Values corresponding to each PGA Selection). Press the Enabled PGA Selection Button. The Input is then sampled and the 'Offset' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Offset Calibration Value and press Enabled PGA Selection Button again. Repeat this step for all PGA Selections.

6. Press 'Gain Cal' Button. This enables Gain calibration for ALL PGA Selections.

7. To the screw terminals of the selected channel(s), input exactly the Gain Calibration Value for a particular PGA Selection for which a button is currently Enabled. (Note: Refer to the table below for Gain Calibration Values corresponding to each PGA Selection). Press the Enabled PGA Selection Button. The Input is then sampled and the 'Gain' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Gain Calibration Value and press Enabled PGA Selection Button again. Repeat this step for all PGA Selections.

8. Connect 383 Ohm resistor(s) to the selected channel(s) in a 4 wire configuration (resistor is connected to '+' and '-' terminals, and sense wire is connected to 'L' and 'H' terminals).

9. Press '383 Ohm Current Cal' Button. The Input is then sampled and the '383□' LED(s) should transition to Green. If the resistor value is wrong or the connection is not correct, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the resistor value is exactly the specified value and is properly connected in a 4-wire configuration and press '383 Ohm Current Cal' Button again.

10. Connect 100 Ohm resistor(s) to the selected channel(s) in a 4 wire configuration.

11. Press '100 Ohm Current Cal' Button. The Input is then sampled and the '100□' LED(s) should transition to Green. If the resistor value is wrong or the connection is not correct, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the resistor value is exactly the specified value and is properly connected in a 4-wire configuration and press '100 Ohm Current Cal' Button again.

12. Select Thermistor(s) for Cold Junction Compensation calibration. Replace the selected cold junction compensation thermistor(s) by a 10K Ohm resistor(s).

13. Press 'Cold Junction Compensation Calibration' Button. The LED(s) next to the selected thermistor(s) should transition to Green. If the resistor(s) value is wrong, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the resistor value is exactly the specified value and it is properly connected in a 4-wire configuration and press 'Cold Junction Compensation Calibration' Button again.

14. If you need to continue the calibration for other channels or thermistors, repeat from step 1) until all channels and thermistors are calibrated correctly.

15. When the calibration has succeeded, press 'Stop Calibration Mode' button. All LEDs transition to White and the Navigator Tab becomes enabled.

10.2.10 Series A Temperature Input (Rail I/O) Calibration #1 Value Tables

Programmable Gain Amplifier Selection	Offset Value	Offset Tolerance	Gain Value	Gain Tolerance
Gain = 1	0.000 mV	+/-13.2 mV	330.000 mV	+/-13.2 mV
Gain = 2	-30.000 mV	+/-6.6 mV	100.000 mV	+/-6.6 mV
Gain = 4	-10.000 mV	+/-3.3 mV	77.000 mV	+/-3.3 mV
Gain = 8	-5.000 mV	+/-1.1 mV	48.000 mV	+/-1.1 mV
Gain = 16	-1.000 mV	+/-1.6 mV	22.000 mV	+/-1.6 mV

Current Nominal Resistance	Accepted Values
100 Ohms	90 Ohms - 175 Ohms

Current Nominal Resistance	Accepted Values
383 Ohms	373 Ohms - 458 ohms

CJC Nominal Resistance	Accepted Values
10k Ohms	9.2k Ohms - 11.9k Ohms

Notes:

- The accuracy of voltage source should be 0.01% or better.
- Offset and Gain calibration should be done before other parameters are calibrated.
- Cold Junction calibration should be done after the Offset and Gain calibration of Channel 0.
- 100 Ohm Current Calibration should be done after 383 Ohm Current Calibration.
- Loop Resistance Compensation is not part of calibration, it is a tuning procedure that calculates automatically RTD loop resistance offset and is used if during configuration of the module, the RTD loop resistance offset was selected to be 'Determined'. To compensate for loop resistance, either {1} determine cable resistance by measurement and place a resistor of the same value across terminals or {2} short the cable as close to RTD as possible.

10.2.11 Series A Temperature Input (Rail I/O) Module Calibration #2

> **Attention**
> There are two Temperature Input (Rail I/O) Module calibration procedures. This procedure only applies to TC-FIL081. The previous procedure applies to TC-PIL081.

1. Select a Channel to be calibrated with the 'Select' check box next to the Channel Number. You can also select 'Sel All' to calibrate all channels at the same time.
2. Press 'Start Calibration Mode' Button. Calibration is prohibited if the Module is in RUN Mode. Please inactivate and unload (delete) the Module from the Controller before proceeding with Calibration. If the calibration can proceed, the 'Cal Active' LED on the top left corner transitions to Green.
3. Connect 0.000mV across each input channel. Connect all high signal terminals together and attach to the positive lead from the precision voltage source. Connect all low signal terminals together and attach to the negative lead. The Offset Calibration Value is 0.000mV.
4. Press 'Offset Cal' Button. This enables Offset calibration for the selected channel(s).
5. The Input is then sampled and the 'Offset' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Offset Calibration Value.
6. If the Offset Calibration was successful, then proceed to the Gain Calibration. Connect exactly 75.000mV (the Gain Calibration Value) across each input channel.
7. Press 'Gain Cal' Button. This enables Gain calibration for the selected channel(s).
8. The Input is then sampled and the 'Gain' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Gain Calibration Value.
9. If you need to continue the calibration for other channels, repeat from step 1) until all channels are calibrated correctly.
10. When the calibration has succeeded, press 'Stop Calibration Mode' button. All LEDs transition to White and the Navigator Tab becomes enabled.

10.2.12 Series A RTD Input (Rail I/O) Module Calibration

> **Attention**
> This procedure only applies to TC-FIR081.

1. Select a Channel to be calibrated with the 'Select' check box next to the Channel Number. You can also select 'Sel All' to calibrate all channels at the same time.

2. Press 'Start Calibration Mode' Button. Calibration is prohibited if the Module is in RUN Mode. Please inactivate and unload (delete) the Module from the Controller before proceeding with calibration. If the calibration can proceed, the 'Cal Active' LED on the top left corner transitions to Green.

3. Connect 1.00 ohm resistors across each input channel. Connect the low signal side to 24Vdc common. If using a decade box, connect all high signal terminals together and attach to one lead from the decade box. Connect all low signal terminals together and attach to the other lead and to 24V dc common. Set the decade box for 1.00 ohm. The Offset Calibration Value is 1.00 ohm.

4. Press 'Offset Cal' Button. This enables Offset calibration for the selected channel(s).

5. The Input is then sampled and the 'Offset' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Offset Calibration Value.

6. If the Offset Calibration was successful, then proceed to Selecting the RTD type for the Gain Calibration. Use the table below to determine the Gain Calibration.

7. Connect the correct resistors across each input channel. Connect the low signal side to 24V dc common. Resistor values are shown in the table below. If using a decade box, connect all high signal terminals together and attach to one lead from the decade box. Connect all low signal terminals together and attach to the other lead and to 24V dc common. Set the decade box for the value shown in the table below.

8. Press 'Gain Cal' Button. This enables Gain calibration for the selected channel(s).

9. The Input is then sampled and the 'Gain' LED(s) should transition to Green. If the Input is out of range, the LED(s) transition to Red. In this case the calibration did not succeed. Verify that the voltage source connection is correct and that the input is exactly the specified Gain Calibration Value.

10. If you need to continue the calibration for other channels, repeat from step 1) until all channels are calibrated correctly.

11. When the calibration has succeeded, press 'Stop Calibration Mode' button. All LEDs transition to White and the Navigator Tab becomes enabled.

10.2.13 Series A RTD Input (Rail I/O) Calibration Value Table

Type of RTD	Offset Calibration Value	Gain Calibration Value
100 ohm Pt. (alpha = 0.00385)	1 ohm, 0.1%, 5ppm/deg C	
100 ohm Pt. (alpha = 0.003916)	1 ohm, 0.1%, 5ppm/deg C	432ohm, 0.01%, 5ppm/deg C
120 ohm Nickel (alpha = 0.00672)	1 ohm, 0.1%, 5ppm/deg C	432ohm, 0.01%, 5ppm/deg C
100 ohm Nickel (alpha = 0.00618)	1 ohm, 0.1%, 5ppm/deg C	432ohm, 0.01%, 5ppm/deg C
10 ohm Copper (alpha = 0.00427)	1 ohm, 0.1%, 5ppm/deg C	432ohm, 0.01%, 5ppm/deg C
200 ohm Pt. (alpha = 0.00385)	1 ohm, 0.1%, 5ppm/deg C	864 ohm, 0.01%, 5ppm/deg C
200 ohm Nickel (alpha = 0.00618)	1 ohm, 0.1%, 5ppm/deg C	864 ohm, 0.01%, 5ppm/deg C

Type of RTD	Offset Calibration Value	Gain Calibration Value
500 ohm Pt. (alpha = 0.00385)	1 ohm, 0.1%, 5ppm/deg C	1728 ohm, 0.01%, 5ppm/deg C
500 ohm Nickel (alpha = 0.00618)	1 ohm, 0.1%, 5ppm/deg C	

10.2.14 Series A Diagnostic Output Module SHORT / THERMAL OVERLOAD faul

When a Diagnostic Output Module is selected in the Navigator tab, the Utilities Tab is enabled. The Utilities Tab is used to reset Diagnostic Output Module SHORT / THERMAL OVERLOAD Faults as follows:

1. Be sure that the condition, which caused the Short/Overload, has been corrected.
2. Enable the Channel or Channels to be reset with the 'Enable Reset' check boxes.

1. Press the RESET COMMAND Button.
2. A RESET COMMAND WARNING Message Box will appear. This reminds the User to confirm that Only Shorted Channels should be Enabled.
3. Press 'YES' if ready to Send the Command or 'NO' if you wish to change any Reset Enable selections before sending the Command.
4. When the Command is sent, the Fault condition should be cleared for the Channel(s) selected as indicated by {1} the I/O Module Detail Display on STATION, {2} the I/O Channel Function Block in Control Builder, or {3} the LED status on the front of the I/O Module.

10.3 Using C200/C200E CPM Tools

CPM Tools for C200/C200E is a command line (pcmana.exe), diagnostic application intended for internal Experion Engineering usage. Certain situations, however, merit its usage by users in conjunction with our Technical A.

This utility supports both Ethernet and ControlNet networks. With the possibility of having multiple RSLinx drivers, the user must first select the driver needed to communicate with the module under investigation. A list of currently configured drivers is presented to the user that the user can select from. Once a driver is selected, the main menu is presented to the user. Note that all of the functionality offered on the main menu can be obtained by using the NetworkTools application.

10.3.1 CPM Tools 'd' - Display Module State

Selecting 'd' from the Main Menu displays the module's current state.

10.3.2 CPM Tools 'v' - Display Module Version

Selecting "v" from the Main Menu displays the module's Boot and Application firmware version.

```
> v

MODULE 03-03:
        BOOT            = cpmboot2
            VERSION     = PS320.0-14.1
            CREATED     = Tue May 23 11:14:47 2000

        PERSONALITY     = ceerex2
            VERSION     = PS320.0-14.1
            CREATED     = Tue May 23 12:42:08 2000
```

10.3.3 CPM Tools 'b' - Display Module Startup Information

Selecting "b" from the Main Menu displays the module's reasoning for vetoing a Retention Startup. The first non-false reason encountered in the list indicates why Retention Startup was not possible. More specifically, the list of reasons, from top-to-bottom, is ordered in the sequence that the controller performs the test on the individual items.

For example, the following illustrates the Startup Information for a controller that did not perform Retention Startup because it was rebooted as a consequence of Application firmware upgrade:

```
> b

  RSU Veto Category                   State
  ============================= =====
 RAM/ROM corruption (or No PI Loaded).0x03
    CPM slot # changed..................T
    CPM chassis serial # changed.......T
    Supervisory CNB MAC ID changed.....F
    I/O Manager database invalid.......F
    Logical Shared Memory invalid......F
    Strategy download in progress......F
    Commanded shutdown.................F
    (spare)............................F
    (spare)............................F
    (spare)............................F
    Initial redundancy state = sec.....F
```

As another example, the following illustrates the Startup Information for a controller that did perform Retention Startup:

```
> b

  RSU Veto Category                   State
  ============================= =====
 RAM/ROM corruption (or No PI Loaded)...F
    CPM slot # changed..................F
    CPM chassis serial # changed.......F
    Supervisory CNB MAC ID changed.....F
    I/O Manager database invalid.......F
    Logical Shared Memory invalid......F
    Strategy download in progress......F
    Commanded shutdown.................F
    (spare)............................F
    (spare)............................F
    (spare)............................F
    Initial redundancy state = sec.....F
```

10.3.4 CPM Tools 'f' - Display SIM FTA Information

Selecting "f" from the Main Menu displays the SIM's FTA(s) information.

```
> f

SIM0105-0506:
        A (channels  0-15):
        FTA is missing or is unpowered!
            updates/sec: 0.000000
              writes/sec: 0.000000
          overruns/sec: 0.000000
                reserved: 0.000000

        B (channels 16-31):
        FTA is missing or is unpowered!
            updates/sec: 0.000000
              writes/sec: 0.000000
          overruns/sec: 0.000000
                reserved: 0.000000
```

10.3.5 CPM Tools 'r' - Recover Failed Module

Selecting "r" from the Main Menu attempts to recover the module from the faulted state.

```
> r

 RECOVER results in a FAILED->READY or ALIVE state transition
 Would you like to continue? y/n
> y


!!! WAITING FOR MODULE 03-03 TO REBOOT ....................................

MODULE 03-03 IS NOW READY
```

10.3.6 CPM Tools 's' - Start Module

Selecting "s" from the Main Menu reboots the module from execution in the Boot firmware (e.g. the Alive or Ready states) into the application firmware (e.g. No Database or Ok states).

```
> s

 START results in a READY->OK state transition
Would you like to continue? y/n
> y


!!! WAITING FOR MODULE 03-03 TO REBOOT ...................................

MODULE 03-03 IS NOW NODB
```

10.3.7 CPM Tools 'c' - Module Crash Analysis

Selecting "c" from the Main Menu displays the module's crash block.

```
> c
C:\ /<null>     Thu Jun 22 08:04:44 2000


MODULE 03-03:
        BOOT        = cpmboot2
            VERSION   = PS320.0-14.1
            CREATED   = Tue May 23 11:14:47 2000

        PERSONALITY  = ceerex2
            VERSION   = PS320.0-14.1
            CREATED   = Tue May 23 12:42:08 2000

  CR    = 0x20000000  MSR   = 0x0000b930  HID0  = 0x9000c000  XER   = 0x20000000
  LR    = 0xffc0d5f4  CTR   = 0x00000000  SRR0  = 0xffc088b8  SRR1  = 0x0000b930
  DEC   = 0x0000f297  IP    = 0xffc0d5f0  HSR   = 0x20004bf7
  DSISR = 0x00000000  DAR   = 0x00000000

  R00   = 0xffc0d5a0  R01   = 0x00240db8  R02   = 0xffd7ab60  R03   = 0x00001234
  R04   = 0xffc0edb0  R05   = 0x00240ca4  R06   = 0x00240ca0  R07   = 0x00182844
  R08   = 0x0000b930  R09   = 0x00184b0c  R10   = 0x00000002  R11   = 0x00000002
  R12   = 0x001c9ae8  R13   = 0x0002028c  R14   = 0x00000000  R15   = 0x00000000
  R16   = 0x00000000  R17   = 0x00000000  R18   = 0x00000000  R19   = 0x00000000
  R20   = 0x00000000  R21   = 0x00000000  R22   = 0x00000000  R23   = 0x00000000
  R24   = 0x00000000  R25   = 0x00000000  R26   = 0x00000000  R27   = 0x00000000
  R28   = 0x00000000  R29   = 0x00000000  R30   = 0x00000000  R31   = 0x00019618

Application error address - 0xffc0d5f0

Initialized data address   0x00006000 (size 0x12600)
Uninitalized data address 0x00018600 (size 0x13abc0)
Stack address              0x00240db8 (size 0x800)

User defined error code  -- 0x1234,  message -- EDO_TEST_CRASH - forced pcm crash.

DO YOU WISH TO CREATE A CRASH DUMP FILE? y/n
> y

 ENTER A NEW FILENAME TO CREATE (e.g. >'pcmdata.txt')
 or press 'ENTER' for the default name = pcmcrash.txt

>

Data file is pcmcrash.txt


!!!!!!!!!! CRASH FILE CREATED OK !!!!!!!!!!!!!!
```

10.3.8 CPM Tools 'i' - Load Module Program Image

Selecting "l" from the Main Menu allows the user to update the module's Boot or Application firmware.

```
> 1

---------- LOADING UTILITY for CPM and SIM -------------------
   Ver 10.2        May 23 2000 11:18:23

Driver AB_PCIC-1 is opened
ENTER LOAD IMAGE FILENAME for MODULE AB_PCIC-1-03-03
>c:\ceerex2.pcm
 Calculating CheckSum for File ceerex2

    >>>>>>>>>>>>>>>>  OK


 ********* image 1 --> ceerex2 *********
   1)Filename        ---------- ceerex2
       File version ---------- PS320.0-14.1
       File date    ---------- Tue May 23 12:42:08 2000

 --->  LOADABLE

Load file size  ---------------- 1595904 bytes

!!!!! PERSONALITY WILL BE LOADED/REPLACED !!!!!

PROCEED WITH LOAD/REPLACE ? Y/N
>y

Loading... ceerex2

Load Complete -- 1595904 bytes transferred

!!!!!!! REBOOTING TO START THE LOADED PROGRAM !!!!!!!

!!! WAITING FOR MODULE 03-03 TO REBOOT .....................
MODULE 03-03 IS NOW NODB
```

10.3.9 CPM Tools 'p' - Select New Module Path

Selecting "p" from the Main Menu allows the user to change the communication path to the module under investigation.

```
> p
The running dtl32.dll can handle 16 drivers.
There are 1 drivers installed.

 1    AB_PCIC-1 IS A CONTROLNET DRIVER
 ENTER DRIVER NUMBER
1
 YOU SELECTED AB_PCIC-1
 This is a ControlNet Driver
Remote chassis [Y or N]?
> y
Remote segment is EtherNet or ControlNet [E or C]?
c
 ENTER MACID of supervisory CNI [1..99]
> 1
 ENTER slot no. of downlink CNI [0..17]
> 5
 ENTER MACID of remote CNI [1..99]
> 5
 ENTER SLOT NUMBER of the Target Module [0..17]
> 6
using path: AB_PCIC-1-0105-0506
```

10.3.10 CPM Tools 't' - Force Shutdown Of Module

Selecting "t" from the Main Menu forces the module to transition to the Ready State. This option is useful when performing module firmware update.

⚠ **CAUTION**

Use extreme caution when forcing shutdown and double check that the path is properly specified because execution of this option results in an immediate loss-of-control.

```
> t

 SHUTDOWN results in a OK->Ready state transition.
 WARNING: This will result in immediate loss of control!
 Would you like to continue? y/n
> y


 !!! WAITING FOR MODULE 03-03 TO REBOOT ...................................

 MODULE 03-03 IS NOW READY
```

10.3.11 CPM Tools 'x' - Exit Program

Selecting "x" from the Main Menu exits the CPM Tools application.

11 Database Administration Utility (DBADMIN)

Related topics

11.1 Using DBADMIN

The Database Administration (DBADMIN) tool is a utility for maintaining the Engineering Repository Database (ERDB) used by the Experion system to create and maintain the control strategies, the Qualification and Version Control System (QVCS) database for maintaining version control, and the databases for the wireless Directory Server (DS), Key Server (KS), and HART parameters. It enables users to initiate the following database maintenance tasks:

The following list provides guidelines for using the DBADMIN.

- Display and clear locks left in the ERDB, Custom Algorithm Block (CAB), and/or Phase Block after abnormal termination of the Control Builder, CAB, or Phase configuration.
- Restore the 'clean' database for the selected database function.
- Detach and copy the primary ERDB to specified location.
- Check the consistency of the ERDB.
- Re-organize data and index pages, and update statistics of the ERDB.
- Expand the size of the ERDB database.
- Create a backup of the current database - ERDB, QVCS, DS, KS, and/or wireless HART parameters.
- Restore a backup database in the primary ERDB, QVCS, DS, KS, and/or wireless HART parameters.
- Synchronize the Qualification and Version Control System (QVCS) database with the ERDB and clear any QVCS locks

And, for redundant Servers only:

- Recover a Primary or Secondary ERDB.
- Synchronize ERDBs to start and stop replication.

11.1.1 DBADMIN interface

The Microsoft Management Console hosts the DBADMIN tool with a typical Windows type interface. The interface includes dropdown menus, directory tree pane and a view pane as shown in the following figure.
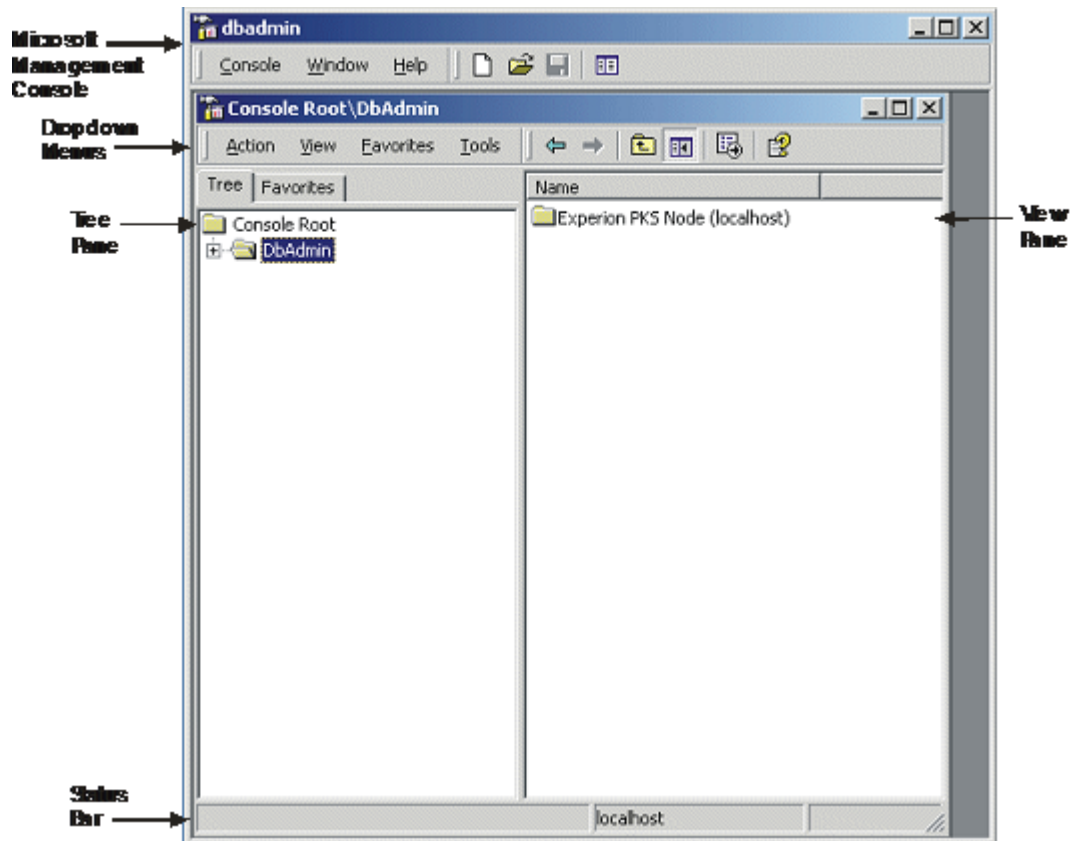
Figure 1: MMC hosts DBADMIN Tool with common Windows type interface.

11.1.2 Terminology

Term	Definition
CAB	Custom Algorithm Block
EMB	Enterprise Model Builder
ERDB	The Experion Engineering Repository relational database.
Master	Also referred to as Design Master or Primary ERDB. The primary copy of a redundant ERDB.
ODBC	(Open Database Connectivity) - A protocol for accessing databases that is used by Experion applications.
Replica	A secondary or backup copy of the ERDB that is maintained in sync with the design master.
Replicated	An ERDB that has been] synchronized copies for ERDB redundancy purposes.
SQL	(Structured Query Language) - A database sublanguage used in querying, updating, and managing relational databases. Used by Experion applications to access the ERDB.
Synchronize	The process of copying database information between master and replica to bring both copies up to date.
VCS	Qualification and Version Control System
DS	Wireless Directory Server (R311 or greater only)

Term	Definition
KS	Wireless Key Server (R311 or greater only)

11.1.3 Installation

The DBADMIN tool (dbadmin.msc) executable resides in this Experion directory *Program Files\Honeywell \Experion PKS\Engineering Tools\system\bin*. It is installed as part of the Experion process software installation procedure for Engineering Tools.

11.2 Starting DBADMIN

Use the following procedure to launch the DBADMIN tool through Configuration Studio for the control strategy Engineering Repository Database (ERDB), QVCS database, DS database, KS database, or wireless HART parameters database.

Prerequisites

- You have enabled the **Allow Single Signon** option through Station and have previously logged onto the computer with appropriate security level to initiate actions through the DBADMIN tool

To launch DBADMIN through Configuration Studio for ERDB, QVCS, DS, KS, and HART parameters

1 Click the Start button on the taskbar. Click **Programs** > **Honeywell Experion PKS** > **Server** > **Configuration Studio**.
    Launches the Configuration Studio.

2 On **Connect** dialog, select applicable Experion Server. Click the **Connect** button
    Opens Server directory in Configuration Explorer tree view.

3 Click Control Strategy icon.
    Opens Categories in view window.

4 On **Process Control Strategies** category, click **Administer the control strategy database**.
    Launches the DbAdmin utility.
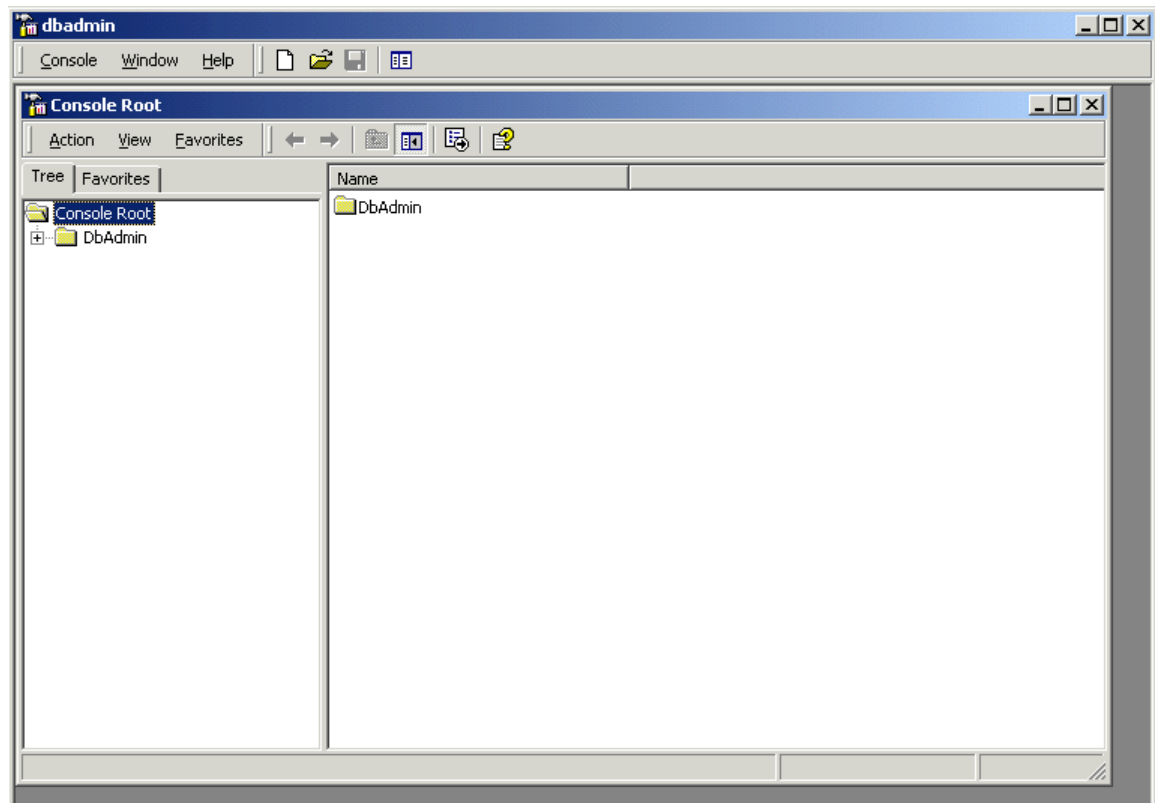
5 Click the plus sign for DbAdmin folder icon and then plus sign for Server folder icon.
    Expands Server directory of database functions.

6 Please go to the next section *Menu or tree pane functions* for a list of the functions you can initiate using this utility.

To launch DBADMIN through Configuration Studio for EMDB

1 Click the Start button on the taskbar. Click **Programs** > **Honeywell Experion PKS** > **Server** > **Configuration Studio**.

Launches the Configuration Studio.

2 On **Connect** dialog, select applicable Experion System. Click the **Connect** button

Opens SystemName directory in Configuration Explorer tree view.

3 On **System Tasks** category, click **Administer the system database**.

Launches the DbAdmin utility.
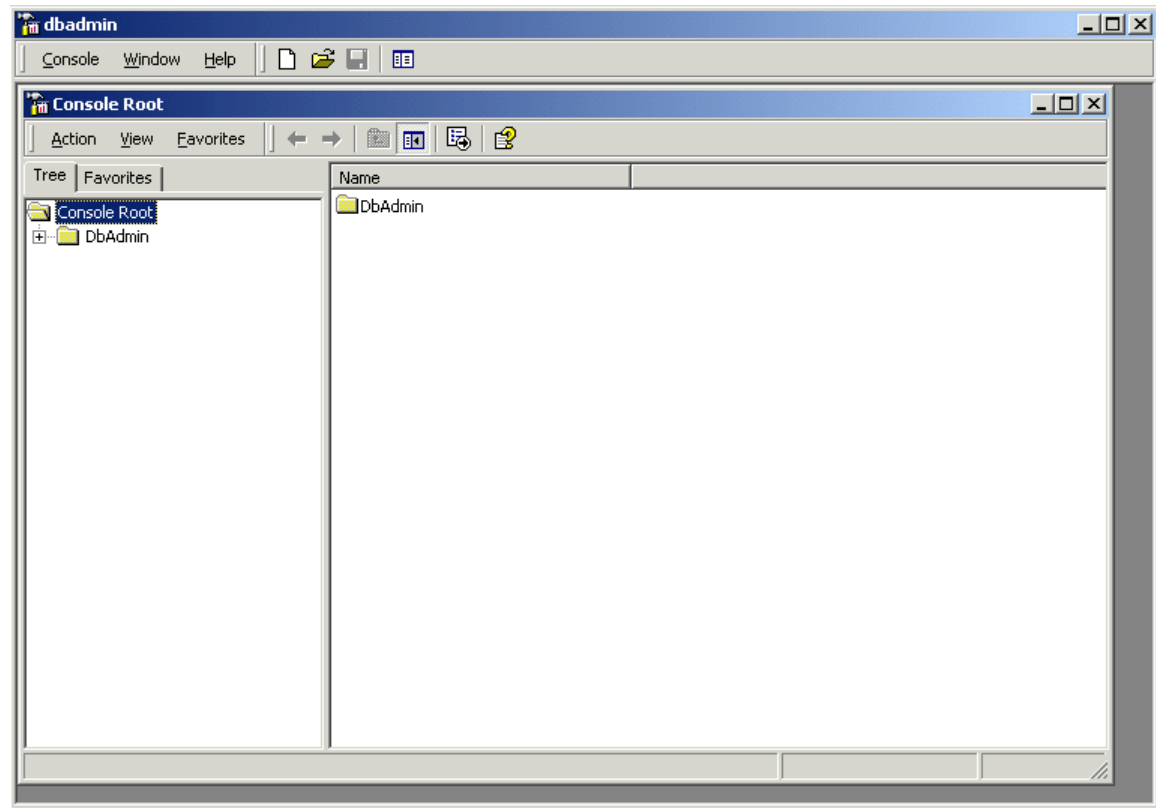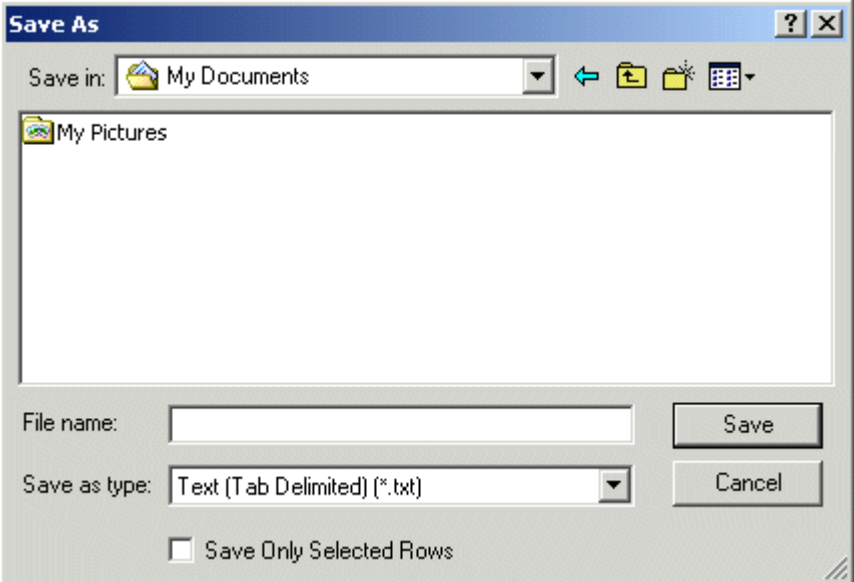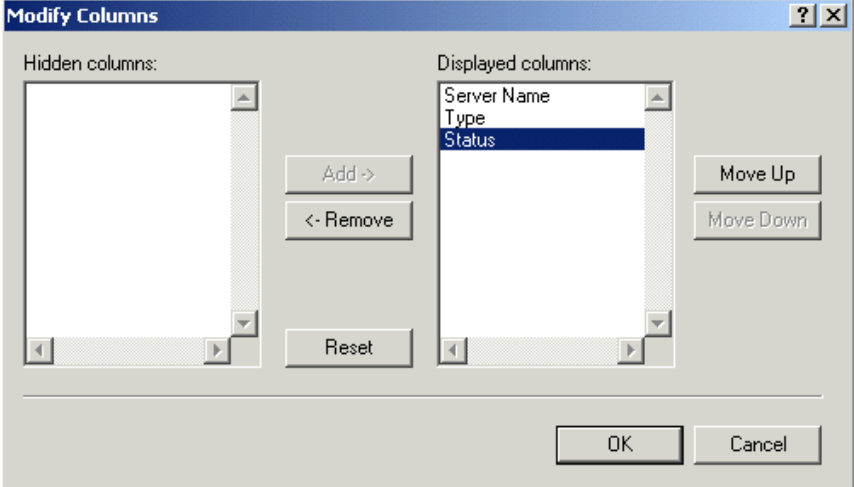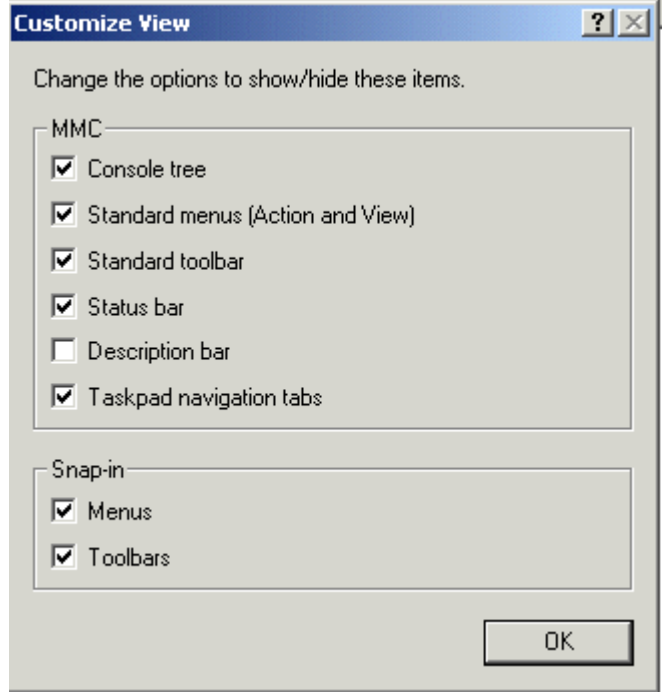
4 Click the plus sign for DbAdmin folder icon and then plus sign for Server folder icon.

Expands Server directory of database functions.

5 Please go to the next section *Menu or tree pane functions* for a list of the functions you can initiate using this utility.
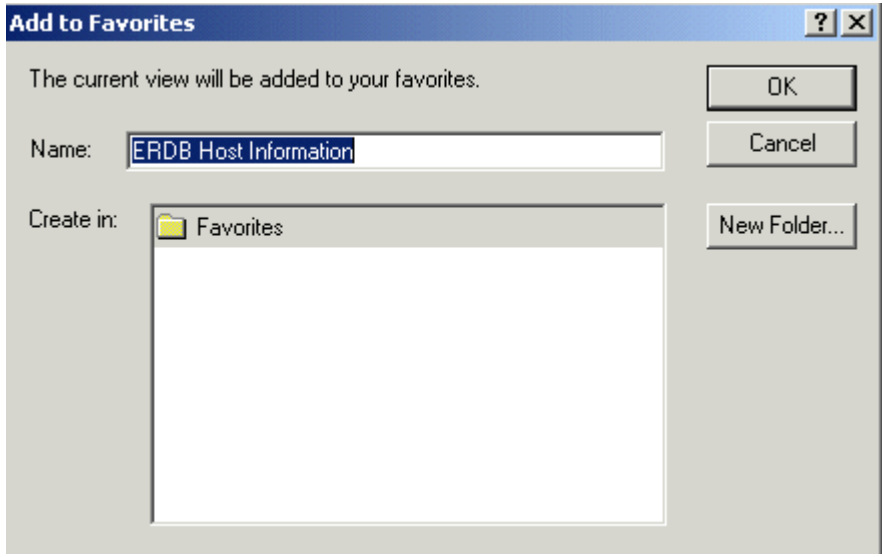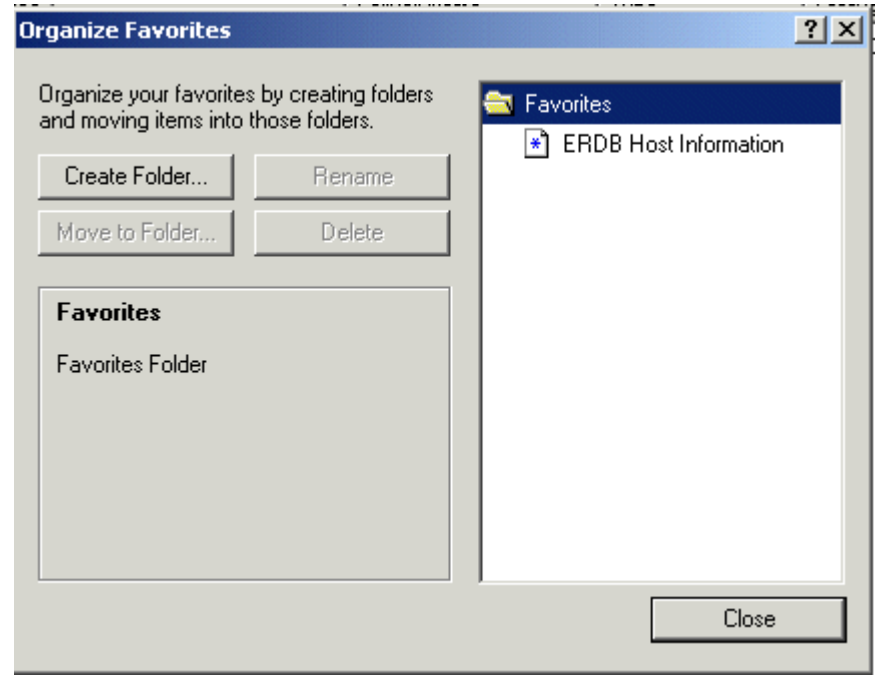
11.2.1 Menu or tree pane functions
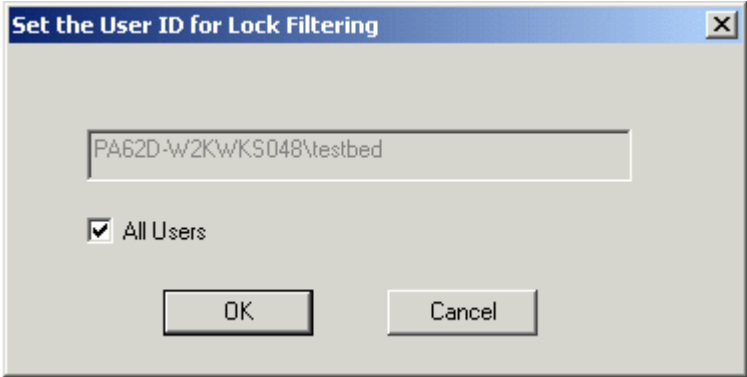
The following table summarizes the functions you can initiate through a given menu or tree pane selection for reference. If you are familiar with working in a Windows type environment, you should be able to intuitively interact with all the functions provided through DBADMIN tool menu selections. Please note that the selections available in a given menu will vary depending on the current active function.
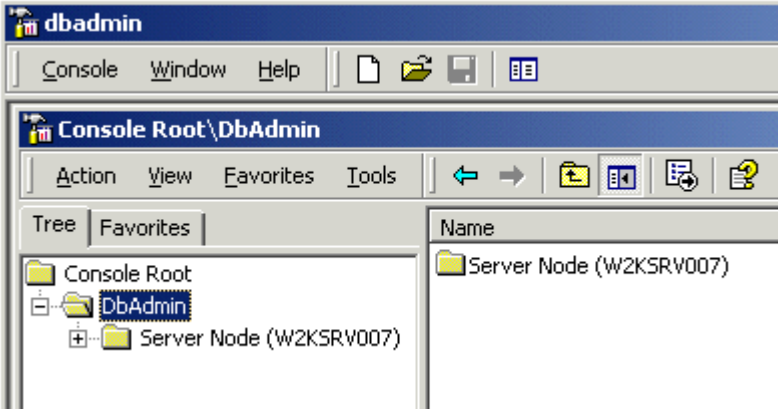
Click This Menu Selection . . .	To Initiate This Function . . .
Action->New Window from Here	Opens new console root window.
Action->New Taskpad View	Open New Taskpad View Wizard to create another taskpad view.
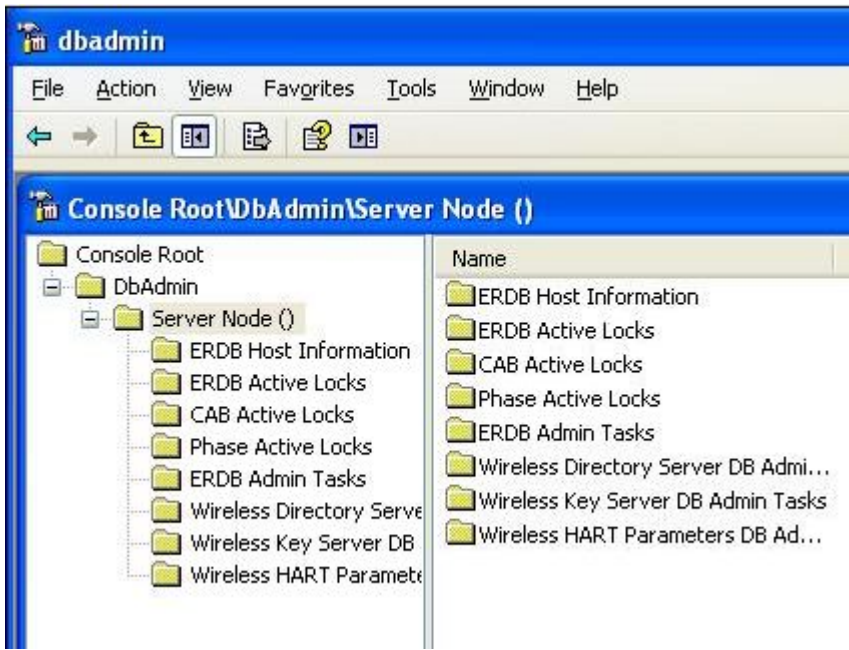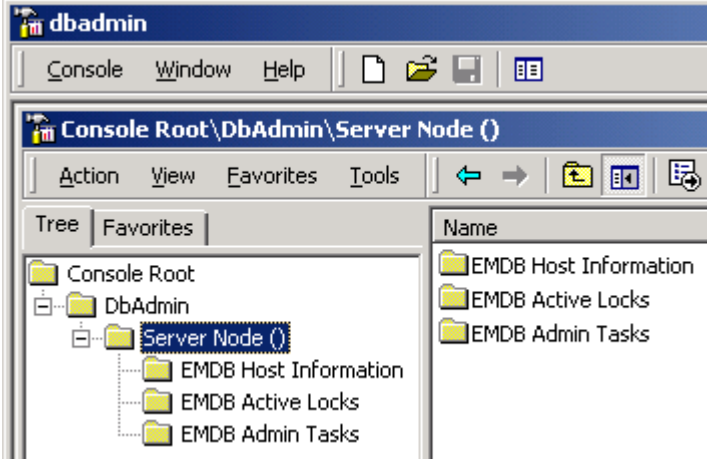
Click This Menu Selection . . .	To Initiate This Function . . .
Action->Export List	Opens Save as dialog box to save data as text file to specified location.
Action->Help	Calls up Microsoft Management Console help.
View->Choose Columns	Calls up Modify Columns dialog box. Use buttons provided to move, remove, or add columns as applicable.
View->Large Icons	Changes view to use Large Icons style.
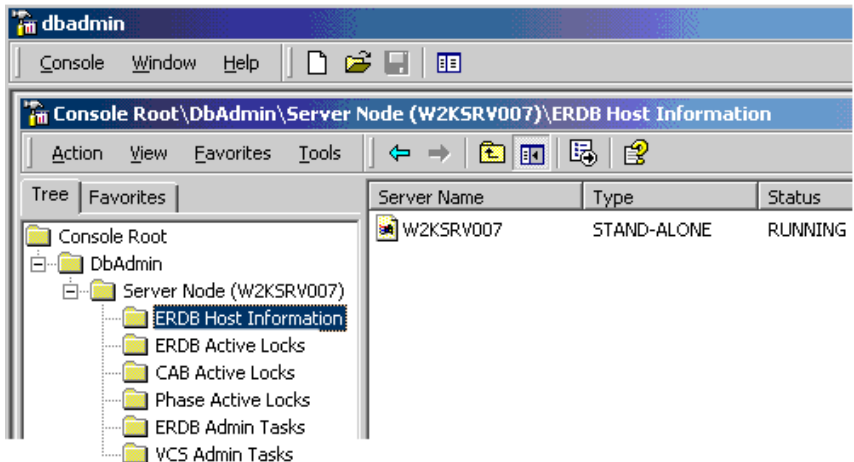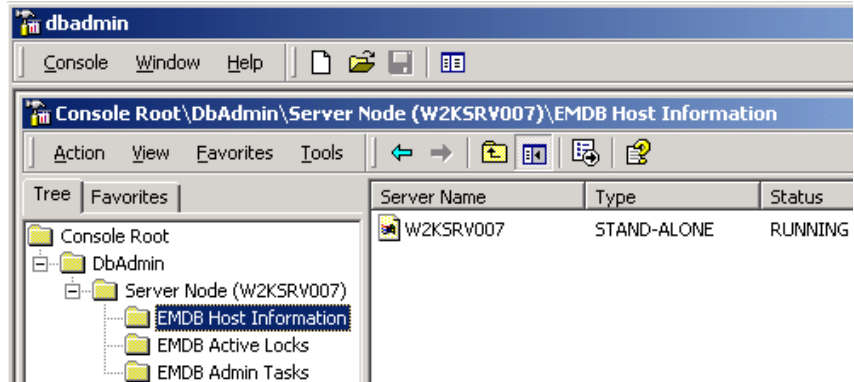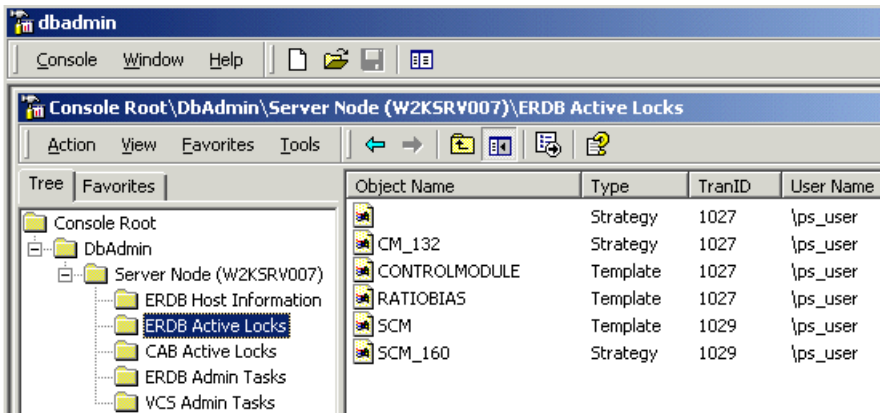
Click This Menu Selection . . .	To Initiate This Function . . .
View->Small Icons	Changes view to use Small Icons style. pa62d-w2kwks048
View->List	Changes view to use List style. pa62d-w2kwks048
View->Detail	Changes view to use Detail style. | Server Name	Type	Status
pa62d-w2kwks048	STAND-ALONE	RUNNING	
View->Customize	Calls up Customize View dialog box. Use checkbox selections to view or hide the listed items. **Customize View** Change the options to show/hide these items. MMC ☑ Console tree ☑ Standard menus (Action and View) ☑ Standard toolbar ☑ Status bar ☐ Description bar ☑ Taskpad navigation tabs Snap-in ☑ Menus ☑ Toolbars OK
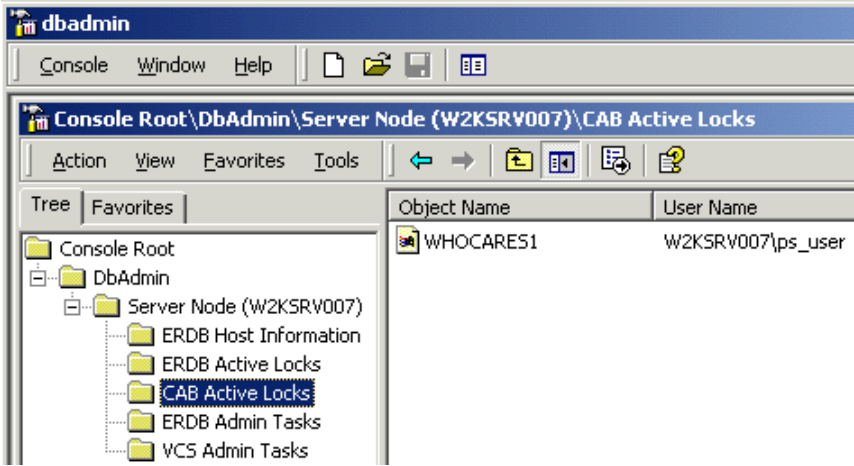
Click This Menu Selection . . .	To Initiate This Function . . .
Favorites->Add Favorites	Calls up Add to Favorites dialog box. Lets you add views to favorites tab. Favorite is also added to the Favorites dropdown menu.
Favorites->Organize Favorites	Opens Organize Favorites dialog box. Lets you create folders and move items into folders.
Tools->Refresh Status	Refresh data in View pane. (Only active for selected directory tree functions.)
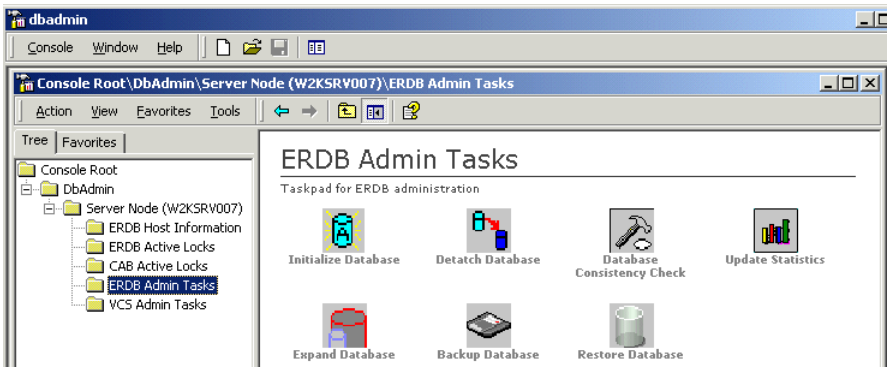
Click This Menu Selection . . .	To Initiate This Function . . .
Tools->User Filter	Opens the Set the User ID for Lock Filtering dialog box. Lets you restrict lock access to the specified user for the selected node. The value entered is saved in the Windows Registry and becomes the default for the next session. The user ID includes the machine name and the login name for the user whose locks are to be cleared. The default selection is 'All Users', which defeats the 'by user' filtering mechanism. (Only active for selected directory tree functions.)
Tools->Refresh Locks	Refreshes the View pane to show the most current lock information in the ERDB, CAB or Phase. (Only active for selected directory tree functions.)
Tools->Clear All Locks	Clears all the current locks in the ERDB, CAB, or Phase. The current User Filter setting is applied, when clearing the list of associated locks. (Only active for selected directory tree functions.)

Click this Tree Pane Selection . . .	To Initiate This Function . . .
DbAdmin	Access Experion Node folder.
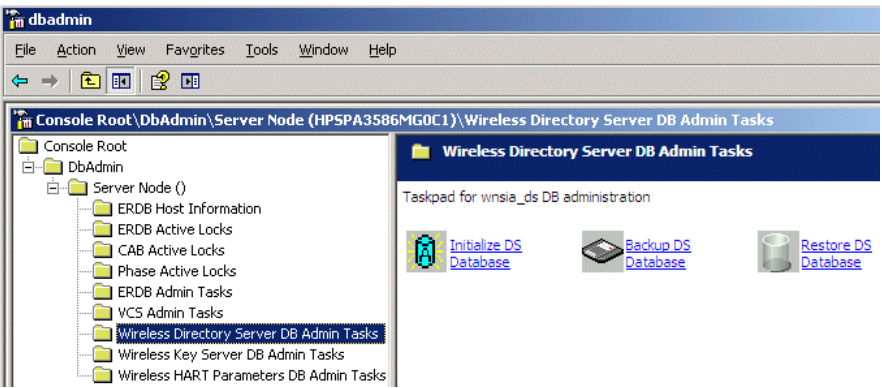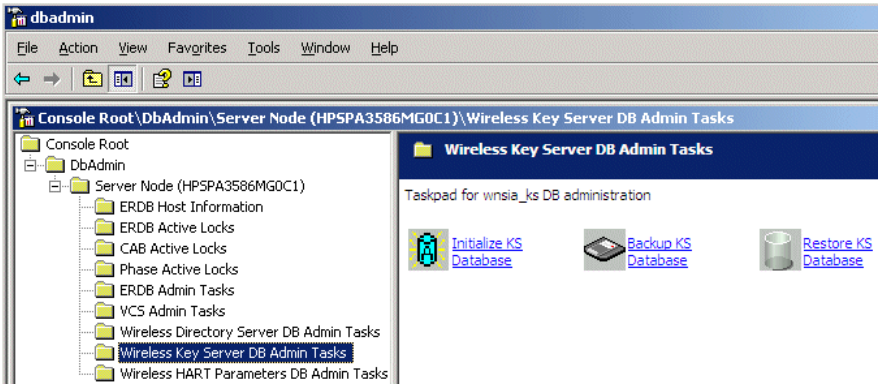
Click this Tree Pane Selection . . .	To Initiate This Function . . .
Experion Node (ERDB for control strategy)	Access ERDB Host Information, ERDB Active Locks, CAB Active Locks, Phase Active Locks, ERDB Admin Tasks, and VCS Admin Tasks folders.
Experion Node (EMDB for Experion system)	Access EMDB Host Information, EMDB Active Locks, and EMDB Admin Tasks folders.
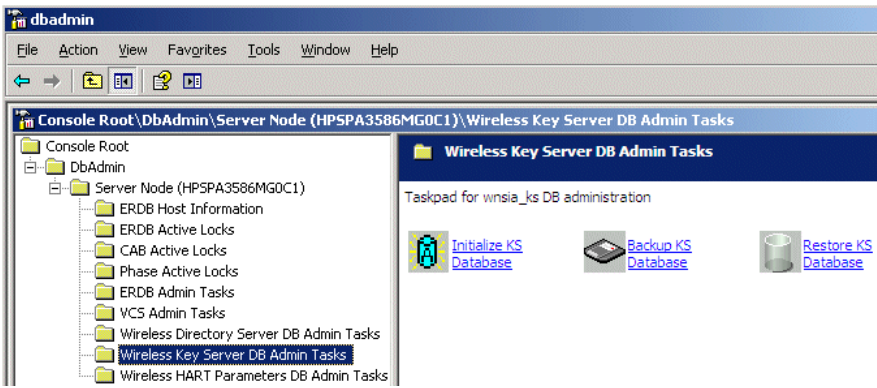
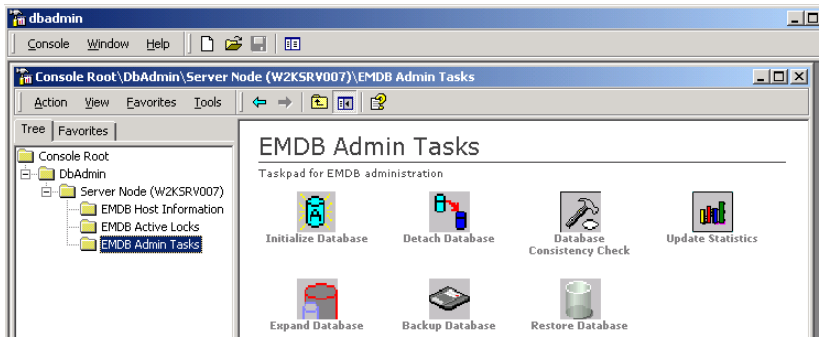| Click this Tree Pane Selection . . .	To Initiate This Function . . .
ERDB Host Information	Display host name, type, and status in the View pane.
EMDB Host Information	Display host name, type, and status in the View pane. Before clearing locks or performing database operations at a remote server node, insure that tasks such as Control Builder and Import/Export are shut down at that node.
ERDB Active Lock	Display active locks in the View pane. (Click **Tools-** > **Clear All Locks** or right-click in open area of view pane and select Clear All Locks from pop-up menu to clear current locks from the database.)

Click this Tree Pane Selection . . .	To Initiate This Function . . .
CAB Active Lock	Display active locks in the View pane. (Click **Tools-** > **Clear All Locks** or right-click in open area of view pane and select Clear All Locks from pop-up menu to clear current locks from CAB.) ![dbadmin console screenshot showing Console Root\DbAdmin\Server Node (W2KSRV007)\CAB Active Locks tree with CAB Active Locks selected and Object Name WHOCARES1, User Name W2KSRV007\ps_user]
Phase Active Lock	Display active locks in the View pane. (Click **Tools-** > **Clear All Locks** or right-click in open area of view pane and select Clear All Locks from pop-up menu to clear current locks from Phase.)
EMDB Active Locks	Display active locks in the View pane. (Click **Tools-** > **Clear All Locks** or right-click in open area of view pane and select Clear All Locks from pop-up menu to clear current locks from EMDB.)

Click this Tree Pane Selection . . .	To Initiate This Function . . .
ERDB Admin Tasks	Display the following Engineering Repository Database (ERDB) Admin Tasks as Icons in the View pane. There are additional tasks available for redundant Servers. • Initialize Database - Restores the Clean database (ps_erdb_clean.bak) in the Primary ERDB. • Detach Database - Shutdowns the database services, detaches the Primary ERDB, copies and attaches database to the c:\Temp directory location, re-attaches Primary ERDB and restarts database services. **❗ Attention** Though the Detach Database function copies the database files to a temporary location, you must be aware that you cannot reuse these files again with the DBADMIN utility. Please note that this function cannot be used for backing up purposes. • Database Consistency - Checks the consistency of the database and rebuilds indexes using the SQL Server. • Update Statistics - Runs the DBCC REINDEX to reorganize data and index pages followed by update statistics. • Expand Database - Expands the size of the database • Backup Database - Creates a backup copy of the current database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is c:\Program Files \Honeywell\Experion PKS\Engineering Tools\system\ER. The backup of the database is allowed only to a local (non-networked) location. • Restore Database - Restores the user selected backup database (*.bak) in the primary ERDB through the Restore From dialog box. The default directory is c:\Program Files \Honeywell\Experion PKS\Engineering Tools\system\ER.

Click this Tree Pane Selection . . .	To Initiate This Function . . .
	The following tasks are only available for Redundant Servers. • Recover Primary Database - Recovers Primary database from secondary database. If a valid Primary (master) ERDB exists, it merely resets the mastership ID so that the primary database is the Design Master. If the master ERDB no longer exists, the utility first makes the secondary database (at SERVERA) the master temporarily. Then it replicates this database to the primary (SERVERB). Finally, it switches mastership back to the new copy at SERVERB. • Recover Secondary Database - Recovers Secondary database from Primary database. It creates a new replica from the Design Master, which is assumed to be located at the path set by data source 'ps_erdb'. It creates the new replica at the server node previously specified during installation as the secondary ERDB server. • Enable Replication - Starts replication of the ERDB from the Primary to the Secondary. This enables replication from scratch. • Disable Replication - Stops the replication function completely. This is not a temporary interruption of the replication function.
VCS Admin Tasks	Display the following Qualification and Version Control System (QVCS) Admin Tasks as Icons in the View pane. • Synchronize VCS - Synchronizes the Qualification and Version Control System database with the Engineering Repository database and clears any QVCS locks. • Backup VCS Database - Creates a backup copy of the current QVCS database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER. • Restore VCS Database - Restores the user selected backup QVCS database (*.bak) in the primary ERDB through the Restore From dialog box. The default directory is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.

Click this Tree Pane Selection . . .	To Initiate This Function . . .
Wireless Directory Server DB Admin Tasks	Display the following Wireless Directory Server (DS) DB Admin Tasks as Icons in the View pane. • Initialize Database - Restores the Clean database (WNSIA_DS_Clean.bak) in the DS database. • Backup DS Database - Creates a backup copy of the current DS database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER. • Restore DS Database - Restores the user selected backup DS database (*.bak) in the DS database through the Restore From dialog box. The default directory is *c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.*
Wireless Key Server DB Admin Tasks	Display the following Wireless Key Server (KS) DB Admin Tasks as Icons in the View pane. • Initialize Database - Restores the Clean database (WNSIA_KS_Clean.bak) in the KS database. • Backup KS Database - Creates a backup copy of the current KS database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is *c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.* • Restore KS Database - Restores the user selected backup KS database (*.bak) in the KS database through the Restore From dialog box. The default directory is *c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.*

Click this Tree Pane Selection . . .	To Initiate This Function . . .
Wireless HART Parameters DB Admin Tasks	Display the following Wireless HART Parameters DB Admin Tasks as Icons in the View pane. • Initialize Database - Restores the Clean database (HARTParameters_clean.bak) in the wireless HART parameters database. • Backup wireless HART parameters Database - Creates a backup copy of the current HART parameters database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is *c:\Program Files\Honeywell\Experion PKS\Engineering Tools \system\ER.* • Restore wireless HART parameters Database - Restores the user selected backup HART parameters database (*.bak) in the HART parameters database through the Restore From dialog box. The default directory is *c:\Program Files\Honeywell\Experion PKS \Engineering Tools\system\ER.*

Click this Tree Pane Selection . . .	To Initiate This Function . . .
EMDB Admin Tasks	Display the following Enterprise Model Database (EMDB) Admin Tasks as Icons in the View pane. • Initialize Database - Restores the Clean database (epks_emdb_clean.bak) in the EMDB. • Detach Database - Shutdowns the database services, detaches the EMDB, copies and attaches database to the c:\Temp directory location, re-attaches EMDB and restarts database services. ⚠ **CAUTION** Though the Detach Database function copies the database files to a temporary location, you must be aware that you cannot reuse these files again with the DBADMIN utility. Please note that this function cannot be used for backing up purposes. • Database Consistency - Checks the consistency of the database and rebuilds indexes using the SQL Server. • Update Statistics - Runs the DBCC REINDEX to reorganize data and index pages followed by update statistics. • Expand Database - Expands the size of the database • Backup Database - Creates a backup copy of the current database as a '.bak' file under the user specified name and in the user selected directory location on a local drive through the Back To dialog box. A common directory location is c:\Program Files \Honeywell\Experion PKS\Engineering Tools\system\ER. • Restore Database - Restores the user selected backup database (*.bak) in the EMDB through the Restore From dialog box. The default directory is c:\Program Files \Honeywell\Experion PKS\Engineering Tools\system\ER.

11.2.2 Viewing Server information

Use the following procedure to view the information about the logged on Server. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.

1 Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2 Click ERDB Host Information folder.

General information about the logged on Server appears in the view pane. The following illustration shows a typical view for a non-redundant Server.

For Redundant Servers, information for both the Primary and Secondary Servers is shown.

3   Click **Tools-** > **Refresh** Status.
Updates Host information in the display to reflect current data.

4   This completes the procedure. Go to the next procedure Changing lock display filter or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.3 Changing lock display filter

Use the following procedure to change the User Filter to filter the lock display by user or bypass the filter by enabling All Users. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

2   Click the ERDB Active Locks or CAB Active Locks folder.
Selects the folder and activates lock menu selections.

3   Click **Tools-** > **User Filter**.
Calls up the Set the User ID for Lock Filtering dialog box.
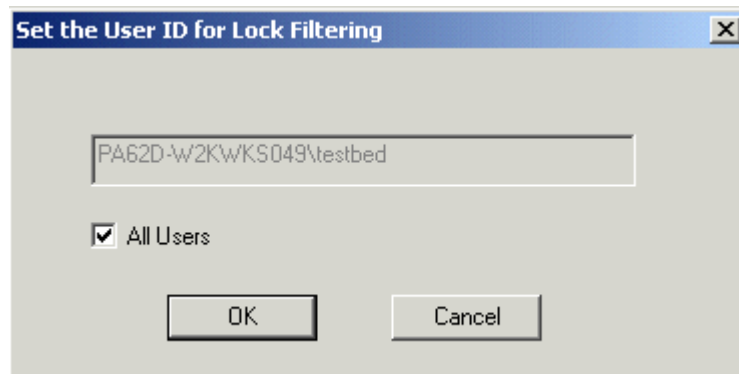
4   Click All Users checkbox.
Removes checkmark and disables the All Users function, and activates the User ID field.
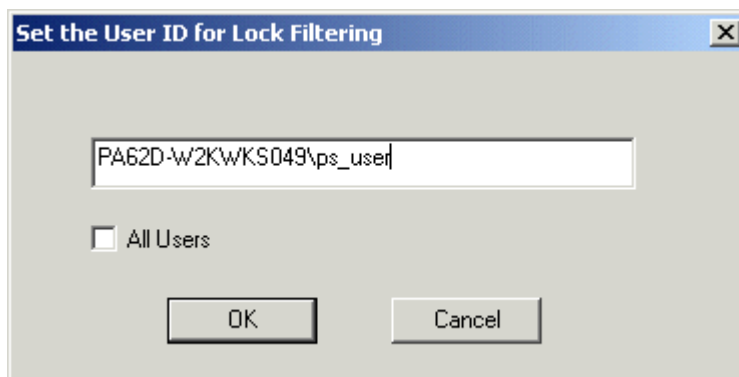
5   Key in desired Server name and/or user name for 'by user' lock display access. Click OK.
Closes the dialog box and enables lock display filter for specified user.

6   Repeat Steps 3 and 4.
Adds checkmark and enables the All Users (default) function and disables the filter mechanism.

7   Click OK.

Closes the dialog box and refreshes the lock display for all users.

8   This completes the procedure. Go to the next procedure *Clearing current locks* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.4 Clearing current locks

Use the following procedure to clear current locks in the database. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section and set the desired lock display filter as outlined in the prior procedure.

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2   Click the ERDB Active Locks, CAB Active Locks, or Phase Active Locks folder.

Selects the folder, activates lock menu selections, and displays current locks in the view pane.

3   Click **Tools-** > **Refresh** Locks.

Updates the display to make sure the view is current.

> **Tip**
> You can also right-click the cursor in an open area in the view pane and select Refresh Locks or Clear All Locks from the pop-up menu.

---

4   Click **Tools-** > **Clear All Locks**.

Clears current locks from the database and the view pane.

5   This completes the procedure. Go to the next procedure *Making a backup database* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

## 11.2.5 Making a Backup ERDB database

Use the following procedure to make a backup copy of the current ERDB database. This procedure assumes that you have started the DBADMIN utility as outlined in the previous **Startup** section.


> **Attention**
> It is a good idea to close the Control Builder application while running the DBADMIN utility.

---

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2   Click the ERDB Admin Tasks folder.

Calls up ERDB Admin Tasks in the view pane.

3   Are you using a redundant Server?

If the answer is **Yes**, go to the next Step.

If the answer is **No**, go to Step 6.

4   Be sure you are logged onto the Server with the Primary database.

Want to Backup the Design Master (Primary) database.

5   Click the Disable Replication icon.

Stops the replication function.

6   Click the Backup Database icon.

Calls up one of the following dialog boxes depending on QVCS license.

With QVCS license, **Select and/or Create a folder to store backup set** dialog - Go to Step 7:
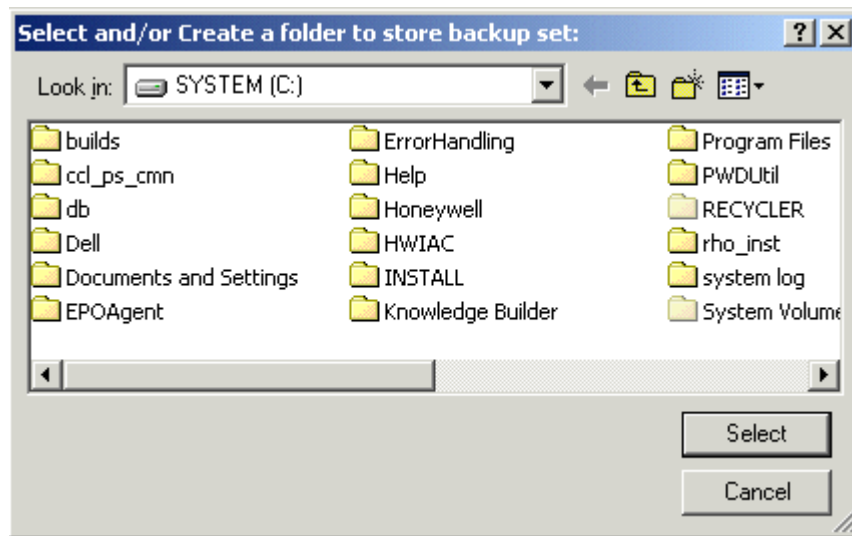
Without QVCS license, **Backup To** dialog - Go to Step 9:
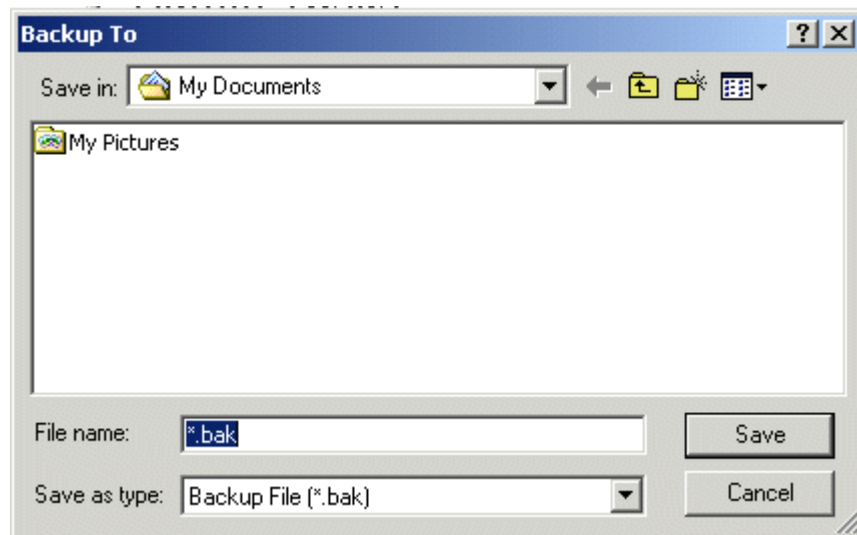
7   Click ▼ button in the Look in field to select the desired folder and/or use the folder buttons on the dialog to navigate to another folder or create a new folder.

Define location to backup database as complete set.

8   Click the Select button.

Calls up confirmation dialog, click the OK button to initiate the backup. Go to Step 11.

- Click ▼ button in the Save in field and select the desired directory location on a local drive from the drop-down menu. Common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.

- Key in desired file name in the File name field. For example, >ps_erdb_1.bak<.

Defines backup to location and backup database name. The following illustration is for example purposes only.
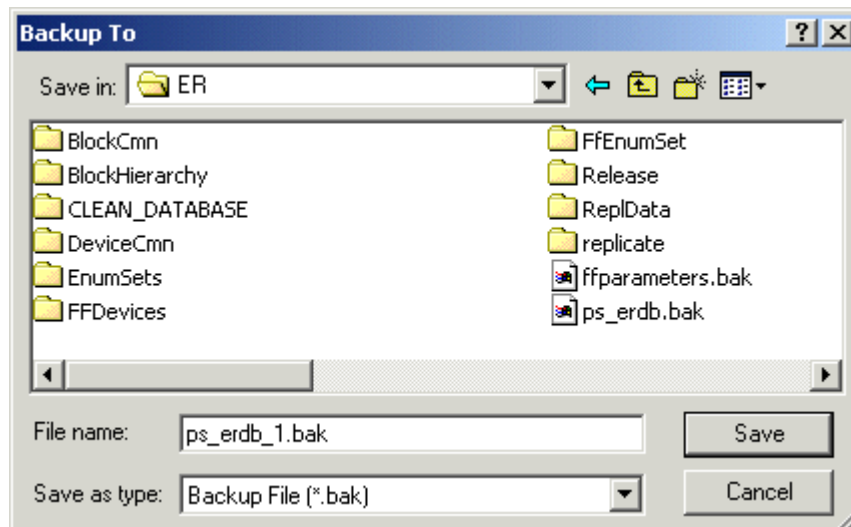
9 Click the Save button.

Imitates the backup function.

10 Wait for message prompt to announce the successful completion of the backup. Click the OK button.
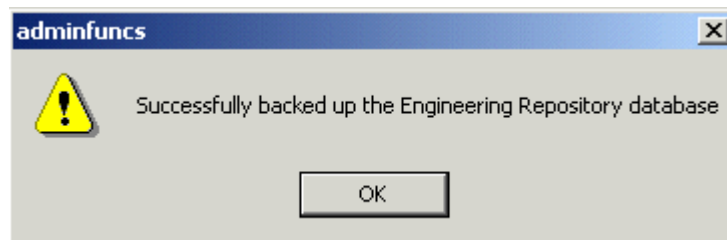
Acknowledges prompt.

11 This completes the procedure. Go to the next procedure *Restoring a backup database* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.6 Restoring a backup ERDB database

Use the following procedure to restore a backup ERDB database. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section and you have created a backup database as outlined in the prior procedure.

Attention

Disconnect all clients before initiating a database restore function.


Attention

Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be a temporary loss of view to both servers. View will be back once the servers are restarted, approximately one minute.

Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be temporary loss of view to both servers. View to the CEE points are restored once the 'ERDB to SR sync status' in the Server Redundancy page is set to 'Synchronized.'

Failover: If the recovery is performed on Server B without losing the hard drive, PC or powering it off, then upon database recovery on Server B, Server A will also fail over to Server B. This is to ensure both SRs are in Sync after the database recovery process.

To restore a backup ERDB database

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
    Expands the directory tree.

2   Click the ERDB Admin Tasks folder.
    Calls up ERDB Admin Tasks in the view pane.

3   Are you using a redundant Server?
    If the answer is **Yes**, go to the next Step.

    If the answer is **No**, go to Step 6.

4   Be sure you are logged onto the Server with Primary database.
    Want to restore the backup as the Design Master (Primary) database.

5   Click the Disable Replication icon.
    Stops the replication function.

6   Click the Restore Database icon.
   Prompt asks if replication is disabled and if you want to continue.
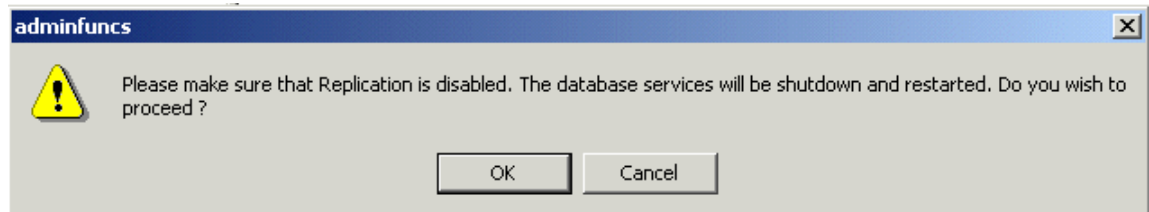
7   Click the OK button.
   Calls up the Restore From dialog box.
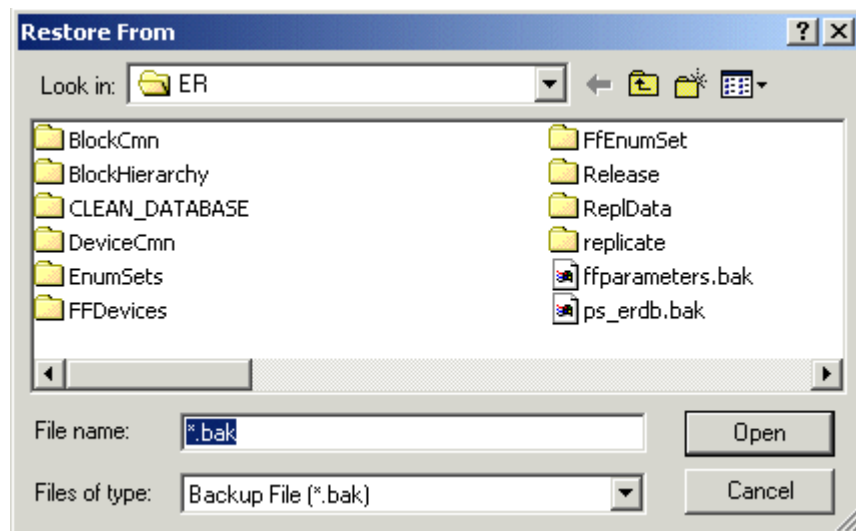
- Click ▼ button in the Look in field and select the desired directory location from the drop-down menu.
  Common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.

- Select the desired backup database (*.bak) in the list box, so it appears in the File name field. For
  example, >ps_erdb_1.bak<.

Selects the backup database to be restored.
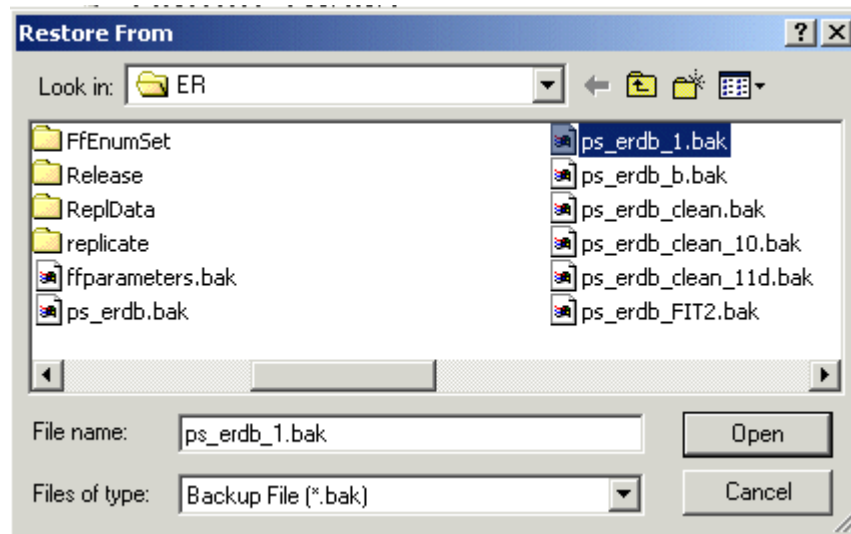
8   Wait for message prompt to announce the successful completion of the restore. Click the OK button.
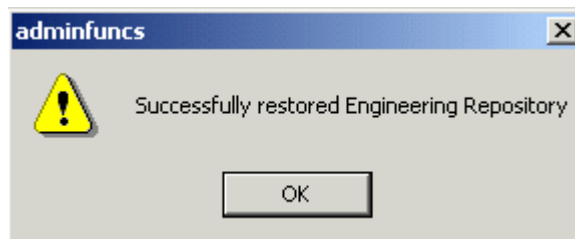
Acknowledges prompt.

9   This completes the procedure. Go to the next procedure *Restoring a clean database* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.7 Restoring 'clean' database

Use the following procedure to restore the 'clean' database that is provided with the Experion Engineering Tools software. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.

> **Attention**
>
> Disconnect all clients before initiating a database restore function.

> **Attention**
>
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be a temporary loss of view to both servers. View will be back once the servers are restarted, approximately one minute.
>
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be temporary loss of view to both servers. View to the CEE points are restored once the 'ERDB to SR sync status' in the Server Redundancy page is set to 'Synchronized.'
>
> Failover: If the recovery is performed on Server B without losing the hard drive, PC or powering it off, then upon database recovery on Server B, Server A will also fail over to Server B. This is to ensure both SRs are in Sync after the database recovery process.

To restore 'clean' database

1 Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

2 Click the ERDB Admin Tasks folder.
Calls up ERDB Admin Tasks in the view pane.

3 Are you using a redundant Server?
If the answer is **Yes**, go to the next Step.

If the answer is **No**, go to Step 6.

4 Be sure you are logged onto the Server with the Primary database.
Want to restore the clean database as the Design Master (Primary) database.

5 Click the Disable Replication icon.
Stops the replication function.

6 Click the Initialize Database icon.
Prompt asks if replication is disabled and if you want to continue.
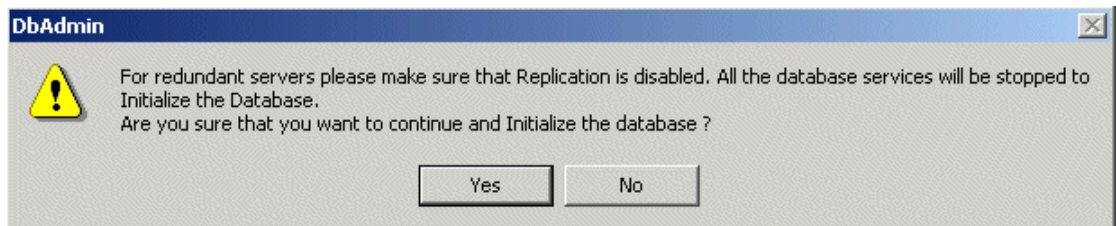
7 Click the Yes button to continue.
Prompt asks if you want to initialize the QVCS database as well.
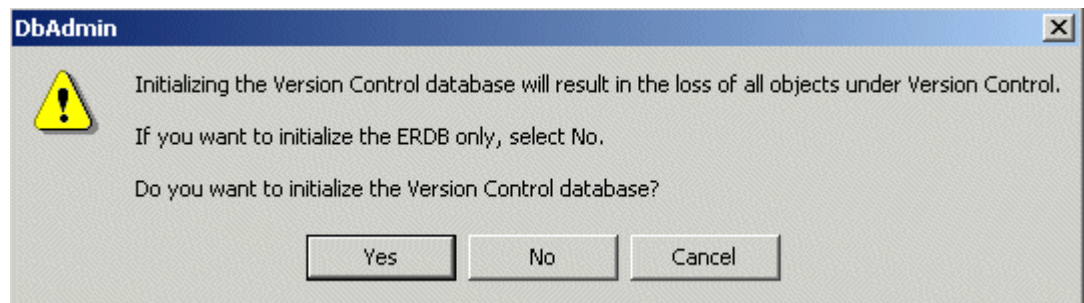
- To initialize the ERDB only, click the No button.
- To initialize both the ERDB and the QVCS database, click the Yes button.

Initiates the initialization function.

8 Wait for message prompt to announce the successful completion of the initialization. Click the OK button.
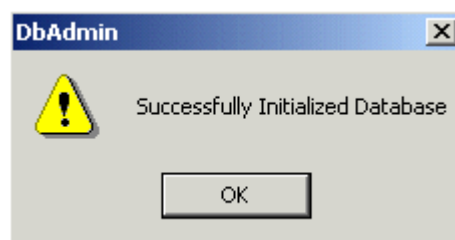
Acknowledges prompt.

9 Did you initialize the Primary database on a redundant Server?
If the answer is **Yes**, go to the next Step.

If the answer is **No**, go to Step 13.

10 Click the Recover Secondary Database icon.
Initializes the secondary database.

11 Wait for message prompt to announce the successful completion of the initialization. Click the OK button.
Acknowledges prompt.

12 This completes the procedure. Go to the next procedure *Detaching database* or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.8 Detaching database

Use the following procedure to detach and copy the database file to a specified location. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.
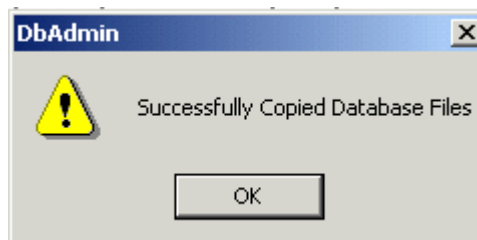
> **Attention**
> Disconnect all clients before detaching a database.

1 Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

2 Click the ERDB Admin Tasks folder.
Calls up ERDB Admin Tasks in the view pane.

3 Click the Detach Database icon.
Prompt asks if you want to continue.
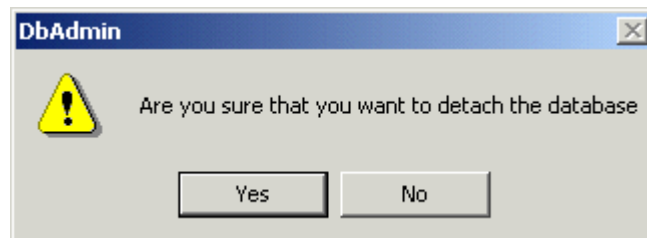
4 Click the Yes button.
Initiates the function that stops database services, detaches the database, copies files ps_erdb.mdf and ps_erdb_log.idf to the *c:\Temp* directory, re-attaches the database, and starts database services.

5 Wait for prompt to announce successful completion of the operation. Click the OK button.

Acknowledges prompt.

6 This completes the procedure. Go *to the next procedure Expanding database* or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.9 Expanding database

Use the following procedure to expand the database if more than 75% of the allocated hard-disk space is in use. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
    Expands the directory tree.

2   Click the ERDB Admin Tasks folder.
    Calls up ERDB Admin Tasks in the view pane.

3   Click the Expand Database icon.
    Prompt asks you to confirm the action.

4   Click the Yes button.
    Initiates the function.

5   Wait for prompt to announce the successful completion of the expansion. Click the OK button.
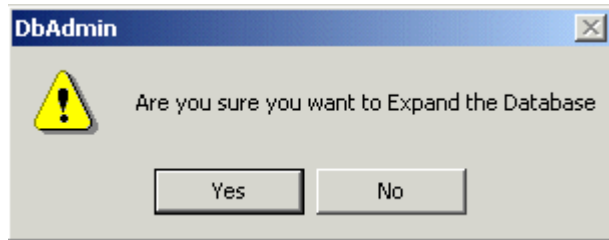   Acknowledges prompt.

6   This completes the procedure. Go to the next procedure *Recovering Primary database* or return to normal
    operation.
    Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.10 Recovering Primary ERDB database

Use the following procedure to recover a Primary ERDB database in a redundant Server application only. This
procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section on
the redundant Server running the Primary database.

> ❗ **Attention**
> Disconnect all clients before initiating a database recovery function.

> ❗ **Attention**
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will
> be a temporary loss of view to both servers. View will be back once the servers are restarted, approximately one
> minute.
>
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will
> be temporary loss of view to both servers. View to the CEE points are restored once the 'ERDB to SR sync status' in
> the Server Redundancy page is set to 'Synchronized.'
>
> Failover: If the recovery is performed on Server B without losing the hard drive, PC or powering it off, then upon
> database recovery on Server B, Server A will also fail over to Server B. This is to ensure both SRs are in Sync after
> the database recovery process.

To recover primary ERDB database

1   Click the Start button in the taskbar. Click **Settings-** > **Control Panel**
    Opens Control Panel window.

2   Double-click Administrative Tools folder 🗂 Administrative Tools .
    Opens Administrative Tools window

3   Double-click Services icon 🗇 Services .
    Opens Services window.

4   Scroll the list box to find the Experion System Repository service. Double-click this service.
    Opens the Experion System Repository Properties dialog box.

5   Click the Stop button.

Initiates service shutdown.

6   Wait for service status to change to stopped. Click the OK button.

Closes the dialog box.

7   Close the Services, Administrative Tools, and Control Panel windows.

Completes tasks.

8   In dbadmin window, click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

9   Click the ERDB Admin Tasks folder.

Calls up ERDB Admin Tasks in the view pane.

10   Click the Recover Primary Database icon.

Prompt asks if you want to continue.

11   Click the Yes button.

Initiates function to backup the Secondary database and use it to restore the Primary database.

12   Wait for prompt to announce the successful completion of the action. Click the OK button.

Acknowledges prompt.

13   Repeat Steps 1 to 8, modifying Step 5 to click the **Start** button.

Starts Experion database services.

14   This completes the procedure. Go to the next procedure *Recovering Secondary database* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.11 Recovering Secondary ERDB database

Use the following procedure to recover a Secondary ERDB database in a redundant Server application only. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section on the redundant Server running the Primary database.

> ❗ **Attention**
> Disconnect all clients before initiating a database recovery function.

> ❗ **Attention**
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be a temporary loss of view to both servers. View will be back once the servers are restarted, approximately one minute.
>
> Loss of View: While following restoration/recover procedures for Primary database and Secondary database, there will be temporary loss of view to both servers. View to the CEE points are restored once the 'ERDB to SR sync status' in the Server Redundancy page is set to 'Synchronized.'
>
> Failover: If the recovery is performed on Server B without losing the hard drive, PC or powering it off, then upon database recovery on Server B, Server A will also fail over to Server B. This is to ensure both SRs are in Sync after the database recovery process.
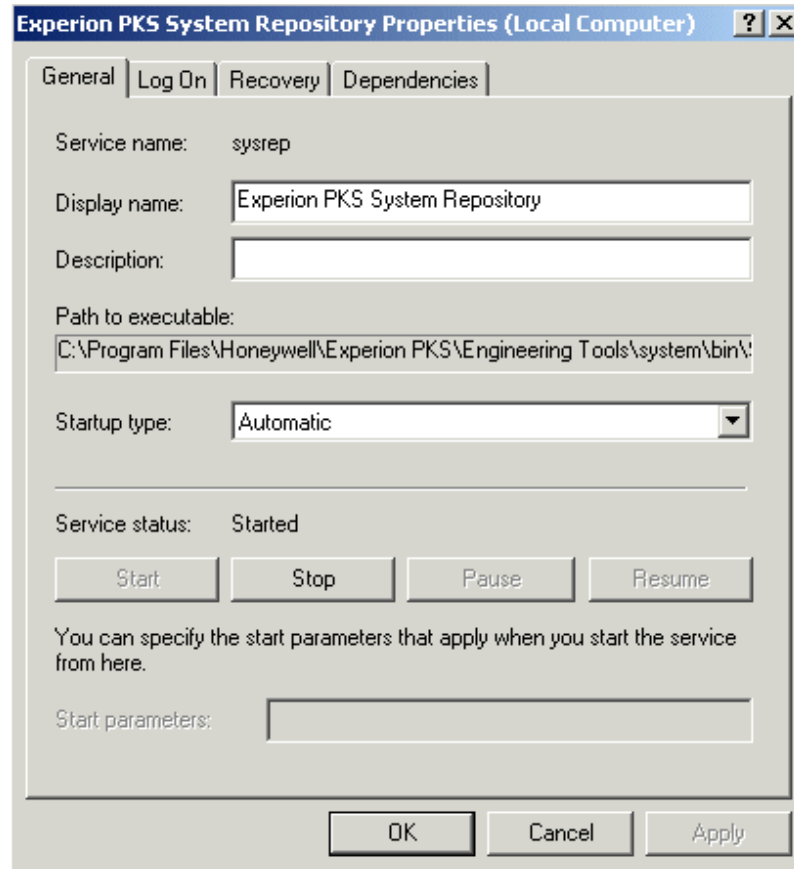
To recover secondary Primary ERDB database

1   Click the Start button in the taskbar. Click **Settings-** > **Control Panel**

Opens Control Panel window.

2   Double-click Administrative Tools folder 🗐 Administrative Tools .

Opens Administrative Tools window

3   Double-click Services icon

.
Opens Services window.

4   Scroll the list box to find the Experion System Repository service. Double-click this service.
Opens the Experion System Repository Properties dialog box.

5   Click the Stop button.
Initiates service shutdown.

6   Wait for service status to change to stopped. Click the OK button.
Closes the dialog box.

7   Close the Services, Administrative Tools, and Control Panel windows.
Completes tasks.

8   In dbadmin window, click the ⊞ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

9   Click the ERDB Admin Tasks folder.
Calls up ERDB Admin Tasks in the view pane.

10 Click the Recover Secondary Database icon.
Prompt asks if you want to continue.

11 Click the Yes button.
Initiates function to backup the Primary database and use it to restore the Secondary database.

12 Wait for prompt to announce the successful completion of the action. Click the OK button.
Acknowledges prompt.

13   Repeat Steps 1 to 8, modifying Step 5 to click the **Start** button.

Starts Experion database services.

14   This completes the procedure. Go to the next procedure *Enabling replication* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.12 Enable replication failed

In the process of restoring Server B from a hardware failure or a failure due to a corrupted database, the following error message is displayed from the DBAdmin tool after Server B recovery:

```
Enable Replication: Unable to compare the primary and secondary database IDs to ensure that they
are in synch.
Make sure the Database Services are started.
Cannot Enable Replication.
```

Cause

The DBAdmin tool has improperly formed database connection strings to the ERDB. Therefore, the DBAdmin tool fails to connect to the ERDB to perform the **Enable Replication** operation.

Solution

If you encounter this error, perform the following tasks to resolve the issue:

1.   Close the DBAdmin tool and the Configuration Studio applications.

2.   Reopen the DBAdmin tool, and select **Enable Replication**.

> **Tip**
> To avoid this error, ensure that you open the DBAdmin tool only after all Server B recovery operations have completed successfully.

11.2.13 Enabling replication

Use the following procedure to initiate the replication function in a redundant Server application only. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section on the redundant Server running the Primary database.

1   Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2   Click the ERDB Admin Tasks folder.

Calls up ERDB Admin Tasks in the view pane.

3   Click the Recover Secondary Database icon.

Prompt asks if you want to continue.

4   Click the Yes button.

Initiates function to backup the Primary database and use it to restore the Secondary database. This action **synchronizes** the databases in preparation for replication.

5   Wait for prompt to announce the successful completion of the action. Click the OK button.

Acknowledges prompt.

6   Click the Enable Replication icon.

Initiates replication of the database from the Primary to the Secondary. It sets up and starts the SQL server jobs to do the replication.

7   Wait for prompt to announce the successful completion of this operation. Click the OK button.

Acknowledges prompt.

8   This completes the procedure. Go to the next procedure *Disabling replication* or return to normal operation.

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.14 Disabling replication

Use the following procedure to stop the replication function and delete the configured replication setup. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section on the redundant Server running the Primary database.

1 Click the ➕ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

2 Click the ERDB Admin Tasks folder.
Calls up ERDB Admin Tasks in the view pane.

3 Click the Disable Replication icon.
Prompt asks if you want to continue.

4 Click the Yes button.
Stops the replication jobs and deletes the configured replication setup.

5 Wait for prompt to announce the successful completion of the action. Click the OK button.
Acknowledges prompt.

6 This completes the procedure. Go to the next procedure *Initiating QVCS database synchronization* or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.15 Initiating QVCS database synchronization and clearing locks

Use the following procedure to synchronize the QVCS database with the ERDB and clear any QVCS locks. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section.

> **Attention**
> It is a good idea to close the Control Builder application while running the DBADMIN utility.

1 Click the ➕ sign for the DbAdmin and Server Node (servername) folders.
Expands the directory tree.

2 Click the VCS Admin Tasks folder.
Calls up VCS Admin Tasks in the view pane.

3 Click the Synchronize VCS icon.
Prompt asks if you want to synchronize VCS database with the ERDB.

4 Click the Yes button.
Imitates the synchronization function and clears any VCS locks.

5 Wait for message prompt to announce the successful completion of the synchronization. Click the OK button.

Acknowledges prompt.

6 This completes the procedure. Go to the next procedure *Making a backup QVCS database* or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

11.2.16 Making a Backup QVCS, DS, KS, or HART Parameters database

Use the following procedure to make a backup copy of the current QVCS, DS, KS, or HART Parameters database. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section. It is based on backing up a QVCS database, but it can be easily adapted to backing up a wireless DS, KS, or HART Parameters database by selecting the applicable icon in the directory.

> ❗ **Attention**
>
> It is a good idea to close the Control Builder application while running the DBADMIN utility.

1 Click the ➕ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2 Click the VCS Admin Tasks folder.

Calls up VCS Admin Tasks in the view pane.

3 Click the Backup VCS Database icon.

Calls up the Backup To dialog box.
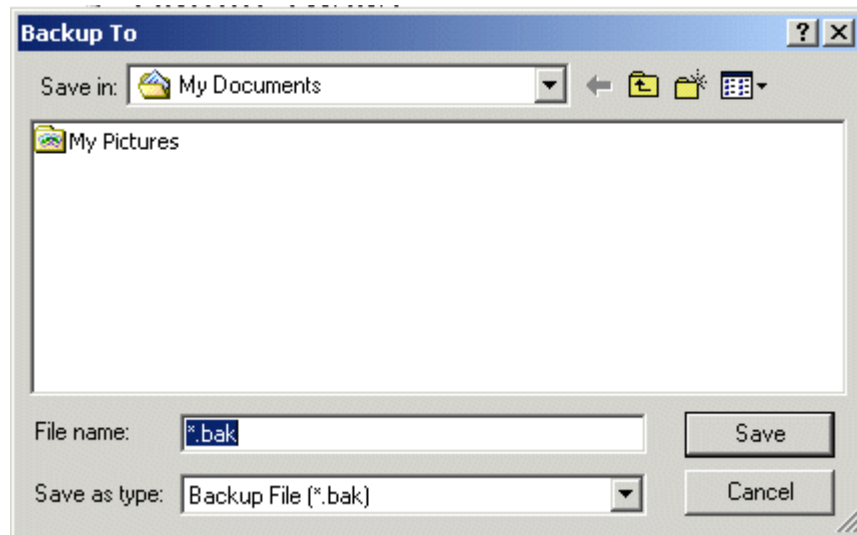
- Click ▼ button in the Save in field and select the desired directory location on a local drive from the drop-down menu. Common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.

- Key in desired file name in the File name field. For example, >versioncontrol_1.bak<.

Defines backup to location and backup database name. The following illustration is for example purposes only.

4 Click the Save button.

Imitates the backup function.

5 Wait for message prompt to announce the successful completion of the backup. Click the OK button.
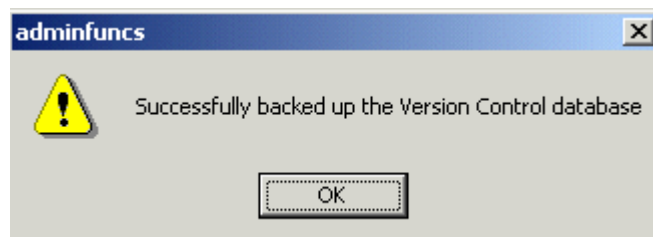
Acknowledges prompt.

6 This completes the procedure. Go to the next procedure *Restoring a backup QVCS database* or return to normal operation..

Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

## 11.2.17 Restoring a backup QVCS, DS, KS, or HART Parameters database

Use the following procedure to restore a backup QVCS, DS, KS or HART Parameters database. This procedure assumes that you have started the DBADMIN utility as outlined in the previous *Startup* section and you have created a backup database as outlined in the prior procedure. It is based on restoring a backup QVCS database, but it can be easily adapted to restoring a backup wireless DS, KS, or HART Parameters database by selecting the applicable icon in the directory.

> **Attention**
>
> Disconnect all clients before initiating a database restore function.

1 Click the ⊞ sign for the DbAdmin and Server Node (servername) folders.

Expands the directory tree.

2 Click the VCS Admin Tasks folder.

Calls up VCS Admin Tasks in the view pane.

3 Click the Restore VCS Database icon.

Prompt asks if replication is disabled and if you want to continue.

4 Click the OK button.
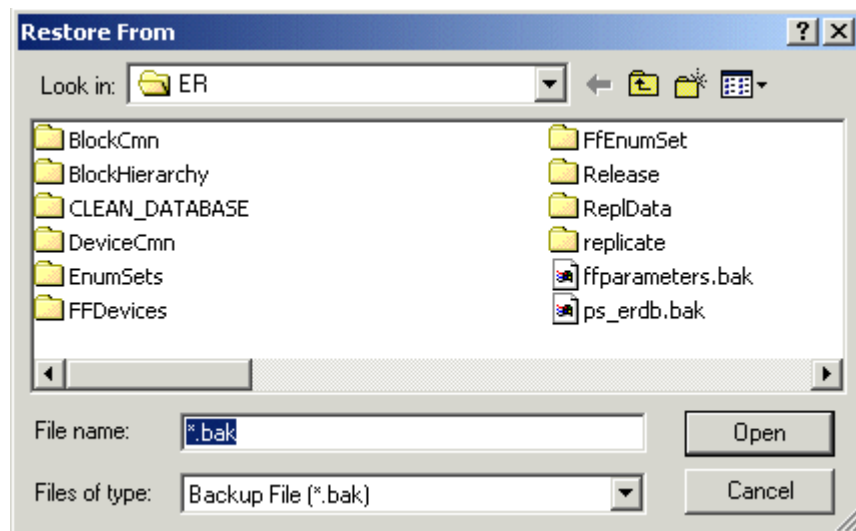
Calls up the Restore From dialog box.
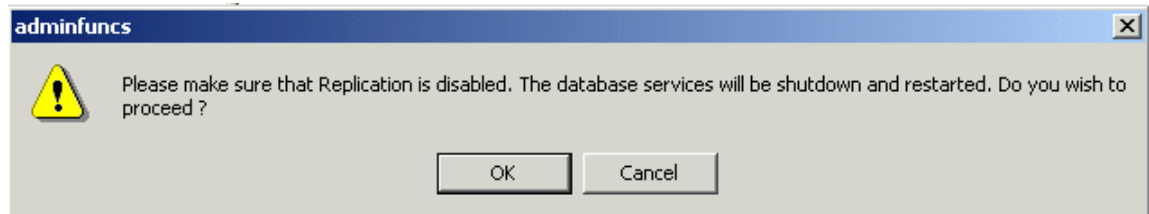

- Click ▼ button in the Look in field and select the desired directory location from the drop-down menu. Common directory location is c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\ER.
- Select the desired backup database (*.bak) in the list box, so it appears in the File name field. For example, >versioncontrol_1.bak<.

Selects the backup database to be restored. The following illustration is for example purposes only.
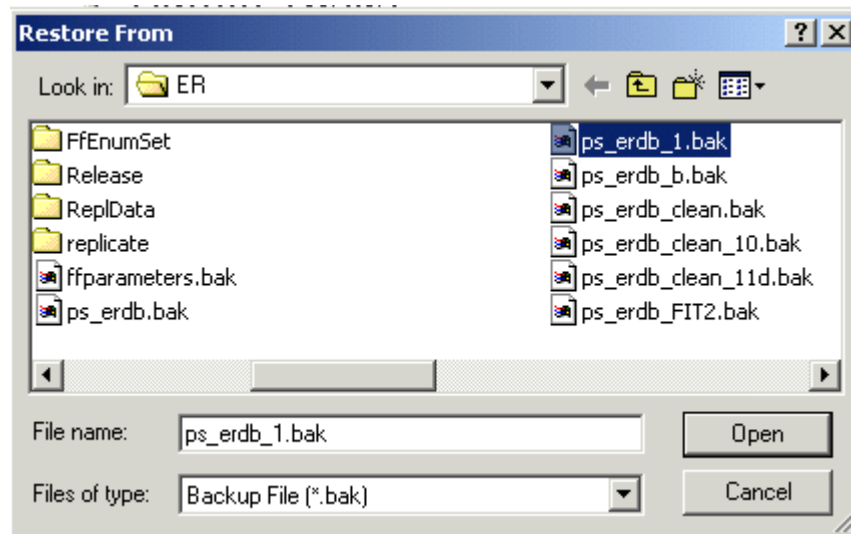
5   Wait for message prompt to announce the successful completion of the restore. Click the OK button.
Acknowledges prompt.

6   This completes the procedure. Go to another procedure or return to normal operation.
Click **Console-** > **Exit** to close dbadmin window and return to normal operation.

12 Series CSeries C Firmware Load Tool (CTool) for Series C Components

The Series C Firmware Load Tool (CTool) utility lets you efficiently upgrade firmware in Series C components with minimal user interaction, as reflected by the features listed below.

- Uses color-coded display of firmware versions for quick identification of obsolete or old firmware.
- Uses one button to select all modules with old firmware for upgrading.
- Uses one button to activate automatic loading of firmware to multiple devices.
- Shows status of modules including online detection of network changes such as added module, removed module, and cable removed as well as firmware upgrade progress.
- Provides protection against updating nodes while on-control.

12.1 CTool user interface description

The following figure and associated table describe the user interface components of the CTool utility.

Callout	Function	Description
1	+ / - icon	• Click the plus sign to expand the submenu to show all the components linked to the top level device. • Click the minus sign to collapse the submenu.
2	Check Box	• Select to choose the module for firmware upgrade or diagnostic data capture. • Clear to **not** choose the module for firmware upgrade or diagnostic data capture.
3	Index	The module's Device Index setting.
4	Address	The module's IP address or its I/O Link address.
5	Tagname	The configured tag name for the module in Control Builder.
6	Type	The type of Series C form factor component.
7	State	The current operating state of the module.
8	Boot Ver	The module's current version of Boot firmware that is displayed using the following color coding scheme. • **Red** - The module type is recognized, however, the device firmware version/revision is obsolete and no longer supported. • **Green** - The module type is recognized and the device firmware version/revision is associated with the current release of Experion. • **Blue** - The module type is recognized and the device firmware version/revision is interoperable with the current release of Experion, however, it is *not* the most recent version/revision of the firmware but it is still supported. • **Black** - The loading of this module type is *not* supported by the CTool utility.

Callout	Function	Description
9	App Ver	The module's current version of Application firmware that is displayed using the same color coding scheme noted in the previous row.
10	Progress	The progress of the current operation in percentage completed.
11	Status	The status of the current operation.
12	Check/Uncheck	Click this button to alternately select or clear the check boxes for all devices that have old firmware. This only works for devices that have old firmware. It does not select the check box for device with current or compatible firmware. You can manually select an individual check box at any time regardless of firmware condition.
13	Load FW	Click this button to initiate an automatic load of firmware to all devices with a selected check box. This function loads the current Release firmware as specified in the ver_rev.txt file for the given module/model. The usual default directory location for the ver_rev.txt file is: `C:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\bin`
14	System Prefs	Click this button to optionally change the default path to the Control File (*.lcf) firmware to use when upgrading firmware in a single device.
15	Refresh Grid	Click this button to update the contents of the module listing table.
16	Diagnostic	Click this button to open the **Diagnostic Capture** dialog to initiate a crash block or user log diagnostic information capture for the selected module. Can only run diagnostic check on one module at a time.
17	Abort Load	Click this button to stop the firmware load function. The modules already upgraded will **not** revert to the old firmware and the current module firmware download will be completed before the load function is stopped.
18	Exit	Click this button to close the CTool window. If you click this button while a firmware upgrade is in progress, the CTool utility wil complete the ongoing process before it closes.
19	Status Message Box	Provides real-time status information for monitoring the load operation.

12.2 CTool menu functions

The following table outlines the functions you can initiate using the CTool menu selections. Note that the **Edit** and **Options** menus selections also apply when viewing data in the **History Log** window.

Menu	Selection	Function
File	Save	Save the module listing table into a fixed format file with name and storage location of your choice.
	Print . . . Ctrl+P	Print a copy of the displayed module listing table.
	Exit	Stop the CTool utility and close its window.
Edit	Cut Ctrl+X	With the **Allow Cell Selection** option enabled, provides the same function as the Copy operation below. You cannot cut data from the module listing table.
	Copy Ctrl+C	With the **Allow Cell Selection** option enabled, copy selected row(s) or column(s) for pasting into another application such as Microsoft Word. Use standard Windows based shortcut keys and mouse operations to select multiple rows and/or columns for copying such as **Shift**+Click and Click and drag.
	Paste Ctrl+V	This function is not applicable, since you cannot paste information into the module listing table.
	Select All Ctrl+A	With the **Allow Cell Selection** option enabled, select all data in the module listing table for copying.
Options	Cell Selecting	Select (check mark) **Allow Cell Selection** to permit selection of row(s) and column(s) in the module listing table or clear (no check mark) to disable selection of row(s) and column(s) in the table.
	Grid Lines	Select (check mark) **Show Horizontal Lines** to include horizontal grid lines in the module listing table or clear (no check mark) to remove horizontal grid lines from the table.
		Select (check mark) **Show Vertical Lines** to include vertical grid lines in the module listing table or clear (no check mark) to remove vertical grid lines from the table.
	Grid Options	Select (check mark) **Enable Title Tips** to enable pop up showing full text when cursor is moved over truncated table entry or clear (no check mark) to disable pop ups.
		Select (check mark) **Track Focus Cell** to enable shadow showing current row and column selected or clear (no check mark) to disable shadow.
		Select (check mark) **Frame Focus Cell** to show a frame around the currently selected cell in the module listing table or clear (no check mark) to not show a frame.
		Select (check mark) **Fixed Cell Italic** to display cell headings text in italics or clear (no check mark) to display cell headings in standard text.

Menu	Selection	Function
Select (check mark) **Fixed cells have Vertical Text** to display cell headings in vertical plane instead of horizontal one or clear (no check mark) to display headings in horizontal plane.		
List Mode	Select (check mark) **Use List Mode** to enable list mode or clear (no check mark) to disable list mode. With **Use List Mode** enabled, click anywhere in a row to select the entire row.	
	When **Use List Mode** is enabled, select **Single Selection Mode** to enable single selection only or clear (no check mark) to disable single selection mode. With **Single Selection Mode** enabled, you cannot use shortcut keys to select multiple rows at one time.	
Resizing	Select (check mark) **Allow Row Resizing** to allow rows to be resized in the module listing table or clear (no check mark) to disable row resizing. You can resize a row by moving the cursor over the grid line in the header row so it changes to a double ended arrow and then clicking and dragging the grid line to the desired position.	
	Select (check mark) **Allow Column Resizing** to allow columns to be resized in the module listing table or clear (no check mark) to disable column resizing. You can resize a column by moving the cursor over the grid line in the header column so it changes to a double ended arrow and then clicking and dragging the grid line to the desired position.	

Menu	Selection	Function
Help	About CTools	Calls up the **About Series C Hardware Tool** dialog that displays CTool version information.

12.3 Using CTool to upgrade firmware

Refer to the *Upgrading Firmware in Series C Components* section in the Control Hardware and I/O Module Firmware Upgrade Guide for details about using CTool to upgrade firmware in Series C components.

12.4 Using CTool to capture diagnostic data or view history log

You can use the CTool utility to capture crash block or user log diagnostic data associated with a given Series C device as well as view history log data. You need remember the following while using the CTool utility.

- You must run one instance of CTool on either the primary or backup Experion server.
- The first time you launch the CTool utility it may take up to 40 seconds before the Series C devices on the network appear in the module listing table.
- The CTool detects when modules are added or removed as well as when I/O Link cables are added or removed, which affect the presence of I/O Modules.
- You can click the **Save User Log** button on the **Diagnostic Capture** dialog to save a user readable file listing firmware download data to a directory location of your choice.
- You can click the **Save Data** button on the **Diagnostic Capture** dialog to save a crash information file to a directory location of your choice that can be transferred to Honeywell TAC for fault analysis.

Prerequisites

- You have installed the Experion R300.1 software, configured the base IP address as well as addresses for time servers through the **System Preferences** selection in the Control Builder's **Tools** menu, and set the Device Index number for each C300 and FIM4 through the Binary Coded Decimal switches on its input/ output termination assembly (IOTA).
- You have configured and loaded all C300 blocks, since Series C I/O Modules are only shown in CTool when the I/O Link is configured and loaded.

To capture diagnostic data using CTool

1   Use the following procedure as a guide to capture diagnostic data for the selected Series C device. This data will help the Honeywell Technical Assistance Center (TAC) diagnose the cause of any premature failure of a given Series C component.

   a   Click **Start** on the task bar and choose **Run** to open the **Run** dialog.

   b   Click the **Browse** button to open the **Browse** dialog.

   c   Navigate to this directory location: *C:\Program Files\Honeywell\Experion PKS\Engineering Tools \system\Firmware\CTools*.

   d   Select the CTools.exe file so it appears in the **File Name** field and click the **Open** button to close the **Browse** dialog.

   e   Click the **OK** button to launch the CTool application and close the **Run** dialog.

2   Wait for the module listing table to appear in the **CTool** window.
For C300 devices, click the plus sign in the first table column to expand the table listing to show the C300's configured I/O Links and associated Series C I/O Modules, as shown in the following example illustration excerpt of the module listing table.

|		Index	Addr	Tagname	Type	State	Boot Ver	App Ver
⊟	☐	11	192.168.0.11	C300_133	C300	IDLE	EXP300.1-15.0	EXP300.1-15.0
			Link 1	IOLINK_135		ONLINE(SeriesCIO)		
	☐		1A		AI_HART	Not_Config	01.01.14	01.01.14
	☐		2A		AO_HART	Not_Config	01.01.14	01.01.14
	☐		3A		DI_24	Not_Config	01.01.11	01.01.14
	☐		4A		DO_24B	Not_Config	01.01.11	01.01.14
			Link 2	IOLINK_136		ONLINE(None)		

3   Click the check box for the Series C device in the module listing table that you want to capture diagnostic information about to select it and go to Step 4. Or, Right-click in the row for the Series C device in the module listing table that you want to capture diagnostic information about to open the shortcut menu, Select **Capture** > **Upload** to call up the **Diagnostic Capture** dialog, as shown in the following illustration, and go to Step 5.

4   Click the **Diagnostic** button to call up the **Diagnostic Capture** dialog, as shown in the following illustration.
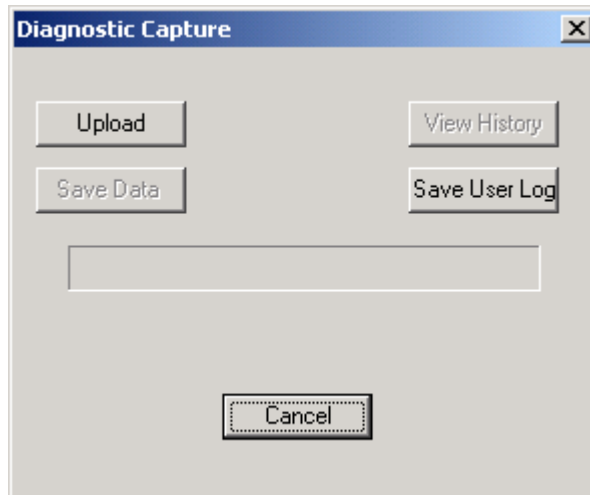
5   Click the **Upload** button to make **Save Data** and **View History** buttons available, once the upload is completed.
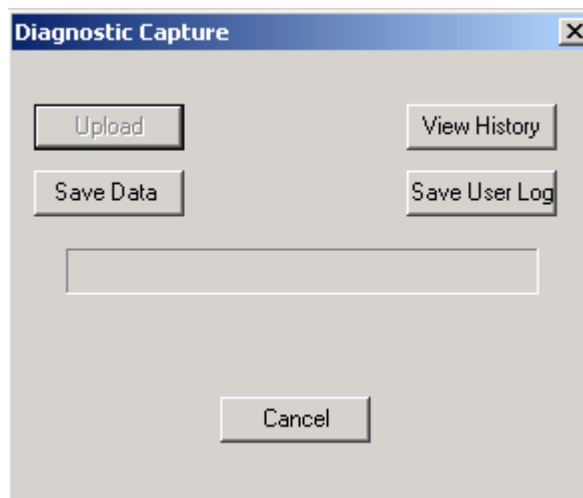
6   Click the **Save User Log** button to call up the **Open** dialog, as shown in the following illustration. Navigate to the directory/folder location where you want to store the user log file, double-click the selected folder so its name appears in the **Look in** field, key in the desired name for the .LOG file in the **File name** field, and click the **Open** button to save the file to the selected directory location.
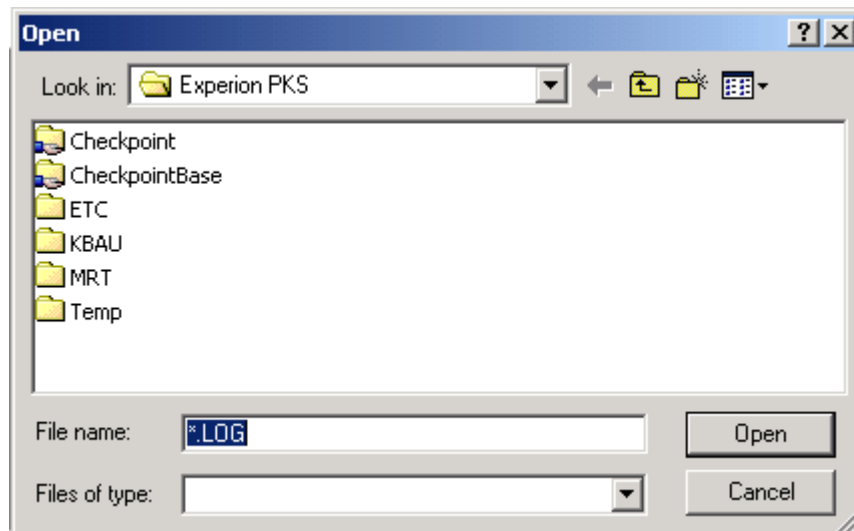
7 Click the **Save Data** button to call up the **Open** dialog. Navigate to the directory/folder location where you want to store the capture file, double-click the selected folder so its name appears in the **Look in** field, key in the desired name for the capture (.CAP) file in the **File name** field, and click the **Save** button to save the file to the selected directory location.

8 Click the **OK** button to acknowledge the Save complete message.
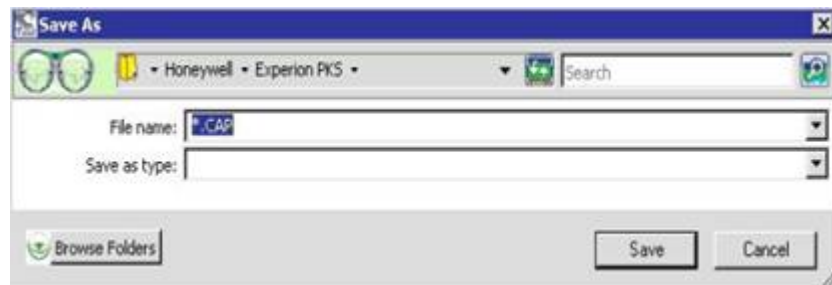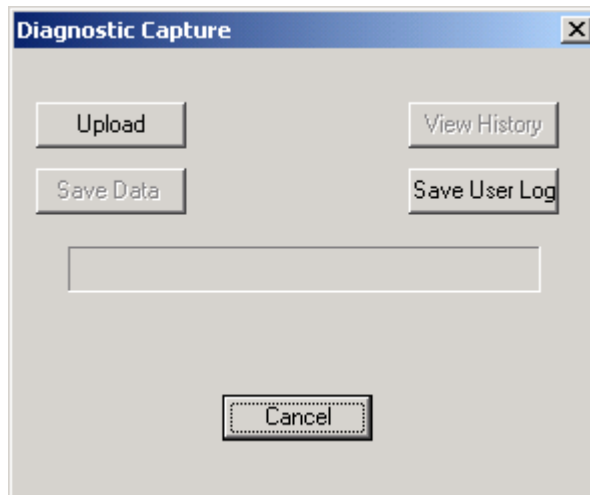

9 Click the close button icon ⊠ in the upper right-hand corner of the dialog to close the **Diagnostic Capture** dialog.

To view history log

1 Use the following procedure as a guide to capture diagnostic data for the selected Series C device. This data will help the Honeywell Technical Assistance Center (TAC) diagnose the cause of any premature failure of a given Series C component.

    a Click **Start** on the task bar and choose **Run** to open the **Run** dialog.

    b Click the **Browse** button to open the **Browse** dialog.

    c Navigate to this directory location: *C:\Program Files\Honeywell\Experion PKS\Engineering Tools \system\Firmware\CTools*.

    d Select the CTools.exe file so it appears in the **File Name** field and click the **Open** button to close the **Browse** dialog.

    e Click the **OK** button to launch the CTool application and close the **Run** dialog.

2 Wait for the module listing table to appear in the **CTool** window.

For C300 devices, click the plus sign in the first table column to expand the table listing to show the C300's configured I/O Links and associated Series C I/O Modules, as shown in the following example illustration excerpt of the module listing table.

		Index	Addr	Tagname	Type	State	Boot Ver	App Ver
⊟	☐	11	192.168.0.11	C300_133	C300	IDLE	EXP300.1-15.0	EXP300.1-15.0
			Link 1	IOLINK_135		ONLINE(SeriesCIO)		
	☐		1A		AI_HART	Not_Config	01.01.14	01.01.14
	☐		2A		AO_HART	Not_Config	01.01.14	01.01.14
	☐		3A		DI_24	Not_Config	01.01.11	01.01.14
	☐		4A		DO_24B	Not_Config	01.01.11	01.01.14
			Link 2	IOLINK_136		ONLINE(None)		

3   Click the check box for the Series C device in the module listing table that you want to capture diagnostic information about to select it and go to Step 4. Or, Right-click in the row for the Series C device in the module listing table for which you want to view the history log to open the shortcut menu, Select **History** > **Log** to call up the **Diagnostic Capture** dialog, as shown in the following illustration, and go to Step 5.

4   Click the **Diagnostic** button to call up the **Diagnostic Capture** dialog, as shown in the following illustration.

5   Click the **Upload** button to make **Save Data** and **View History** buttons available.

6 Click the **View History** button to call up the **History Log** window, as shown in the following illustration.
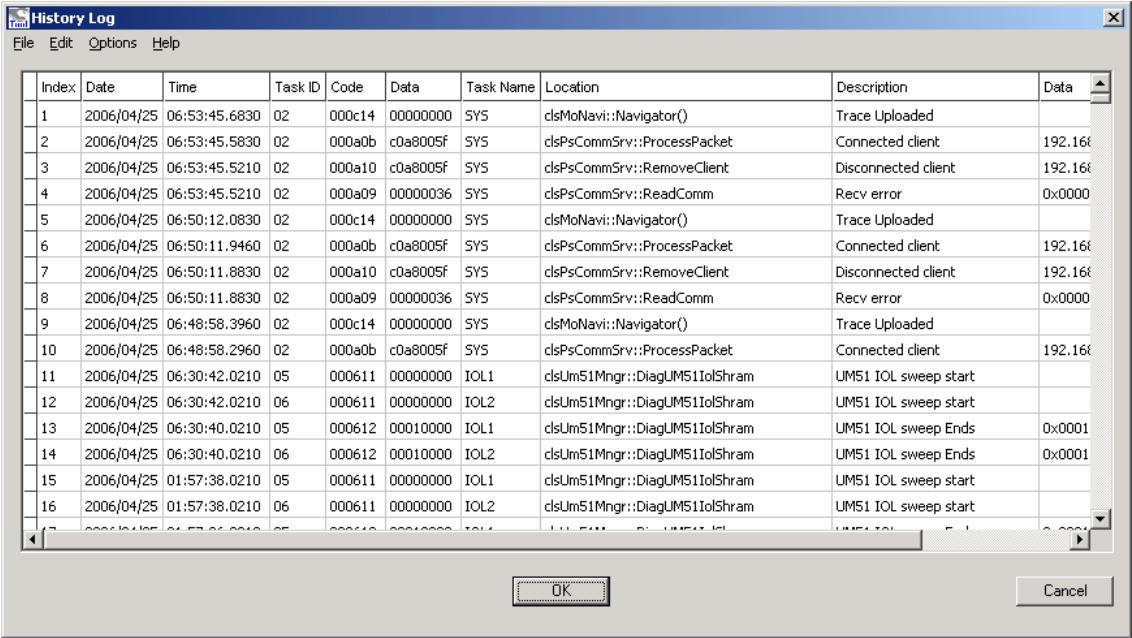
7 Click the **OK** button to close the **History Log** window.

8 Click the close button icon ✕ in the upper right-hand corner of the dialog to close the **Diagnostic Capture** dialog.

12.5 Fixing Common Problems with CTool
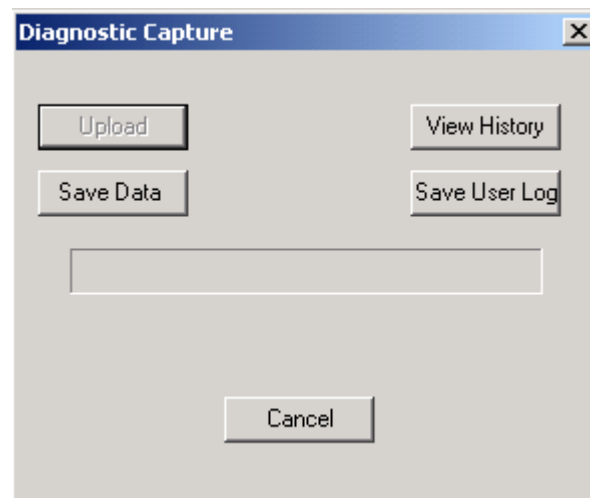
This section identifies some common problems and describes how you might fix them.

Related topics

"Database could not be contacted" on page 605

12.5.1 Database could not be contacted

The CTool utility cannot connect to the database to populate the module listing table.

Diagnostic check

- *The Database Could not be contacted* message appears in the status message box.
- The following Error dialog appears.
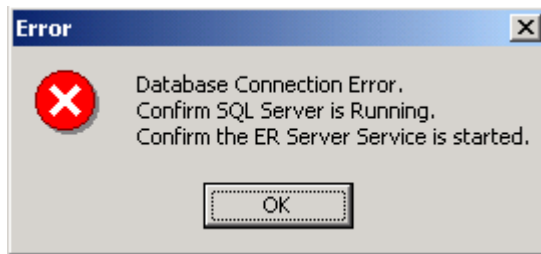
Cause

One or more Experion system services including BOOTP Server and SQL Server are not running.

Solution

- Launch **Control Panel** > **Administrative Tools** > **Services** and confirm that these Experion PKS services are running and Start any service that is not running.
- BOOTP Server
- Control Data Access Server
- ER Server
- GCL Name Server
- System Repository
- Check SQL Server icon on the Task Bar to confirm that it is running. If not, right-click the icon and select **MSQLServer - Start** from the list.

Cause

The Base IP address has not been configured in Control Builder.

Solution

- On the **Tools** menu in Control Builder, click **System Preferences**.
- In the **System Preferences** dialog, click the **Embedded FTE** tab and confirm that the Base IP Address is configured. If not, select the **Edit network parameters** check box and configure the applicable **Base IP Address**. Click the **OK** button to save the setting and close the dialog.

13 Effective Trouble Reporting

Related topics

"What Makes A PAR Effective" on page 608

13.1 What Makes A PAR Effective

A PAR (Product Anomaly Report) is the formal means by which problems are documented, from identification to eventual resolution, fix verification, and closure.

The life cycle of a PAR is very much dependent on a thorough description of the problem. When filing a PAR, the following guidelines will help enhance the effectiveness of the report:

Clue	Value
Component Version & Revision	Problems are many times unique to a release or set of releases. Code inspections and problem reproducibility are dependent on this information.
	Always provide the Experion release number, e.g., EXP100.0-24.1.
	Where a problem has been localized to a module or modules, go to NetworkTools and get the version/revision numbers for those modules. To reinforce the Experion release number, it is also helpful to record RSLinx, KTC and CNI release numbers.
	TAC will contact the user if specific version/revision information is needed.
Topology	A general description of the system topology is usually important.
	e.g., Redundant server, dual media ControlNet, 1 RCP with 2 downlinks, 1 RCP with 1 downlink, and 1 non-redundant controller with 2 downlinks, single I/O rack with all downlinks.
	If the problem is thought to be topology oriented, then a more detailed description/drawing is appropriate, including MAC ID assignments.
Symptoms	What about system operation is abnormal?
	What CNI, CPM, RM, CB, and/or SCAN error/fault indicators (LED states or error codes) are present?
	What alarms surround the abnormal condition?
Preceding Events & Actions	What lead up to this situation?
	Where actions were being taken prior to the event?
	What was the state of the system prior to the event?
	It is important that this information be recorded while it is still fresh in the User's mind.
Logs (see the respective Tool sections for details on log retrieval procedures)	What recorded events surround the abnormal condition?
	This question is best handled by printing/saving pertinent log content and attaching the printouts/files to the report. error on the side of too many (vs. too few) events.
	The following logs should be considered for storage and attachment:
	• SCAN Logs (both if redundant) • CB Logs • CPM Breadcrumbs (both if redundant) (see NetworkTools) • RM Event Logs (both) (see NetworkTools)
Recovery procedures	What recovery procedures where taken? Many times this information is extremely helpful in pinpointing the states of the components prior to recovery.
	NOTE: Controller Redundancy is designed to maintain control through a very large percentage of fault and recovery situations. It is very important that prescribed recovery procedures be followed.
Repeatability	If a problem is persistent, how persistent? This information is helpful in determining how the problem reproduction is approached.

14 Spare Parts

Related topics

14.1 ControlNet Interface (CNI) Spare Parts

> **Attention**
> Upon redundant controller switchover, the CNIs within the Redundant Chassis Pair (RCP) are temporarily not visible on their respective ControlNet segments. To ensure that the network is maintained, a minimum of two other ControlNet Nodes must remain on the ControlNet segment during the switchover operation. A method to avoid a single ControlNet node from going lonely during RCP switchover is to add another CNI module, or another Series A/H Rail Gateway module, or another Foundation Fieldbus Linking Device to the same ControlNet segment. This additional ControlNet device is commonly known as a 'Buddy Node'.

> **Attention**
> Note that after reprogramming the Secondary CNI's ControlNet parameters to match that of the Primary CNI, the Secondary CNI must be power-cycled so that redundant partner compatibility checks are re-attempted.

Related topics

14.1.1 TC-CCN011

Description	Single Media Series A ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesA\
Controller Redundancy	Not supported. This implies that this CNI cannot be present in a RCP. However, this CNI can be used in a remote I/O chassis or as a 'Buddy Node'.

> **CAUTION**
> At this time a TC-CCN011 cannot be used as a 'Buddy Node' in a redundant media system.

14.1.2 TC-CCR011

Description	Redundant Media Series A ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesA\
Controller Redundancy	Not supported. This implies that this CNI cannot be present in a RCP. However, this CNI can be used in a remote I/O chassis or as a 'Buddy Node'.

14.1.3 TC-CCN012

Description	Single Media Series C ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesC\

Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCN012 is compatible with another TC-CCN012 that has the same ControlNet parameter configuration and firmware revision.
	Furthermore, If a model TC-CCN012 module fails in a redundant chassis pair (RCP), you must replace both partner modules with the model TC-CCN014 Series E ControlNet module. Both partner modules in a RCP must be the same type. Synchronization is allowed one time from the backup to the primary. Failure to replace the older CNI module will disable synchronization.

14.1.4 TC-CCR012

Description	Redundant Media Series C ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesC\
Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCR012 is compatible with another TC-CCR012 that has the same ControlNet parameter configuration and firmware revision.
	Furthermore, If a model TC-CCR012 module fails in a redundant chassis pair (RCP), you must replace both partner modules with the model TC-CCR014 Series E ControlNet module. Both partner modules in a RCP must be the same type. Synchronization is allowed one time from the backup to the primary. Failure to replace the older CNI module will disable synchronization.

14.1.5 TC-CCN013

Description	Single Media Series D ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesD\
Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCN013 is compatible with another TC-CCN013 that has the same ControlNet parameter configuration and firmware revision.
	Furthermore, If a model TC-CCN013 module fails in a redundant chassis pair (RCP), you must replace both partner modules with the model TC-CCN014 Series E ControlNet module. Both partner modules in a RCP must be the same type. Synchronization is allowed one time from the backup to the primary. Failure to replace the older CNI module will disable synchronization.

14.1.6 TC-CCR013

Description	Redundant Media Series D ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesD\
Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCR013 is compatible with another TC-CCR013 that has the same ControlNet parameter configuration and firmware revision.
	Furthermore, If a model TC-CCR013 module fails in a redundant chassis pair (RCP), you must replace both partner modules with the model TC-CCR014 Series E ControlNet module. Both partner modules in a RCP must be the same type. Synchronization is allowed one time from the backup to the primary. Failure to replace the older CNI module will disable synchronization.

14.1.7 TC-CCN014

Description	Single Media Series E ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesE\
Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCN014 is compatible with another TC-CCN014 that has the same ControlNet parameter configuration and firmware revision.

14.1.8 TC-CCR014

Description	Redundant Media Series E ControlNet Interface Card.
FW Location	\Program Files\Honeywell\Experion PKS\Engineering Tools\System\Firmware\CNI\SeriesE\
Controller Redundancy	Supported.
Redundancy Compatibility	The TC-CCR014 is compatible with another TC-CCR014 that has the same ControlNet parameter configuration and firmware revision.

14.2 Periodic Maintenance Parts for C200/C200E Controller

Related topics

14.2.1 Recommended replacement parts

The following tables list items that are recommended for periodic replacement maintenance during the life of the C200/C200E Process Controller components.

Part	Description	Recommended Replacement Interval	Model Number
Lithium Battery	Control Processor Module (CPM) Battery Backup	Annually	TC-BATT01
NiCad Rechargeable Battery Pack	Battery Extension Module (BEM) Battery Pack	Every Two (2) Years	TC-BATT03

15 Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

15.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the "Support and other contacts" section of this document.

15.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

*   Send an email to security@honeywell.com.

    or

*   Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the "Support and other contacts" section of this document.

15.3 Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

15.4 Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.