Experion PKS
Control Hardware and I/O Modules Firmware Upgrade Guide

EPDOC-X150-en-500C
May 2018

Release 500
Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2018 - Honeywell International Sàrl
1 About this guide

This guide provides procedures for upgrading Experion control hardware and I/O modules to current firmware versions in an off-process state.

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>November 2016</td>
<td>Draft release of document.</td>
</tr>
<tr>
<td>B</td>
<td>February 2018</td>
<td>Updated PAR # 1-57KHBCL information in the document.</td>
</tr>
<tr>
<td>C</td>
<td>May 2018</td>
<td>Done changes under Firmware upgrades series e devices</td>
</tr>
</tbody>
</table>

Prerequisite skills

This guide is primarily intended for technical staff who are responsible for maintaining system hardware and upgrading hardware firmware versions to current and/or compatible levels. It assumes a high degree of technical knowledge and familiarity with the following:

- Windows operating environment
- Experion Engineering Tools applications:
  - Control Builder
  - Network Tools

Related documents

For more information about using Experion Engineering Tools applications, see:

- Control Building User's Guide
- C200/C200E Controller Troubleshooting and Maintenance Guide
This section lists the tasks that would help you plan for upgrading Experion control hardware and I/O modules. See the Go to column for additional details for each task.

<table>
<thead>
<tr>
<th>Action</th>
<th>Topic reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Familiarize yourself with the Network Tools utility</td>
<td>“Network Tools (NTOOLS)” on page 39</td>
</tr>
<tr>
<td>If you have a Redundant Chassis Pair (RCP), consider turning off power</td>
<td>“About redundant power” on page 15</td>
</tr>
<tr>
<td>Upgrade C200 Process Controllers</td>
<td>“Upgrading firmware in chassis-based components” on page 17</td>
</tr>
<tr>
<td>Upgrade C300 Process Controllers</td>
<td>“Firmware upgrades for Series C devices/EUCN nodes” on page 25</td>
</tr>
<tr>
<td>Upgrade chassis-based C200 controller hardware that includes I/O Modules</td>
<td>“Upgrading firmware in chassis-based components that include I/O Modules” on page 19</td>
</tr>
<tr>
<td>Upgrade Series C I/O Modules</td>
<td>“Firmware upgrades for Series C devices/EUCN nodes” on page 25</td>
</tr>
<tr>
<td>Upgrade Series C Fieldbus interface Modules</td>
<td>“Firmware upgrades for Series C devices/EUCN nodes” on page 25</td>
</tr>
<tr>
<td>Are you using ControlNet or Ethernet as your supervisory network media?</td>
<td>• “Maintaining PCIC devices for ControlNet products” on page 9</td>
</tr>
<tr>
<td></td>
<td>• “Setting CNI module Network Update Timing” on page 21</td>
</tr>
<tr>
<td></td>
<td>• “Verifying dangling control connections” on page 49</td>
</tr>
<tr>
<td></td>
<td>• “Searching for unsupported modules” on page 53</td>
</tr>
<tr>
<td>Do you have model CCN012/CCR012 or CCN013/CCR013 ControlNet Interface Modules in your C200 controller hardware configuration?</td>
<td>• “Replacing ControlNet interfaces within redundant C200 controllers” on page 45</td>
</tr>
<tr>
<td></td>
<td>• “Replacing ControlNet interfaces within non-redundant (or remote) chassis” on page 47</td>
</tr>
</tbody>
</table>
# 3 Maintaining PCIC devices for ControlNet products

The peripheral component interconnect communication (PCIC) interface card allows a computer that has a compatible PCI local bus to communicate directly with ControlNet products. If your Experion server uses a supervisory ControlNet for process points, you must verify the PCIC drivers and firmware are installed and at the latest version for Experion R500.x release.

<table>
<thead>
<tr>
<th>Task</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify PCIC drivers are installed and are the correct version</td>
<td>“Verifying the correct PCIC drivers” on page 10</td>
</tr>
<tr>
<td>If the PCIC driver is not installed, install it</td>
<td>“Installing PCIC drivers” on page 11</td>
</tr>
<tr>
<td>If the driver is not the correct version, upgrade the driver</td>
<td>“Upgrading PCIC drivers” on page 12</td>
</tr>
<tr>
<td>Verify the firmware is the latest available, and upgrade it if necessary</td>
<td>“Upgrading PCIC firmware” on page 13</td>
</tr>
</tbody>
</table>

**Related topics**
- “Verifying the correct PCIC drivers” on page 10
- “Installing PCIC drivers” on page 11
- “Upgrading PCIC drivers” on page 12
- “Upgrading PCIC firmware” on page 13
- “About redundant power” on page 15
3.1 Verifying the correct PCIC drivers

If your Experion server uses a supervisory ControlNet for process points, you must make sure they have the correct PCIC drivers installed.

To verify correct PCIC drivers
1. On the Experion server Desktop, right-click the My Computer icon and choose Manage to open the Computer Management dialog.
2. In the System Tools directory on the Tree tab, click the Device Manager item.
3. Under the computer directory in the view pane, check that the A-B Virtual Backplane item is listed.
   • If A-B Virtual Backplane is listed, go to the next step.
   • If A-B Virtual Backplane is not listed, skip the rest of this procedure and install the PCIC drivers.
4. Click the plus sign to expand the A-B Virtual Backplane item.
5. Double-click the A-B 1784-PCIC(S) item to open its Properties dialog.
6. Click the Driver tab, and then click Driver Details.
7. In the Driver files list box, click the entry that includes the ABPCICSW.sys file. Review the File version entry listed below the list box.
   • If the file version is 5.00.07, go to the next step.
   • If file version is not 5.00.07, skip the rest of this procedure and upgrade the PCIC drivers.
8. In the Driver files list box, click the entry that includes the virtualBackplane.sys file.
   • If the file exists, go to the next step.
   • If the file does not exist, skip the rest of this procedure and upgrade the PCIC drivers.
9. Review the File version entry listed below the list box.
   • If file version is 1.9, go to the next step.
   • If file version is not 1.9, skip the rest of this procedure and upgrade the PCIC drivers.
10. Close the tool:
    a. Click OK to close the Driver File Details dialog.
    b. Click OK to close the Properties dialog.
    c. Close the Computer Management dialog.

Related topics
“Network Tools (NTOOLS)” on page 39
3.2 Installing PCIC drivers

**Prerequisites**
- You have the Experion installation media.
- You have installed RSLinx software.

**To install PCIC drivers**
1. Insert the Experion application media into the Experion server drive.
2. On the Experion server Desktop, right-click the My Computer icon and choose Manage to open the Computer Management dialog.
3. In the System Tools directory on the Tree tab, click the Device Manager item.
4. Right-click in the view pane and choose Scan for hardware changes in the menu.
5. Click Other Device and then click Reinstall Driver.
6. Click Next to start installing the driver.
7. Click Display a list of the known drivers for this device so that I can choose a specific driver and then click Next.
8. Click Other Device.
9. Click Have Disk to display the Install from Disk dialog.
10. Click Browse and then browse to the following folder on the drive: `\RSLinx\RSLinx\pnp_Drivers\win2k\1784-PCIC(S)`
11. Click OK.
12. Click A-B 1784-PCIC(S).
13. Click Next.
14. Click Yes in the update driver warning message dialog box.
15. Click Next.
16. If a confirm file replace message dialog box appears, click Yes to continue the installation.
17. Click Finish to complete the installation.
18. Click Close to close the Properties dialog box.

**Next steps**
For more information about configuring the RSLinx PCIC driver, refer to the Experion Software Installation and Upgrade Guide.

**Related topics**
“Network Tools (NTOOLS)” on page 39
### 3.3 Upgrading PCIC drivers

#### Prerequisites
- You have Experion media.
- You have installed RSLinx software including PCIC drivers.

#### To upgrade PCIC drivers
1. From Experion server desktop, right-click **My Computer** and choose **Manage** to open the **Computer Management** dialog.
2. In the **System Tools** directory on the **Tree** tab, click **Device Manager** item.
3. Under the computer directory in the view pane, click the plus sign in front of the **A-B Virtual Backplane** to expand the item.
4. Double-click the **A-B 1784-PCIC(S)** item to open its **Properties** dialog.
5. Click the **Driver** tab, and then click **Update Driver…**.
6. Click **Next >** in the **Upgrade Device Driver Wizard** window.
7. Select the **Display a list of the known drivers for this device so that I can choose a specific driver** radix, and then click **Next**.
8. With **A-B 1784-PCIC(S)** highlighted, click **Have Disk…**.
9. **Browse…** to the path location of the driver version as identified in the Software Change Notice, for example: \C:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\Firmware\PCIC\DRV_4.02.01.
10. Highlight **abvbp2k.inf**, and click **Open**.
11. Click **OK** in the Install **From Disk** window.
12. Click **Next >** from the **Select a Device Driver** window.
13. Click **Next >** from the **Start Device Driver Installation** window.
14. Click **Yes** to acknowledge any file overwrites.
15. Click **Finish** from the **Completing the Upgrade Device Driver Wizard** window.
16. Click **Close**.
17. Close the **Computer Management** window.

#### Results
Ensure that the new drivers are being used. For more information about verifying the PCIC driver, refer to the “Verifying the correct PCIC drivers” on page 10 topic.

#### Next steps
For more information about configuring the RSLinx PCIC driver, refer to the **Experion Software Installation and Upgrade Guide**.

#### Related topics
“Network Tools (NTOOLS)” on page 39
3.4 Upgrading PCIC firmware

If your Experion server uses a supervisory ControlNet for process points, you must verify the most recent PCIC firmware is installed.

Prerequisites

- Review the Software Change Notice (SCN) for the following items.
  - Special instructions or considerations for upgrading component firmware.
  - File location and name of the latest PCIC firmware update file, usually, the file is located at: C:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\Firmware\PCIC
- Optional: you have stopped the Experion computer data access (CDA) server service through the Control Panel Administrative Tools function.

Attention

When upgrading PCIC firmware, verify the major firmware version remains the SAME. For example, 3.x.x for TC-PCIC01 modules and 4.x.x for TC-PCIC02 modules.

To update PCIC firmware

1. Obtain the name of the local PCIC card:
   a. Open RSLinx and click the Configure Drivers button on the toolbar.
   b. Note the CNetNode number of the PCIC driver (usually 23 or 24).
2. Click Start > Programs > Honeywell Experion PKS > Configuration Studio.
3. Log on with a security level of Engineer or greater.
4. Enable the firmware update option:
   a. In the Configuration Explorer in Configuration Studio, click Control Strategy.
   b. Click Set options for maintaining control system firmware.
   c. Click the Enable updating device firmware option.
5. Launch Network Tools:
   a. In the Configuration Explorer in Configuration Studio, click Control Strategy.
   b. Click Maintain control system firmware.
6. Click OK to acknowledge the Warning message.
7. Click Resume on the toolbar to initiate a network scan.
8. In the Desktop tree, click the local PCIC item. The CNetNode number identified in the RSLinx application appears in the local PCIC item name. Wait for the card details to display in the Detail pane.
9. Click Device > Update Firmware from File.
10. Browse to the file location and then click the firmware (FW) update file.

Tip

The file location and file name of the firmware update for the PCIC card are listed in the SCN as indicated in the Prerequisites of this procedure.

11. Click Open to start the firmware load.
12. Click Yes to confirm the firmware load, and wait for the load to complete.

Tip

You can monitor the load progress in the Status field in the lower portion of the Network Tools dialog.

13. Click OK to acknowledge the firmware load completed with no errors.
14. On the Network Tools menu, click Exit to close the application.
If you have not already done so, verify that your PCIC device driver is up to date. For more information about verifying the PCIC driver, refer to the “Verifying the correct PCIC drivers” on page 10 topic.

Shut down the computer.

Wait 60 seconds and restart the computer. Log on using a Windows account with local administrator privileges.

Related topics

“Network Tools (NTOOLS)” on page 39
3.5 About redundant power

If you are updating components in a Redundant Chassis Pair (RCP), consider turning off the power to the secondary controller chassis in the RCP. This allows the firmware in the selected component to be updated in the powered controller chassis while it is in a primary state with no partner state. After the firmware is updated, turn off the power to this chassis and turn the power on to the other controller chassis. Repeat the firmware update for the other component in the RCP. This avoids confusion caused by a logical change in Network Addresses in response to a controller switchover.

When updating a Redundant Modules (RM), you must turn off the power to the secondary chassis. If you fail to turn off power on the secondary chassis, there may be an unrecoverable loss of the RM.

Related topics

“Upgrading firmware in chassis-based components” on page 17
“Upgrading firmware in chassis-based components that include I/O Modules” on page 19
4 Upgrading firmware in chassis-based components

Use this information to upgrade the boot code and personality images in the following chassis-based components:

- C200 Control Processor Module (C200-CPM)
- Serial Interface Module (SIM)
- I/O Link Module (IOLIM)
- Chassis I/O - Series A Fieldbus Interface Module (FIM)
- Fault Tolerant Ethernet Bridge module (FTEB)

⚠️ **Attention**
- Do not change system time while firmware is being loaded. If system time is changed, the firmware load may fail.

**Prerequisites**

- Verify the process is **Off**. Loading firmware interrupts the component's normal operation.
- Review the *Software Change Notice* (SCN) for the following items.
  - Special instructions or considerations for upgrading component firmware.
  - File location and name of the latest firmware update file, usually, the file is located at: `C:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\Firmware`
- If you have an RCP, consider turning off power to the chassis not being updated. See About power in a Redundant Chassis Pair.

**To load the boot image**

1. Click **Start > Programs > Honeywell Experion PKS > Configuration Studio**.
2. Log on with a security level of Engineer or greater.
3. Enable the firmware update option:
   a. In the *Configuration Explorer* in Configuration Studio, click **Control Strategy**.
   b. Click **Set options for maintaining control system firmware**.
   c. Click the **Enable updating device firmware** option.
4. Launch **Network Tools**:
   a. In the Configuration Explorer in Configuration Studio, click **Control Strategy**.
   b. Click **Maintain control system firmware**.
5. Click **OK** to acknowledge the Warning message.
6. Click **Resume** on the toolbar to initiate a network scan.
7. In the Desktop tree, click the required CNI, ENet, or FTEB icon. Wait for the chassis details to display in the Detail pane.
8. Click the module's graphic representation in the Detail pane.
9. Choose **Device > Update Firmware from File**.
10 Click Yes to acknowledge the warning message dialog.

11 Look at the module's LED display. If the device is not in the Ready (RDY) state, click Yes to issue a stop (shutdown) command to the device and wait for the device to reboot to the RDY state.

12 The location and name of the firmware update for the module's firmware are listed in the SCN, as noted in the Considerations above. Browse to the folder and click the required boot image file.

13 Click Open to start the firmware load.

14 Click Yes to confirm the firmware load, and wait for the load to complete.

**Tip**
You can monitor the load progress in the Status field in the lower portion of the Network Tools dialog.

15 Wait for the load to complete and the module to reboot to its Alive (ALIV) state.

16 Click OK to acknowledge the firmware load completed with no errors.

**To load the personality image**

1 With the module in its Alive (ALIV) state, click the module's graphic representation in the detail pane.

2 On the Device menu, click Update Firmware from File.

3 Click Yes to acknowledge the warning message.

4 The location and name of the firmware update for the module's firmware are listed in the SCN, as noted in the Considerations above. Browse to the folder and click the required personality image file.

5 Click Open to start the firmware load.

6 Click Yes to confirm the firmware load, and wait for the load to complete.

**Tip**
You can monitor the load progress in the Status field in the lower portion of the Network Tools dialog.

7 Wait for the load to complete and the module to reboot to its No Database (NODB) state.

8 Click OK to acknowledge the firmware load completed with no errors.

**Next steps**

Repeat this procedure for each chassis-based CPM, SIM, IOLIM, and FIM component in your system

**Related topics**

“About redundant power” on page 15

“Network Tools (NTOOLS)” on page 39
5 Upgrading firmware in chassis-based components that include I/O Modules

Use this information to upgrade firmware in the following chassis-based components including DIN rail mounted Gateway devices:

- ControlNet Interface Module (CNI)
- I/O Module (IOM)
- Redundancy Module (RM)
- Ethernet Module (ENet)
- Rail I/O Gateway

Attention

To upgrade the firmware for the Rockwell I/O modules 1756/1794, follow the procedures recommended by Rockwell Automation for flashing the modules.

Upgrade each module one at a time.

- Do not change system time while firmware is being loaded. If system time is changed, the firmware load may fail.
- When updating a Redundant Modules (RM), you must turn off the power to the secondary chassis. If you fail to turn off power on the secondary chassis, there may be an unrecoverable loss of the RM.

Prerequisites

- Verify the process is Off. Loading firmware interrupts the component's normal operation.
- Review the Software Change Notice (SCN) for the following items.
  - Special instructions or considerations for upgrading component firmware.
  - File location and name of the latest firmware update file, usually, the file is located at: C:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\Firmware
- If you have an RCP, consider turning off power to the chassis not being updated. See Related topics.

To upgrade firmware in chassis-based components

1. Click Start &gt; Programs &gt; Honeywell Experion PKS &gt; Configuration Studio.
2. Log on with a security level of Engineer or greater.
3. Enable the firmware update option:
   a. In the Configuration Explorer in Configuration Studio, click Control Strategy.
   b. Click Set options for maintaining control system firmware.
   c. Click the Enable updating device firmware option.
4. Launch Network Tools:
   a. In the Configuration Explorer in Configuration Studio, click Control Strategy.
   b. Click Maintain control system firmware.
Click **OK** to acknowledge the Warning message.

Click **Resume** on the toolbar to initiate a network scan.

In the Desktop tree, click the required CNI, ENet, or FTEB icon. Wait for the chassis details to display in the Detail pane.

Click the module's graphic representation in the Detail pane.

Choose **Device > Update Firmware from File**.

Click **Yes** to acknowledge the warning message dialog.

Clear the **Update all other identical types in this controller (only) now** option.

Click **Yes** to acknowledge the use extreme care warning dialog.

Clear the **Update all other identical types in this controller (only) now** option.

The location and name of the firmware update for the module's firmware are listed in the SCN, as noted in the Considerations above. Browse to the folder and click the required personality image file.

Click **Open** to start the firmware load.

Click **Yes** to confirm the firmware load, and wait for the load to complete.

**Tip**

You can monitor the load progress in the **Status** field in the lower portion of the **Network Tools** dialog.

Wait for the load to complete and the module to reboot to its Alive (ALIV) state.

Click **OK** to acknowledge the firmware load completed with no errors.

**Next steps**

Repeat this procedure for each chassis-based CNI, IOM, RM, ENet and Rail I/O Gateway component in your system

**Related topics**

“About redundant power” on page 15

“Network Tools (NTOOLS)” on page 39
6 Setting CNI module Network Update Timing

Use this information to adjust Network Update Time (NUT) on new CNI modules received from the factory. The ControlNet parameters are updated for all CNIs on the ControlNet at the same time. Skip this procedure if you have previously set the NUT for all the CNI modules in your system.

Prerequisites
- You have launched Configuration Studio with a security level of at least Engineer.
- To change ControlNet parameters, the CNI module must be on a ControlNet that is plugged into a chassis, it must be cabled to the ControlNet, and it must have a unique MAC address.

To set CNI module NUT timing
1. Click Start > Programs > Honeywell Experion PKS > Configuration Studio.
2. Launch Network Tools:
   a. In the Configuration Explorer in Configuration Studio, click Control Strategy.
   b. Click Maintain control system firmware.
3. Click OK to acknowledge the Warning message.
4. Click Resume on the toolbar to initiate a network scan.
5. In the Desktop tree, click the required CNI icon. Wait for the chassis details to display in the Detail pane.
6. Click the CNI module's graphic representation in the Details pane. The CNI module is the item with the Network Address displayed.
7. Click Change ControlNet on the toolbar to display the Keeper Values dialog.
8. Click the Change tab.
9. Confirm all parameter values match the ones listed in ControlNet parameters.
10. Clear the My System uses Fiber Optics option.
11. If you did not change any of the parameter values, click Cancel and continue to step 12.
12. Click OK.
13. Click Yes to acknowledge the confirmation messages. Wait for the data transfer to complete.
14. Click OK to acknowledge the completion of the update without errors.
15. If a communications message dialog appears, click OK to acknowledge the message dialog and then click Pause on the toolbar to halt the network scan.
16. If there are CNIs on I/O networks that need to be updated, click a CNI from each I/O network in step and repeat steps to
17. On the Network Tools menu, click Exit to close the application.

Next steps
After changing the ControlNet parameters on a secondary CNI, it must be power-cycled so that the redundant partner compatibility checks are attempted again.
6 SETTING CNI MODULE NETWORK UPDATE TIMING

Related topics

“Network Tools (NTOOLS)” on page 39
“ControlNet parameters” on page 23
6.1 ControlNet parameters

To change ControlNet parameters, the CNI module must be on a ControlNet that is plugged into a chassis, it must be cabled to the ControlNet, and it must have a unique MAC address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUT Time</td>
<td>10000 uS (10 msec.)</td>
</tr>
<tr>
<td>SMAX</td>
<td>1</td>
</tr>
<tr>
<td>UMAX</td>
<td>32 (set UMAX to 20 for I/O network CNI modules)</td>
</tr>
<tr>
<td>Number of Repeaters</td>
<td>0</td>
</tr>
<tr>
<td>Cable Length</td>
<td>1000 (meters)</td>
</tr>
<tr>
<td>Cable Usage</td>
<td>A+B (for dual media cable configuration) - or -A (for single media cable configuration)</td>
</tr>
</tbody>
</table>

Related topics

“Setting CNI module Network Update Timing” on page 21
“Network Tools (NTOOLS)” on page 39
Before upgrading firmware on Series C devices/EUCN nodes, consider the following:

- You cannot initiate a new firmware download or device reboot, while a firmware load or device reboot is in progress.
- Downloading firmware to a Series C device/EUCN node erases all its configuration information. You must reload the device's configuration information after the firmware is updated.
- The loading of a new BOOT image automatically erases the application (APP) image in a module.
7.1 CTool utility

Use the Series C Firmware Load Tool (CTool) to upgrade firmware on Series C devices/EUCN nodes. Following are the operating characteristics of CTool:

- The first time you launch the CTool utility, it may take up to 40 seconds before the Series C devices/EUCN nodes on the network appear in the module listing table.
- If CTool is unable to load firmware to one of the selected modules, it skips loading firmware to that module and continues to load other selected modules.
- If you simultaneously select Series C I/O Modules and C300 Controller for firmware loading, CTool loads I/O Modules first before loading firmware to C300 Controller and Series C FIM.
- CTool does not allow loading firmware to a synchronized secondary device when the primary device is still on control.
- Since CTool shows only I/O Modules on a loaded I/O Link, loading firmware to a C300 erases the I/O Link, which means the I/O Modules on the link are no longer visible.
- If the device's application (APP) firmware is not the current version, CTool only loads application firmware when you manually select the module and click Load FW.

Use CTool to perform the following:

- Check the status of firmware loads to single or multiple devices through the status message box on the CTool window. CTool only shows updated status information for the modules while it loads the new firmware and/or reboots a module. It continues to monitor for added/removed devices until all operations are complete.
- Detect when modules are added or removed and when I/O Link cables are added or removed, which affects the presence of I/O Modules.

For more information about the CTool utility, see the” Series C Firmware Load Tool (CTool) for Series C Components” topic in the C200/C200E Troubleshooting and Maintenance Guide.

7.1.1 Starting the Series C Firmware Load Tool

You can start the Series C Firmware Load Tool (CTool) from the following folder: \Honeywell\Experion PKS \Engineering Tools\system\bin.

To start CTool
1. Launch Configuration Studio.
2. Select Control Strategy.
3. Select Maintain Control System Firmware from Series C-controller and I/O.

To start CTool from the Configuration Studio
1. Start the Configuration Studio.

   **Attention**

   - This feature is available only on (Server B and Non-redundant) – EMDB server.

2. On the Configuration Studio, click Maintain Control System Firmware under Series C Modules, as illustrated in the following figure.
Results
The CTool window appears with the list of modules.

7.1.2 CTool status indicators for firmware

The CTool display uses the following color coding to indicate the status and the versions for the application and boot firmware.

- **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.
7.1.3 Changing the default path for control file firmware

If you change the previously default folder for the Control File firmware, use this procedure to change the default path used by the CTool utility.

**To change the default path using CTool**

1. Start the CTool utility, as described in “Starting the Series C Firmware Load Tool” on page 26.
2. Wait for the module listing table to appear in the CTool window.
3. Click the System Prefs to open the Browse For Folder dialog.
4 Navigate the directory tree in the list box to find and select the new default folder for firmware files, so the file name appears in the **Folder** field.

5 Click **OK** to save the default path change and close the **Browse For Folder** dialog.

6 Click **Exit** to close the **CTool** window or go to the next section.
7.2 Upgrading firmware using the Series C Firmware Load Tool

You can use (CTool) to load or upgrade the required firmware in the following devices/nodes:

- C300 Controller (C300)
- Series C I/O Modules
- Series C Fieldbus Interface Module (FIM4)
- EUCN nodes (EHPM and ENIM)

**CAUTION**

- Ensure that the power is not turned off while upgrading the firmware. If it is turned off, the upgrade might not complete and the module might have to be replaced.
- Do not change the system time while the firmware is being loaded. If the system time is changed, the firmware load might fail.

For more information about upgrading the firmware, see the relevant topics, as listed in the following table:

<table>
<thead>
<tr>
<th>Device</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>C300 controllers</td>
<td>“Upgrading firmware in C300 controllers” on page 30</td>
</tr>
<tr>
<td>Series C I/O modules and Field Interface modules</td>
<td>“Upgrading firmware in single Series C I/O modules and Field interface modules”</td>
</tr>
<tr>
<td>Multiple Series C I/O modules and Field Interface modules</td>
<td>“Upgrading firmware in multiple Series C I/O modules and Field Interface modules”</td>
</tr>
<tr>
<td>EUCN nodes</td>
<td>“Upgrading firmware in EUCN nodes” on page 32</td>
</tr>
</tbody>
</table>

**Related topics**

- “Upgrading firmware in C300 controllers” on page 30
- “Upgrading firmware in EUCN nodes” on page 32
- “Upgrading firmware in single Series C I/O modules and Field interface modules” on page 34
- “Upgrading firmware in multiple Series C I/O modules and Field Interface modules” on page 35

7.2.1 Upgrading firmware in C300 controllers

You can use the Series C Firmware Load Tool (CTool) to load or upgrade the required firmware in the C300 controller (C300).

You can upgrade the existing firmware in the C300 controllers to the latest firmware.

The following table lists the file location of the required firmware files and the sequence in which the firmware must be upgraded in C300 controllers, based on various scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Firmware file location</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you are upgrading the firmware from releases prior to Experion R430</td>
<td>Upgrade the firmware from the following locations, in the specified order: 1. \Honeywell\Experion PKS\Engineering Tools\system\Firmware\Controllers\c300\R430Migration 2. \Experion PKS\Engineering Tools\system\Firmware\Controllers\c300\R430.1</td>
</tr>
<tr>
<td>When you are upgrading the firmware within Experion R430 release, which includes patch releases</td>
<td>Upgrade the firmware from following location: \Experion PKS\Engineering Tools\system\Firmware\Controllers\c300\R430.1</td>
</tr>
</tbody>
</table>
**Prerequisites**

- Review the applicable *Software Change Notice* (SCN) for the following items.
  - Special instructions or considerations for upgrading the firmware.
  - File location and names of the latest firmware update file.
  - You can compare SCN information to the firmware information in the `ver_rev.txt` file found at \Honeywell\Experion PKS\Engineering Tools\system\bin.
  - You can compare the SCN information to the Control File firmware version listed for a given device found at: \Experion PKS\Engineering Tools\system\Firmware
- IP address and the addresses for the time servers through the *System Preferences* selection in the Control Builder's *Tools* menu are configured.
- Device Index number for each C300 is set through the Binary Coded Decimal switches on its input/output termination assembly (IOTA).
- All C300 blocks are configured and loaded.
- Process is **OFF control**. Loading firmware interrupts the component's normal operation.
- Ensure that BOOTP service is running only on R430.1 servers. You must disable BOOTP services running on the prior-release- based servers to avoid issues like modules not obtaining a system time reference.

**To upgrade or load firmware in a single C300 controller**

1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears.
2. Select the required C300 controller for which you want to upgrade the firmware.
3. Right-click to open the firmware load shortcut menu, as illustrated in the following figure.
4. Select **Load > Control File**.
   - The Image Option Dialog is displayed.
5. Select the appropriate application image version and click **OK**.
6. Navigate to the appropriate file location, which contains the c300.lcf file. Perform one of the following tasks, depending on the required scenario:

<table>
<thead>
<tr>
<th><strong>Experion release</strong></th>
<th><strong>Tasks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Releases prior to Experion R430</td>
<td>If you are migrating from a release prior to Experion R430 to Experion R430, perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to \Honeywell\Experion PKS\Engineering Tools\system\Firmware\Controllers\C300\R430Migration.</td>
</tr>
<tr>
<td></td>
<td>2. Select the c300m.lcf file and click <strong>Open</strong> to initiate the firmware upgrade.</td>
</tr>
<tr>
<td></td>
<td>3. Monitor the firmware update through the status message box and the Status column in the module listing table, and wait for the firmware loading operation to complete.</td>
</tr>
<tr>
<td></td>
<td>4. Navigate to \Experion PKS\Engineering Tools\system\Firmware\Controllers\C300\R430.1 to load another required firmware.</td>
</tr>
<tr>
<td></td>
<td>5. Repeat steps 2 and 3.</td>
</tr>
</tbody>
</table>
Experion release | Tasks
---|---
Within Experion R430, which includes patch releases | If you are upgrading or loading the required firmware within Experion R430, perform the following tasks:
1. Navigate to \Experion PKS\Engineering Tools \system\Firmware\Controllers\C300\R430.1.
2. Select the c300m.lcf file and click **Open** to initiate the firmware upgrade.
3. Monitor the firmware update through the status message box and the Status column in the module listing table, and wait for the firmware loading operation to complete.

7. On the **File** menu, click **Exit** to close the **CTool** window.

To upgrade or load firmware in multiple C300 controllers
1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears.
2. Select the required C300 controllers for which you want to upgrade the firmware.
3. Repeat steps 3 to 7, as described in the procedure, **To upgrade or load firmware in a single C300 controller**.

Results
You have upgraded the required firmware in the C300 controller.

7.2.2 Upgrading firmware in EUCN nodes

Attention
If you are integrating the ENIM/EHPM with Experion R431.1 or later, and the ENIM/EHPM BOOT firmware version is at a minimum of 3.0, you can use CTools to upgrade ENIM/EHPM BOOT firmware to ENIM/EHPM-Experion BOOT and APP images. After the ENIM/EHPM is integrated with Experion, ENIM’s/EHPM’s BOOT and APP firmware images are at a minimum version of R431.1. For subsequent firmware upgrades, use CTools.

You can use the Series C Firmware Load Tool (CTool) to load or upgrade the required firmware in the EUCN nodes
You can upgrade the existing firmware in the EUCN nodes to the latest firmware.

The following table lists the file location of the required firmware files and the sequence in which the firmware must be upgraded in EUCN nodes, based on various scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Firmware file location</th>
</tr>
</thead>
</table>
| Upgrading the ENIM firmware | Upgrade the firmware from following location:  
Computer\C:\Program Files (x86)\Honeywell \Experion PKS\Engineering Tools\system\Firmware \ENIM  |
| Upgrading the EHPM firmware | Upgrade the firmware from following location:  
Computer\C:\Program Files (x86)\Honeywell \Experion PKS\Engineering Tools\system\Firmware \Controllers\EHPM  |

Prerequisites
- Review the applicable **Software Change Notice** (SCN) for the following items.
  - Special instructions or considerations for upgrading the firmware.
- File location and names of the latest firmware update file.
- You can compare SCN information to the firmware information in the `ver_rev.txt` file found at:
  \Honeywell\Experion PKS\Engineering Tools\system\bin.
- You can compare the SCN information to the Control File firmware version listed for a given device found at: \Experion PKS\Engineering Tools\system\Firmware

- **IP address and the addresses for the time servers through the System Preferences selection in the Control Builder's Tools menu are configured.**
- **All EHPM blocks are configured and loaded.**
- **Ensure that all redundant ENIMs are running the odd FTE indexed node as primary. Use $FTESTS1 and select the odd UCN node numbers to ensure that the FTE Index displayed is odd. If it is even, shutdown the Primary ENIM from the Native Window and then reload the ENIM.**
- **Ensure that all redundant EHPMs are running the odd FTE indexed node as primary. Use $FTESTS1 and select the odd UCN node numbers to ensure that the FTE Index displayed is odd. If it is even, perform a commanded “swap primary” on the EHPM pair.**
- **Ensure that BOOTP service is running on R431.1 servers. You must disable BOOTP services running on the prior-release-based servers to avoid issues like modules not obtaining a system time reference.**

**To upgrade or load firmware in an ENIM node**

1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears.
2. Select the Backup ENIM node for which you want to upgrade the firmware and then click **Load FW**. Wait till the firmware loads successfully.
3. Perform the following procedure for the Backup ENIM that has been loaded with firmware:
   a. Shutdown the ENIM from the Native Window.
   b. Power recycle the ENIM from the LCN chassis power supply module.
   c. Reload the ENIM from the Native Window.
4. Repeat steps 2 and 3 for each Backup ENIM.
5. Shutdown the Primary ENIM from the Native Window.
   Ensure the Backup ENIM takes over as primary.
6. Select the original Primary ENIM for which you want to upgrade the firmware and then click **Load FW**. Wait till the firmware loads successfully.
7. Perform the following procedure for the original Primary ENIM that has been loaded with firmware:
   a. Power recycle the ENIM from the LCN chassis power supply module.
   b. Reload the ENIM from the Native Window.
8. Repeat steps 6 and 7 for each original Primary ENIM.

**To upgrade or load firmware in an EHPM node**

1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears.
2. Select the Backup EHPM node for which you want to upgrade the firmware and then click **Load FW**. Wait till the firmware loads successfully.
3. Perform the following procedure for the Backup EHPM that has been loaded with firmware:
   a. Shutdown the EHPM from the Native Window’s UCN Status Display.
   b. Power down the EHPM by removing the High-Performance I/O Link card (which disconnects power supply to the chassis).
   c. Re-insert the High-Performance I/O Link card and then reload the EHPM from the from the Native Window’s UCN Status Display (after it has transitioned to the ALIVE state).
4. Repeat steps 2 and 3 for each Backup EHPM.

5. Wait for five minutes and then perform a commanded swap-over (Swap Primary) of the Primary EHPM and wait for the node’s status to change to BACKUP.

6. Select the original Primary EHPM for which you want to upgrade the firmware and then click **Load FW**. Wait till the firmware loads successfully.

7. Perform the following procedure for the original Primary EHPM that has been loaded with firmware:
   a. Shutdown the EHPM from the Native Window’s UCN Status Display.
   b. Power down the EHPM by removing the High-Performance I/O Link card (which disconnects power supply to the chassis).
   c. Re-insert the High-Performance I/O Link card and then reload the EHPM from the Native Window’s UCN Status Display (after it has transitioned to the ALIVE state).

   **Attention**
   You must power cycle EHPM after loading firmware.

8. Repeat steps 6 and 7 for each original Primary EHPM.

**Results**
You have upgraded the required firmware in the EUCN nodes.

### 7.2.3 Upgrading firmware in single Series C I/O modules and Field interface modules

Use the Series C Firmware Load Tool (CTool) to upgrade firmware in the following single Series C devices:
- Series C I/O Modules
- Series C Fieldbus Interface Module (FIM4)

**Prerequisites**
- You have reviewed the applicable **Software Change Notice** (SCN) for the following items.
  - Special instructions or considerations for upgrading component firmware.
  - File location and name of the latest firmware update file.
  - You can compare SCN information to the firmware information in the `ver_rev.txt` file at: `\Honeywell\Experion PKS\Engineering Tools\system\bin`
  - You can compare the SCN information to the Control File firmware version listed for a given device found at the default path: `\Experion PKS\Engineering Tools\system\firmware`
- Experion R500.x software is installed.
- IP address and the addresses for the time servers through the **System Preferences** selection in the Control Builder's **Tools** menu are configured.
- Device Index number for each FIM4 is set through the Binary Coded Decimal switches on its input/output termination assembly (IOTA).
- Series C devices are set to their corresponding **IDLE** state.
- Process is **OFF control**. Loading firmware interrupts the component's normal operation.
- Series C I/O Modules only show in the CTool when the I/O Link is configured and loaded.
- Fieldbus links to a Series C FIM are **inactive**.
- Ensure that BOOTP service is running only on R500.1 servers. You must disable BOOTP services running on the prior-release-based servers to avoid issues like modules not obtaining a system time reference.
To load firmware in single Series C I/O modules and Field interface modules

1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears. Wait for the list of modules to appear in the CTool window.

2. Open the firmware load shortcut menu:
   - Locate the row in which the module to be upgraded is located.
   - Right-click in the row.

   ![CTool - Series C Firmware Load Tool](image)

   Tip
   If you select a Series C I/O module, the shortcut menu is slightly different.

3. Select the source of the firmware upgrade file:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use the current Release version,</td>
<td>Click Load &gt; Release.</td>
</tr>
<tr>
<td>click Load &gt; Release.</td>
<td></td>
</tr>
<tr>
<td>To use the control file or file.</td>
<td>1. Click Load &gt; Control File or Load &gt; File.</td>
</tr>
<tr>
<td></td>
<td>2. From the Open dialog, navigate to the firmware folder for the selected</td>
</tr>
<tr>
<td></td>
<td>module and double-click folders until the .lcf file appears in the Look in</td>
</tr>
<tr>
<td></td>
<td>field and the file appears in the list box.</td>
</tr>
<tr>
<td></td>
<td>3. Select the file so its name appears in the File Name field.</td>
</tr>
<tr>
<td></td>
<td>4. Click Open to initiate the upgrade.</td>
</tr>
</tbody>
</table>

4. Monitor the firmware update through the status message box and the Status column in the module listing table, and wait for the firmware load operation to complete.

5. Repeat step 4 through step 6 to upgrade firmware in other modules.

6. On the File menu, click Exit to close the CTool window.

7.2.4 Upgrading firmware in multiple Series C I/O modules and Field Interface modules

Use the Series C Firmware Load Tool (CTool) to upgrade firmware in the following multiple Series C devices.

- Series C I/O Modules
- Series C Fieldbus Interface Module (FIM4)
Prerequisites

- You have reviewed the applicable Software Change Notice (SCN) for the following items.
  - Special instructions or considerations for upgrading component firmware.
  - File location and name of the latest firmware update file.
  - You can compare SCN information to the firmware information in the `ver_rev.txt` file at: {Honeywell\Experion PKS\Engineering Tools\system\bin}
  - You can compare the SCN information to the Control File firmware version listed for a given device found at the default path: {Experion PKS\Engineering Tools\system\firmware}
- Experion R500.x software is installed.
- IP address and the addresses for the time servers through the System Preferences selection in the Control Builder's Tools menu are configured.
- Device Index number for each FIM4 is set through the Binary Coded Decimal switches on its input/output termination assembly (IOTA).
- Series C devices are set to their corresponding IDLE state.
- Process is OFF control. Loading firmware interrupts the component's normal operation.
- Series C I/O Modules only show in the CTool when the I/O Link is configured and loaded.
- Fieldbus links to a Series C FIM are inactive.
- Ensure that BOOTP service is running only on R500.1 servers. You must disable BOOTP services running on the prior-release- based servers to avoid issues like modules not obtaining a system time reference.

To load firmware in multiple Series C I/O modules and FIM devices

1. Start the CTool utility as described in “Starting the Series C Firmware Load Tool” on page 26. The CTool — Series C Firmware Load Tool appears. Wait for the list of modules to appear in the CTool window.
2. Select all modules that require a firmware update as shown in the following example.

   ![CTool Image]

   Tip
   Use the horizontal and vertical scroll bars to scroll through the information in the table.
3 Manually select those modules that are coded in blue. These are modules that have interoperable firmware for the current Experion release but not the newest version. These modules will not be selected automatically for updating.

4 Click **Load FW** to initiate the firmware update of the selected modules. CTool updates all the selected modules.

5 Monitor the firmware update through the status message box and the Status column in the module listing table as shown in the following example. Wait until the load operation completes and displays the updated details of the **Boot Ver** and **App Ver** entries.

6 On the **File** menu, click **Exit** to close the CTool window.
Use the Network Tools (NTools) utility to access operating data about Experion Process Controllers and related chassis-based hardware within the Experion system. NTools scans all the nodes on the supervisory network connected to your Experion server and displays the following information:

- In the tree pane, it displays the nodes connected to your computer in a hierarchical order,
- In the list pane, it displays information about the communication status of the supervisory network.
- In the detail pane, it displays a graphical representation of the modules included in the chassis.

Related topics

“Upgrading PCIC firmware” on page 13
“Verifying the correct PCIC drivers” on page 10
“Installing PCIC drivers” on page 11
“Upgrading PCIC drivers” on page 12
“Upgrading firmware in chassis-based components” on page 17
“Upgrading firmware in chassis-based components that include I/O Modules” on page 19
“Setting CNI module Network Update Timing” on page 21
“ControlNet parameters” on page 23
“Searching for unsupported modules” on page 53
8.1 Network Tools usage guidelines

Under abnormal network conditions, the NTOOLS utility may negatively impact network performance. Please observe the following usage guidelines.

- Do not set Network Tools to run continuously on heavily loaded systems. It places a load on the communications network. This means that running NTOOLS may cause some degradation to the network on systems that are already heavily loaded.

- Do not open more than two instances of Network Tools across the entire system simultaneously.

Network Tools includes a message meter that displays a Warning Message after every 5000 messages that it sends to the Controller. This Warning Message is a reminder to users not to leave NTOOLS running continuously since it may degrade network performance.
8.2 Starting Network Tools

Use the following procedure to make the initial settings the first time you start the Network Tools application on your computer.

Prerequisites

- You have launched Configuration Studio with Security level of at least Engineer.
- You know the number of slots in the local chassis.
- If your system includes a remote chassis, you know the following details:
  - The number of slots in the remote chassis.
  - The assigned network address (MAC ID) of the remote chassis. The assigned network address appears in the module's LED display in the format A# nn, where nn is the network address.
  - The slot number where the downlink CNI is installed in your local chassis.

To start Network Tools

1. On the Configuration Explorer tab in Configuration Studio, click Control Strategy and then click Maintain control system firmware to launch Network Tools.

2. Click OK to acknowledge the Warning message.

3. Select the Desktop icon in the Tree pane, and then click Settings on the toolbar to call up the Settings dialog.

4. Configure settings:
   a. In the Delay between scans (seconds) text box, type 2, and click Periodic (automatic).
   b. Check Enable Module Version Revision Checking.
   c. Check Enable ControlNet Parameter Checking.
   d. Click OK.

5. Click Resume in the toolbar.

6. When network nodes are displayed under the Desktop item in the Tree pane, click the first CNI, Ethernet, or FTE Bridge icon.

7. Click the Local Chassis tab.

8. In the Number of Slots in Local Chassis box, click or type the number of slots.

9. If your system includes a remote chassis:
   a. Click a Remote Chassis tab.
   b. Click Check here if Remote Chassis installed.
   c. In the Number of Slots in Remote Chassis box, click or type the number of slots.
   d. In the Remote Chassis CNI MAC ID box, click or type the network address of the remote chassis.
   e. In the DownLink CHI Slot number box, click or type the slot number where the downlink CNI is installed on the local chassis.
   f. Repeat all these sub-steps for each remote chassis, selecting the next available numbered remote chassis tab, for example, Remote Chassis2.

10. Click Ok.

11. In the Detail pane, the chassis graphic appears, including the remote chassis, if applicable.

12. In the Tree pane, click the next CNI, Ethernet, or FTE Bridge icon.
13 Repeat steps to until all CNI or Ethernet items are configured.
14 On the Network Tools menu, click Exit to close the application.

Next steps
For additional help about the Network Tools application, select Help > Help Topics in the application's window.
8.3 About module graphics

Each module graphic displays the following details about the module:

- The module base model number of the module, without the TC- prefix.
- The module state.
- The CEE type of the CPMs (standard is 50ms and fast is 5ms)
- The module firmware version, including application version (AV) and boot version (BV), if applicable.
### 8.4 Network Tools status indicators for firmware

NTools uses the following color coding to display a component's current version/revision level:

- **Red** The module type is recognized, however, the device firmware version/revision is not known.
- **Green** The module type is recognized and the device firmware version/revision is associated with the current release of Experion.
- **Cyan** 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.
- **Yellow** The module type is *not* recognized.
9 Replacing ControlNet interfaces within redundant C200 controllers

Within a redundant chassis pair, the model CCN012/CCR012 or CCN013/CCR013 modules are not compatible with model CCN014/CCR014 modules.

Upon switch-over to the primary role, the CCN014/CCR014 is not compatible with the CCN012/CCR012 or CCN013/CCR013 because the CCN014/CCR014 has more resources (for example, memory) than the previous models.

While the following procedure pertains to replacing a CCN013/CCR013 with a CCN014/CCR014, it can easily be adapted for CCN014/CCR014 replacements for CCN012/CCR012 modules.

Attention

- If a model CCN012/CCR012 or CCN013/CCR013 module fails in a redundant chassis pair (RCP), you must replace both partner modules with the model CCN014/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.

  Redundant chassis pair synchronization will be dropped while performing module replacement.

Prerequisites

- The CCN012/CCR012 ControlNet Interface modules must be at 4.24 version firmware.
- The CCN013/CCR013 ControlNet Interface modules must be at 5.36 (or later) version firmware.
- The replacement CCN014/CCR014 ControlNet Interface modules must be at 10.06 (or later) version firmware.

To replace CCN013/CCR013 ControlNet interfaces in redundant chassis

1. Remove power from the secondary chassis.
2. Disconnect the ControlNet cables (at the module) and extract the CCN013/CCR013 modules from the secondary chassis.
3. Insert the CCN014/CCR014 replacement modules and reconnect the ControlNet cables.
4. Apply power to the secondary chassis.
5. If necessary, set the CNI Module NUT Timing.
6. In the RM detail display's Summary tab, click Synchronize Secondary and then click Yes to commence initial synchronization, if not automatically triggered.
7. Wait until the redundant chassis pair is synchronized.
8. In the RM detail display's Summary tab, click Initiate Switchover and a then click Yes to change redundancy role. At this point in time, the new CCN014/CCR014 modules are operating in the primary redundancy role.
9. Remove power from the secondary chassis.
10. Disconnect the ControlNet cables (at the module) and extract the CCN013/CCR013 modules from the secondary chassis.
11 Insert CCN014/CCR014 replacement modules and reconnect the ControlNet cables.

12 Apply power to the secondary chassis.

13 If necessary, set the CNI Module NUT Timing. See Setting CNI module Network Update Timing for more information about this.

14 In the RM detail display's Summary tab, click Synchronize Secondary and then click Yes to commence initial synchronization, if not automatically triggered.
10 Replacing ControlNet interfaces within non-redundant (or remote) chassis

Within a non-redundant chassis, replacement of CCN012/CCR012 with CCN013/CCR013 or CCN014/CCR014 ControlNet Interface is an off-process operation resulting in loss-of-view and/or loss-of-control. The same is true for replacement of CCN013/CCR013 with CCN014/CCR014 module.

Prerequisites
The affected chassis is power-cycled making this an off-process operation.

To replace CCN013/CCR013 ControlNet interfaces in non-redundant chassis
1 Remove power from the chassis.
2 Disconnect the ControlNet cables (at the module) and extract the CCN013/CCR013 modules from the chassis.
3 Insert CCN014/CCR014 replacement modules and reconnect the ControlNet cables.
4 Apply power to the chassis.
5 If necessary, set the CNI Module NUT Timing. See CNI module Network Update Timing for more information.
11 Verifying dangling control connections

Use this information to verify dangling control connections.

**Prerequisites**
- You have launched Configuration Studio with Security level of at least Engineer.
- You are running Control Builder on Experion server.

**To verify dangling connections**
1. From Control Builder Set Control Builder, right-click the Monitoring tab and select Assignment View.
2. On the Monitoring tab, click C200_CPM icon.
3. On the Controller menu, click Checkpoint > Rebuild selected object(s) and contents checkpoint from monitoring tab.
4. Resolve any Block at other end of connection missing errors before starting the on-process migration.
12 Verifying switch port settings

Use this procedure to verify the switch port settings are correct before you start a controller upgrade.

Prerequisites
• You know the name of Yellow and Green switches.
• You know the IP addresses of the Yellow and Green switches.
• You know the login name and password.

To verify port settings
1 Click Start on the task bar and choose Run to open the Run dialog.
2 Type cmd in the Open box and click OK to open the DOS command window.
3 At the DOS prompt, type telnet ip_address where ip_address is the IP address of the switch. Press the Enter key.
4 At the password prompt, type the password and then press the Enter key.
5 Type enable and press the Enter key.
6 Type password and press the Enter key.
7 Type sho run and press the Enter key.
8 Verify that the switch port connected to the FTEB has the following settings:
   • No IP address
   • Duplex full
   • Spanning-tree portfast trunk. If the port speed is set to Auto, it is not displayed. If it is set to 100Mbps, it will be displayed as Speed 100. For FTEB, the port speed should be set to Auto.
9 If the settings in your switch are not the same, contact your local Honeywell Technical Assistance Center (TAC).
13 Searching for unsupported modules

Use this procedure to search for unsupported chassis-based modules.

**Prerequisites**

- You have launched Configuration Studio with Security level of at least Engineer.
- You are familiar with Network Tools.

**To search for unsupported chassis-based modules**

1. On the **Configuration Explorer** tab in Configuration Studio, click **Control Strategy** and then click **Maintain control system firmware** to launch Network Tools.
2. Click **OK** to acknowledge the Warning message.
3. Click **Resume** on the toolbar to initiate a network scan.
4. In the Desktop tree, click the required CNI, ENet, or FTEB icon. Wait for the chassis details to display in the Detail pane.
5. Check each module display for any version information displayed in red or yellow color. Take appropriate action to correct any version incompatibility that is indicated. See Upgrading firmware in chassis-based components for more information.

**Related topics**

“Network Tools (NTOOLS)” on page 39
14 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.

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).

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:
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” section of this document.

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.

Training classes
Honeywell holds technical training classes about 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.