Honeywell

Experion PKS
System Alarms Reference

EPDOC-X140-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X140-en-431A	431	0	February 2015

Disclaimer

Contents

About this reference

This reference describes how to respond to Experion system alarms.

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

Archive system alarms

The following topics describe archive-related system alarms and how to respond to them.

Related topics

“Archive - Archive Failed: Low Disk Space” on page 16
“Archive - Failed To Archive History” on page 17

Archive - Archive Failed: Low Disk Space

Potential causes

The drive where online history archives are to be stored (typically in 'data\archive') does not have enough free space.

Consequence of inaction

Online history could be lost if not archived. If history is lost, depending on the type lost and history archiving settings, Trends may show gaps where history is missing.

Corrective actions

1. Call up the **History Archiving** display.
2. Check that the History Archiving Disk Limit is configured appropriately.
3. Check that the 'Location to Move History Archive to' exists and has enough free space.
4. Call up the **Server Configuration** display.
5. Check that the archive folder exists and has enough free space.

For more information, see “Configuring history archives”.

Time to respond

Immediate.

Archive - Failed To Archive History

Potential causes

1. Online history files could not be copied to the online history archive folder (typically 'data\archive').
2. Error creating online history archive files in the destination archive folder.
3. Error writing to the online history archive files in the destination archive folder.

Consequence of inaction

Online history could be lost if not archived. If history is lost, trends may show gaps where history is missing (depending on the type lost and history archiving settings).

Corrective actions

1. Open the **Experion PKS Server Configuration Panel**.
2. Check that the archive folder exists.
3. Check that MNGR user has permission to create files and directories and write to the archive folder.

For more information, see “Configuring history archives”.

Time to respond

Immediate.

COMMS system alarms

The following topics describe communication-related system alarms and how to respond to them.

Related topics

COMMS - Backup: Not Synchronized

Potential causes

The Experion PKS Server state has changed to Database Only. CDA or SR services on the primary or backup may have been stopped or failed, or the system may be experiencing network issues.

Consequence of inaction

Server synchronization has failed. Future modifications to primary System Repository content will not be synchronized with the backup, and may be lost.

Corrective actions

If the backup server is in Database Only state, return it to Running state. Synchronization will occur automatically.

Otherwise, go to the Server Redundancy display and check the System Repository backup status. If the status is 'Stopped,' go to the services and start the Experion PKS System Repository service. You may also need to check that the status of the Experion PKS Control Data Access Server service is running.

Time to respond

Immediate.

COMMS - Backup Server

Potential causes

The backup server is not running.

Consequence of inaction

Backup Server (and therefore server redundancy) is not available. The system will continue to run on Primary, but without redundancy.

Corrective actions

1. Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.
2. Set the backup server status to System Running.

Time to respond

Backup Server is unavailable as when alarm is raised. The time to respond will depend on assessment of process/site/operations for criticality/risk of running without backup server available.

COMMS - CHANNEL <channel number>

Potential causes

A SCADA channel is marginal or failed.

Consequence of inaction

If a SCADA channel fails, process data from point parameters on that channel will not be available. It will also not be possible to initiate control.

Corrective actions

1. Check the SCADA controller status on the **System Status** display.
2. Check communication links to SCADA devices and the devices themselves.

Time to respond

The corrective actions should be initiated immediately to prevent loss of process data on the SCADA channel.

COMMS - CONTROLLER <controller number>

Potential causes

A SCADA device is marginal or failed.

Consequence of inaction

If a SCADA controller fails, process data from point parameters on that controller will not be available. It will also not be possible to initiate control.

Corrective actions

1. Check the SCADA controller status on the **System Status** display.
2. Check communication links to SCADA devices and the devices themselves.

Time to respond

The corrective actions should be initiated immediately to prevent loss of process data on the SCADA controller.

COMMS - CStnxx: Data connection to <server name> is blocked. Remote server is busy

Potential causes

The numbered Console Station has notified that the server is not responding in a timely manner.

Consequence of inaction

The Console Station will not be able to view data from the mentioned connection. If the blocked connection is the cluster server connection, the Console Station will not be able to view SCADA, DSA, or third-party OPC data, but direct data remains unaffected.

Corrective actions

1. Call up the **Console Station Status Detail** display on the remote server.
2. Use Windows Performance Monitor on the remote server to make sure CPU load and free memory are within the Experion Specification limits. The Experion Specification is available from Honeywell.

Time to respond

Immediately.

COMMS - CStnxx: Notification Server on <server name> OVERLOADED

Potential causes

The numbered Console Station has notified that the DSA remote server is experiencing alarm overload. The remote server may be experiencing high system load and is having trouble sending alarms to the local server fast enough.

Consequence of inaction

There may be a delay before notifications from that server are displayed on the Console Station. If the Experion cluster server is overload, DSA, SCADA, and third-party OPC alarms will be delayed.

Corrective actions

1. Call up the **Console Station Status Detail** display on the remote server.
2. Use Windows Performance Monitor on the remote server to make sure CPU load and free memory are within the Experion Specification limits. The Experion Specification is available from Honeywell.

Time to respond

Immediately.

COMMS - CStn<nn>: Not Synchronized

Potential causes

CDA or SR services on the Console Station might have been stopped or failed, or the system might be experiencing network issues.

Consequence of inaction

Server synchronization has failed. Future modifications to primary System Repository content will not be visible on the Console Station. If the CDA or SR services have failed, you might not be getting data updates from CDA. CDA data might appear in inverse video and No Tag alarms might be generated.

Corrective actions

Go to the services and check that both the Experion PKS System Repository service and the Experion PKS Control Data Access Server service are running.

Check the connection to CDA. If the status of data or notifications is not OK and/or you are not receiving data updates from CDA, go to the services and start the Experion PKS Control Data Access Server service. You may also need to start the Experion PKS System Repository service.

Time to respond

Synchronization is lost immediately when this alarm occurs. Time to respond will depend on assessment of process/site/operations for criticality/risk of losing synchronization.

COMMS - <CStnxx/Server>: Data connection to <system interface name> failed. Access denied to remote server

Potential causes

The Console Station or server has notified that data-channel communication with <system interface name> has failed.

Consequence of inaction

Point parameter data will not be available from the system interface.

Corrective actions

Call up the **System Interfaces Status Summary** display.

Time to respond

Immediately.

COMMS - <CStnxx/Server>: Data connection to <system interface name> is blocked. Remote server is busy

Potential causes

There are three outstanding requests to the system interface that have not returned. Experion will not create any more requests until one of the outstanding requests is returns.

Consequence of inaction

Point parameter data will not be available from the system interface.

Corrective actions

Check that the server the system interface is connected to is functioning correctly.

Time to respond

Immediately

COMMS - <CStnxx/Server>: Data connection to TPS failed. Remote server version is incompatible

Potential causes

The wrong version of TPN Server has been installed.

Consequence of inaction

Point parameter data will not be available from TPS.

Corrective actions

Install the TPN server version that matches the release of Experion being used.

Time to respond

Immediately.

COMMS - <CStnxx/Server>: Notifications from <system interface name>

Potential causes

The Console Station or server has notified that notifications from the system interface are unavailable.

Consequence of inaction

Notifications will not be available from the system interface.

Corrective actions

1. Call up the **System Status** display.
2. Check that the network connection between the Experion server and the system interface is working correctly.

Time to respond

Immediately.

COMMS - <CStnxx/Server>: Notifications from <system interface name> failed. Access denied to remote server

Potential causes

The local server has notified that notification-channel communication with the remote system interface has failed due to access restriction.

This is commonly caused by incorrect *mngr* password or incorrect RPC setup.

Consequence of inaction

Notifications will not be available from the system interface.

Corrective actions

1. Check that the *mngr* account password is same on both servers.
2. Check that there nothing preventing RPC from communicating between the Experion server and the system interface, such as a firewall or Windows settings.

Time to respond

Immediately.

COMMS - Data Srv on <server name> OVERLOADED

Potential causes

Data from the DSA remote server may not be current due to overload. The remote server may be experiencing high system load and is having trouble sending data to the local server.

Consequence of inaction

Station might display outdated parameter values from this connection.

Corrective actions

1. Call up the **Console Station Status Detail** display.
2. Use Windows Performance Monitor on the remote server to make sure CPU load and free memory are within the Experion Specification limits. The Experion Specification is available from Honeywell.

Time to respond

If the values are changing regularly or the Overload is intermittent, it may be acceptable to take corrective action as soon as suitable technicians are available, but not necessarily immediately.

COMMS - Door Open

Potential causes

Printing failed due to open printer door.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to Failed, at which time subsequent print requests will be discarded.

Corrective actions

Check that all printer doors and enclosures are closed.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Failed - Cannot Access

Potential causes

Access to the printer is denied.

Consequence of inaction

Print of alarm events or report failed and will not be retried. Whilst the alarm is active, subsequent event and report print requests will be discarded.

Corrective actions

Check that the printer name and Windows access rights are correct.

- If the printer is a network printer:
  1. Check that the printer name or URL (network address) is spelled correctly.
  2. Check that the current logon security level user group has access rights to the Windows printer and to the computer hosting the Windows printer.
- If the printer is an Experion system printer:
  1. Check that the printer **Name** property on the Experion server **Printer Summary** display exactly matches the Windows printer name configured on the Experion server computer.
  2. Check that the current logon security level user group for Station has access rights to the Windows printer defined as the Experion system printer.

> **Attention**
> For the printing of Experion reports or alarms and events, the Experion server uses the *mngr* account and password as defined on the Experion server to gain access to the system printer and computer hosting the system printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Failed - Could Not Print

Potential causes

Printing failed.

Consequence of inaction

Print of alarm events or report failed and will not be retried. Whilst the alarm is active, subsequent event and report print requests will be discarded.

Corrective actions

Check that the printer is working correctly.

Use Windows print manager to print a test page to that printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Failed - Printer Not Found

Potential causes

The printer was not found.

Consequence of inaction

Print of alarm events or report failed and will not be retried. Whilst the alarm is active, subsequent event and report print requests will be discarded.

Corrective actions

Check that the printer name and Windows access rights are correct.

- If the printer is a network printer:
  1. Check that the printer name or URL (network address) is spelled correctly.
  2. Check that the current logon security level user group has access rights to the Windows printer and to the computer hosting the Windows printer.
- If the printer is an Experion system printer:
  1. Check that the printer **Name** property on the Experion server **Printer Summary** display exactly matches the Windows printer name configured on the Experion server computer.
  2. Check that the current logon security level user group for Station has access rights to the Windows printer defined as the Experion system printer.

> **Attention**
> For the printing of Experion reports or alarms and events, the Experion server uses the *mngr* account and password as defined on the Experion server to gain access to the system printer and computer hosting the system printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Link 0 (LNK00)

Potential causes

Redundancy data link 0 failed.

1. The link has re-established. However, the alarm still exists because it has not been acknowledged.
2. The backup server is not operational or is not connected to the network.
3. There is an invalid or missing entry in the hosts file on one or both of the Experion servers.
4. There is a problem with the network connection between Servers A and B.

Consequence of inaction

Redundancy of links has been lost if Link 1 is configured and remains operational on a dual link configured system. If both links have failed, the No Links Available alarm will be raised.

Corrective actions

1. Acknowledge the alarm.
2. Investigate why the backup server is not operational. Start the backup server and make sure that it is connected to the network.
3. Correct the hosts file on both servers.
4. Verify communications between the Servers using 'ping' command or accessing network shares.
5. Verify on the **Server Redundancy Status** display that the link has been restored, and then re-synchronize the backup and primary servers. For more information, see “Synchronizing the server databases”.

Time to respond

Time to respond will depend on availability of Link 1 (if configured) and an assessment of process/site/operations for criticality/risk of losing synchronization between servers.

COMMS - Link 1 (LNK01)

Potential causes

Redundancy data link 1 failed.

1. The link has re-established. However, the alarm still exists because it has not been acknowledged.
2. The backup server is not operational or is not connected to the network.
3. There is an invalid or missing entry in the hosts file on one or both of the Experion servers.
4. There is a problem with the network connection between Servers A and B.

Consequence of inaction

Redundancy of links has been lost if Link 0 is configured and remains operational on a dual link configured system. If both links have failed, the No Links Available alarm will be raised.

Corrective actions

1. Acknowledge the alarm.
2. Investigate why the backup server is not operational. Start the backup server and make sure that it is connected to the network.
3. Correct the hosts file on both servers.
4. Verify communications between the Servers using 'ping' command or accessing network shares.
5. Verify that link has been restored on **Server Redundancy Status** display, and then re-synchronize the backup and primary servers. For more information, see “Synchronizing the server databases”.

Time to respond

Time to respond will depend on availability of Link 0 (if configured) and an assessment of process/site/operations for criticality/risk of losing synchronization between servers.

COMMS - Low On Toner

Potential causes

The printer is running low on toner.

Consequence of inaction

Printing will continue but might not be of the expected quality.

Corrective actions

Replace the toner in the printer.

Time to respond

At the discretion of the users, based on the quality of printing.

COMMS - No Links Available

No redundancy data links are available.

Potential causes

1. The link has re-established. However, the alarm still exists because it has not been acknowledged.
2. The backup server is not operational or is not connected to the network.
3. There is an invalid or missing entry in the hosts file on one or both of the Experion servers.

Consequence of inaction

It is not possible to synchronize the backup servers without an available link, so the backup server database shall not be updated with the changes on the primary (including point configuration, history, events, etc.) and some automatic failover actions will not be triggered. If the link has failed due to network connection failure between Servers A and B, then both Servers A and B may both run as primary.

Corrective actions

1. Acknowledge the alarm.
2. Investigate why the backup server is not operational. Start the backup server and make sure that it is connected to the network.
3. Correct the hosts file on both servers.
4. Verify communications between the Servers using 'ping' command or accessing network shares.
5. Verify that link has been restored on **Server Redundancy Status** display, and then re-synchronize the backup and primary servers. For more information, see “Synchronizing the server databases”.

Time to respond

Synchronization is lost immediately when this alarm occurs. Time to respond will depend on assessment of process/site/operations for criticality/risk of losing synchronization.

COMMS - Offline

Potential causes

The printer is offline.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Turn on the printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Out of Paper

Potential causes

The printer is out of paper.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Place more paper in the printer's paper tray.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Out Of Service

Potential causes

The printer is out of service.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

To diagnose the problem, see the “The printer does not print anything” topic.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Out Of Toner

Potential causes

The printer is out of toner.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Replace the toner in the printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Output Bin Full

Potential causes

The printer's output bin is full.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Empty the output bin (tray) on the printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Paper Jam

Potential causes

Printing failed due to paper jam.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Clear the paper jam in the printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Paper Problem

Potential causes

Printing failed due to paper related problems.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Check the printer for paper problem.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Paused

Potential causes

The printing is paused.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Un-pause the printing.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Peer Version Match

Potential causes

Occurs when the redundancy primary and backup database versions don't match, and again when they are matched (after having been mismatched).

Consequence of inaction

Backup Server is not available or cannot be synchronized when database versions are mismatched (see corrective actions).

Corrective actions

Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.

- If the backup server status is Failed:

  Check that server A and server B are the same version.
- If the backup server status is Good:

  Notification and logging purposes only. No operator interaction is required.

If the alarm occurs during an On Process Migration (OPM), capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

When this alarm is raised, backup may already be unavailable. The time to respond will depend on assessment of process/site/operations for criticality/risk of running without backup server available.

COMMS - Primary: Unknown Status

Potential causes

CDA or SR services on the primary server may have been stopped or failed, or the system may be experiencing network issues.

Consequence of inaction

If the CDA or SR services have failed, you may not be getting data updates from CDA. CDA data may appear in inverse video and No Tag alarms may be generated.

Corrective actions

Go to the Server Redundancy display and check the System Repository backup status. If the status is 'Stopped,' go to the services and start the Experion PKS System Repository service. You may also need to start the Experion PKS Control Data Access Server service.

Check the connection to CDA. If the status of data or notifications is not OK and/or you are not receiving data updates from CDA, go to the services and start the Experion PKS Control Data Access Server service. You may also need to start the Experion PKS System Repository service.

Time to respond

Immediate.

COMMS - Printer Error

Potential causes

The printer has an error.

Consequence of inaction

Event or report has been sent to printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Check the printer operation.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - SAM connection failed

Potential causes

The Server is unable to connect to the Server Activity Manager (SAM) because the service has stopped. The resulting alarm is raised only on the server, and is replicated to Console Stations.

Consequence of inaction

While the connection is in a failed state it is not possible to:

- Create activities through the Activity Creation interface
- Create activities programmatically through MES 3
- Edit the unit for Class Based Recipe activities

Corrective actions

Restart the SAM service.

Acknowledge the alarm.

Time to respond

Immediate.

COMMS - Server: Data connection to <server name>

Potential causes

The local server has notified that data-channel communication for the mentioned connection (<server name>) has failed.

Consequence of inaction

Data from the mentioned connection (<server name>) will be unavailable. The connection may be a remote DSA server or a local data source such as CDA or TPS. If the data is historized on this server, history samples will not be collected.

Corrective actions

1. Call up the **DSA Status** display for the remote server.
2. Check that the network connection between the two servers is working correctly.

If the mentioned connection (<server name>) is a local data source, such as CDA or TPS:

1. If the mentioned connection (<server name>) is CDA, call up the **Server redundancy status** display and check the System Repository backup status. If the status is “Synchronizing” or “Not synchronized”, wait until the System Repository backup status is “Synchronized” and then check if the CDA connection has been re-established.
2. Otherwise, fail over the server and check whether this restores the connection.
3. For additional assistance resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation. For more information, see the “Creating a diagnostic package for TAC” topic.

Time to respond

The corrective action should be initiated immediately to restore view to data from the mentioned connection (<server name>).

COMMS - Server: Data connection to <server name> failed. Access denied to remote server

Potential causes

The local server has notified that DSA data-channel communication with the DSA remote server has failed due to access restriction.

Consequence of inaction

Data from the mentioned connection will be unavailable.

Corrective actions

1. Call up the **DSA Status** display for the remote server.
2. Check that the mngr account password is same on both servers.
3. Check that there isn't anything preventing RPC from communicating between the two servers, such as a firewall or Windows settings.

Time to respond

The corrective action should be initiated immediately to restore view to data from the mentioned connection.

COMMS - Server: Data connection to <server name> is blocked. Remote server is busy

Potential causes

The local server has notified that the DSA data-channel with the DSA remote server is blocked due to the remote server not responding in a timely manner.

Consequence of inaction

The local server (and all Flex Stations and Console Stations connected to it) will not be able to view data from the DSA remote server.

Corrective actions

1. Call up the **Station Status Detail** display for the remote server.
2. Use Windows Performance Monitor on the remote server to make sure CPU load and free memory are within the Experion Specification limits. The Experion Specification is available from Honeywell.

Time to respond

Immediately.

COMMS - Server: Failed - Access Is Denied

Potential causes

The server has reported that access to the printer is denied.

Consequence of inaction

Printing of alarm events or report failed and will not be retried. Whilst the alarm is active, subsequent alarm events and report print requests will be discarded.

Corrective actions

Check that the *mngr* account is setup with the correct permission to access the printer.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

COMMS - Server: Link to <server name>

Potential causes

The local server has notified that DSA link-channel communication with the DSA remote server has failed.

Consequence of inaction

Data and notifications from the mentioned connection will be unavailable and not accessible on Stations in this subscribing Experion cluster.

Corrective actions

1 Call up the **DSA Status** display for the remote server.

2 Check that the network connection between the two servers is working correctly.

Time to respond

The corrective action should be initiated immediately to restore view to data and notifications from the mentioned DSA remote server.

COMMS - Server: Link to <system interface name>

The server has notified that communication with the system interface has failed.

Consequence of inaction

Point parameter data and notifications will not be available from the system interface.

Corrective actions

1. Call up the **System Status** display.
2. Check that the network connection between the Experion server and the system interface is working correctly.

Time to respond

Immediately.

COMMS - Server: Notifications from <server name>

Potential causes

The local server has notified that DSA notification-channel communication with the DSA remote server has failed.

Consequence of inaction

Notifications from the mentioned connection will be unavailable. The connection may be a remote DSA server or a local source such as CDA or TPS. Existing notifications will show in Station as 'bad quality', and no new or changed notifications will be received.

Corrective actions

1. Call up the **DSA Status** display for the remote server.
2. Check that the network connection between the two servers is working correctly.

If the mentioned connection is a local source, such as CDA or TPS:

1. Fail over the server and check whether this restores the connection.
2. For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation. For more information, see the “Creating a diagnostic package for TAC” topic.

Time to respond

The corrective action should be initiated immediately to restore view to notifications from the mentioned connection.

COMMS - Server: Notifications from <server name> failed. Access denied to remote server

Potential causes

The local server has notified that DSA notification-channel communication with the DSA remote server has failed due to access restriction.

This is commonly caused by incorrect *mngr* password or incorrect RPC setup.

Consequence of inaction

Notifications from the mentioned connection will be unavailable.

Corrective actions

1. Call up the **DSA Status** display for the remote server.
2. Check that the *mngr* account password is same on both servers.
3. Check that there isn't anything preventing RPC from communicating between the two servers, such as a firewall or Windows settings.

Time to respond

The corrective action should be initiated immediately to restore view to notifications from the mentioned connection.

COMMS - Station Failure

Potential causes

Either a Flex Station or a Console Station has been disconnected from the server or Console Station because of:

- A Station being shut down
- A network failure
- A hardware failure

Consequence of inaction

Loss of view on the Station.

Corrective actions

1. Call up the **Station Status Detail** display or the **Console Station Status Detail** display.
2. Check that the Station or Console Station is running.
   - If a Station is shut down, reopen the Station.
   - In the case of a network failure, check that the network connection between the Flex Station or Console Station is operational.

Time to respond

Immediate.

COMMS - Synchronization

Potential causes

Indicates that redundant server synchronization has been lost.

Consequence of inaction

Server synchronization has failed, so the backup server database shall not be updated with the changes on the primary (including point configuration, history, events, etc.) and some automatic failover actions will not be triggered.

Corrective actions

1. Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.
2. Re-synchronize the system. For more information, see “Synchronizing the server databases”.

If synchronization continues to fail, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Synchronization is lost immediately when this alarm occurs. Time to respond will depend on assessment of process/site/operations for criticality/risk of losing synchronization.

COMMS - User Intervention Required

Potential causes

User intervention is required to continue printing.

Consequence of inaction

An event or report has been sent to the printer but will not be printed until the problem is rectified. Subsequent requests will be queued on the printer until the alarm becomes Urgent and Active and the printer status changes to failed, at which time subsequent print requests will be discarded.

Corrective actions

Attend to the printer. Check the printer control panel for an indication of the error. See the printer's documentation for instructions on how to resolve the problem.

Time to respond

Immediate action is recommended if a paper record of all events and periodic reports is important.

DIAG system alarms

The following topics describe diagnostic-related system alarms and how to respond to them.

Related topics

DIAG - A/D Failure

Potential causes

Diagnostics detected defect with Analog to Digital Converter.

Consequence of inaction

Device is offline.

Corrective actions

Replace sensor module.

Time to respond

DIAG - Activity Create Failed

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

If the creation of a new batch activity module is requested when the number of current activity modules running is equal to the number of activity modules set by a user, this alarm is raised.

Consequence of inaction

The activity cannot be created.

Corrective actions

Increase the NUMACT value. NUMACT cannot be 0 or greater than 500.

DIAG - Address Overlap

Applies to SLINK.

Potential causes

An overlap is detected when the starting address of the SIOM plus the slot configuration overlaps with the starting address of the next SIOM. The two SIOMs can be on one or different links. In this situation, only one of the SIOMs comes online and the other SIOM reports an overlap condition on its link and this is reported from primary LIOM.

Consequence of inaction

One of the overlapped SIOM works, while the other SIOMs will not work.

Corrective actions

Assign unique addresses for SIOMs.

Time to respond

Immediate.

DIAG - Asymmetric Response From Probe

Potential causes

Electrochemical response of the probe is not symmetrical.

Consequence of inaction

Incorrect PV.

Corrective actions

Check electrodes for differential attack on electrodes, for example, crevice on one electrode.

Time to respond

DIAG - Backup RAM Scrub Errors

Applies to C300.

Potential causes

The number of bit errors detected and corrected in testing of RAM in which the C300 controller maintains control strategies is greater that than the number determined acceptable. This alarm is referred as corrected RAM sweep error.

Consequence of inaction

A possibility for a backup RAM Sweep Error.

Corrective actions

Consider replacing the C300 controller. Call the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

If the alarm occurs frequently, module replacement should be considered at earliest convenience.

DIAG - Backup RAM Sweep Errors

Applies to C300.

Potential causes

The bit errors detected during testing of the RAM in which the C300 controller maintains control strategies are unable to be corrected. This alarm is referred to as uncorrected RAM sweep errors.

Consequence of inaction

Might cause unexpected behaviors in the process controller.

Corrective actions

The C300 controller needs to be replaced immediately. Call the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

Immediately.

DIAG - Backup State

Applies to C200E, C300, CPMC200, and LIOM.

Potential causes

The secondary generates the Backup State Change Event as part of event regeneration. More specifically, a transition to the Backup State only occurs as part of startup or redundancy role change. For both of these cases, any previously existing notification connection is broken, a new notification connection is reformed, and event regeneration is commanded.

Consequence of inaction

None – expected.

Corrective actions

Normal for backup module/chassis.

Time to respond

N/A.

DIAG - Bad Configuration

Potential causes

Active Diagnostic channel requesting data, when no diagnostic buffer has been configured at the device function block.

Consequence of inaction

Loss of diagnostic data.

Corrective actions

Reconfigure the diagnostic buffer at the device function block.

Time to respond

Immediate.

DIAG - Battery Not OK

Applies to C200E and CPMC200.

Potential causes

Defective battery or invalid battery configuration.

Consequence of inaction

A power failure will result in the loss of configuration.

Corrective actions

Replace the defective battery or correct the invalid battery configuration.

The Battery Extension Module or Lithium battery may be used, but not both. Both batteries have a replacement schedule.

Time to respond

Next maintenance shift.

DIAG - Battery Over Voltage

Applies to C300.

Potential causes

If battery voltage is above 4.8V this alarm is raised. This condition indicates that the battery has been removed or has become open circuit.

Consequence of inaction

This may damage the RAM in the controller and cause the controller to fail. All controllers connected to this battery supply will be affected by this condition.

Corrective actions

Check that the battery is connected and that all wiring is intact. The battery may need to be replaced. Contact your Honeywell Technical Assistance Center for further support.

Time to respond

Next maintenance shift.

DIAG - Battery Under Voltage

Applies to C300.

Potential causes

This alarm is raised if the battery voltage is below 3V. This condition indicates a discharged or defective battery. If discharged due to a system power outage, it should clear in 8-10 hours.

Consequence of inaction

A discharged battery may result in memory loss within the controller. It may require a checkpoint restore and cold start of the controller. All controllers connected to this battery supply will be affected by this condition.

Corrective actions

If this occurs while the system is running, the battery will need to be replaced. Contact your Honeywell Technical Assistance Center for further support.

Time to respond

Before next power failure.

DIAG - BOOTP Enabled

Potential causes

The BOOTP setting of the specified ENET module has not been disabled after updating the ENET module's IP address.

Consequence of inaction

Loss of Communication.

Corrective actions

Utilize the Network Tools application to disable the BOOTP setting of the specified ENET module.

Time to respond

Immediate.

DIAG - Calibration Cleared

Potential causes

User calibration cleared to factory constants. Indicates that both the upper and lower trim points as well as the zero offset has been cleared. The calibration source is none.

Consequence of inaction

Incorrect PV.

Corrective actions

User calibration has been cleared and reset to the factory values. Proceed with user calibration if utilizing probe cables longer than 12 ft and if the anticipated corrosion rate is greater than 200 mpy.

- Select Factory Calibration; or
- Calibrate the zero offset; or
- Calibrate using the lower and upper trim points.

Time to respond

DIAG - Calibration Error

Potential causes

Calibration data invalid or could not be read.

Consequence of inaction

Incorrect PV.

Corrective actions

- Reattempt user calibration.
- Use Cal Clear, Restore, or User Calibrate.

Time to respond

DIAG - CEE Cycle Overruns

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

This alarm occurs if the CPU consumption by the loaded strategies exceeds 100%.

Consequence of inaction

A watchdog timer failure might occur and controller scheduling latency will be higher, resulting in loss of real time nature.

Corrective actions

Reduce the load on the CPU by reducing strategies, and fine tuning phase and order in CEE and CMs.

Time to respond

As early as possible.

DIAG - CEE Hold Breath

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

The term "Hold Breath" refers to stopping normal execution of scheduled function blocks in an ACE CEE because peer pre-fetch data is not available for execution of an ACE Control Module configured for pre-fetch. An ACE Control Module configured for pre-fetch triggers collection of peer data in anticipation that peer data will be available during execution of the ACE Control Module.

The CEE stops execution (hold’s breath) of all (with and without pre-fetch) control strategies, when pre-fetch data is not available prior to scheduled execution for an ACE Control Module. Communication delays long enough to cause the CEE to Hold Breath is rare and usually associated only with either a swap or switch over of a server node.

Consequence of inaction

When a hold breath occurs, the CEE holds execution of all its blocks regardless of whether its PEERREADOPT parameter setting is PREFETCH or PUBSUB. This means all Control Modules along with all SCM, RCM, and UCM in the control strategy will stop executing for the duration of the Hold Breath timeout time.

The CEE does not attempt to recover the scheduling time lost due to the occurrence of Hold Breath.

Corrective actions

- Occurrence of Hold Breath when an HPM point is deleted.

  When the ACE is subscribed to an HPM point that is deleted, the ACE may report Hold Breath events as long as it attempts to access the deleted point. The Hold Breath occurrence increases significantly until the HPM point is re-loaded. In such a scenario, you must remove all ACE references to the deleted point.
- Occurrence of Hold Breath during NIM/HG/AM node failover.

  It is possible that the pre-fetch requests from ACE targeted to LCN data owners may get lost when LCN data owners like NIM/HG/AM failover. During this time, the responses for the pre-fetch requests are not received at the ACE. As a result, Hold Breath can occur on the ACE node. In such a scenario, Hold Breath events occur until the data arrives or until the Hold Breath timeout occurs; whichever is earlier.

Time to respond

DIAG - Channel Hardware Fault

Potential causes

Hardware failure.

Consequence of inaction

Process disruption.

Corrective actions

1. Check the channel status on the card.
2. Replace the I/O card.

Time to respond

Immediate.

DIAG - Characterization Error

Potential causes

Either the sensor cannot access the meter body characterization, or the characterization is invalid.

Consequence of inaction

Incorrect PV.

Corrective actions

Check the connection between the sensor module and the meter body. If this doesn't fix the problem, replace the sensor.

Time to respond

DIAG - Checkpoint Save Status

Potential causes

An error has occurred when saving a Checkpoint. Additional information about the specific error can include:

- Failed/abnormal completion; state of the last checkpoint save for that node. This is indicated by one of the following values in the Checkpoint Status (CPSTATUS):
  - Complete With Stale Data
  - Complete With Dangling Data
  - Complete With Mismatched Data
  - Failed – Other, see server err logs
- RTN - Successful completion; state of the last checkpoint save for that node. This will be indicated by the value “Complete” in CPSTATUS.

Consequence of inaction

Inability to migrate.

Corrective actions

See the following topics in the “Appendix F - Control Builder Checkpoint Reference” section of the *Control Building User's Guide*.

- “Checkpoint file attributes”
- “Checkpoint Alarming”
- “Fixing Common Problems”

Time to respond

Next Checkpoint save.

DIAG - CJ Failure

Potential causes

The Cold Junction has failed.

Consequence of inaction

Input failure.

Corrective actions

Check the connectors on the terminal board and the sensor module. If necessary, replace the terminal board.

Time to respond

DIAG - Cold Junction Fault

Potential causes

Broken lead or a shorted lead to the CJ compensation thermistor.

Consequence of inaction

1. All channels are marked as bad.
2. If a broken lead is detected, 70 C is substituted for the CJC temperature in all calculations.
3. If a short-circuit is detected, 0 C is substituted for the CJC temperature in all calculations.

Corrective actions

Check leads and correct/replace them.

Time to respond

Immediate.

DIAG - Communication Ceased

Applies to SLINK.

Potential causes

When an SIOM goes offline on a serial link, communication on the corresponding serial link, or both serial links, cease operation depending on the serial link fault configuration.

Consequence of inaction

Corrective actions

Enter the command `Restart Slinks` at the LIOM FB configuration form.

Time to respond

As soon as possible.

DIAG - Communication Error

Potential causes

1. Power is disrupted to the I/O chassis.
2. The interface module (for example, CNI, Profibus Interface Module, or DeviceNet Interface Module) has been removed.
3. The controller to interface communication path is broken.
4. The I/O Module has faulted or been removed from the chassis.

Consequence of inaction

Controller to IOM communication connection is broken and results in data loss.

Corrective actions

1. Check the I/O Module to make sure it is not faulted or unpowered.
2. Check the I/O Rack PS and restore power supply if unpowered.
3. Check any interface module in the communication path to make sure that it is not faulted or unpowered.
4. Check the communication path.

Time to respond

Immediate.

DIAG - Communication Fault

Potential causes

- The associated IOM Function Block loses communication with the Communications Adapter
- The associated Communications Adapter losses communication with or detects a major fault on the drive device.

Consequence of inaction

Connections to the drive are lost. The drive goes into the Faulted state, drive behavior is based on the Communications Adapter configuration.

Corrective actions

Restore the cable connection or Communications Adapter.

Time to respond

Immediate.

DIAG - Communication With This Point Is Lost. Load Server Point Immediately

Potential causes

The top-level block has not been loaded.

Consequence of inaction

Loss of communication.

Corrective actions

Check for devices with EEs that are missing a top level block. Load server point (top level block).

Time to respond

Immediate.

DIAG - Configuration Error

Potential causes

Invalid, inconsistent, corrupted, or lost static data.

Consequence of inaction

User cannot modify static data.

Corrective actions

None.

Time to respond

DIAG - Connection Error

Potential causes

The DTL connection has failed.

Consequence of inaction

Loss of communication.

Corrective actions

If the disconnection is unexpected and unexplained, examine the alarm summary, network communication nodes, network connectors and network cabling for the source of the network fault.

Time to respond

Immediate.

DIAG - Connection Failed

Potential causes

The DTL connection has failed.

Consequence of inaction

Loss of communication.

Corrective actions

If the disconnection is unexpected and unexplained, examine the alarm summary, network communication nodes, network connectors and network cabling for the source of the network fault.

Time to respond

Immediate.

DIAG - Connection Timeout

Potential causes

The DTL connection has failed.

Consequence of inaction

Loss of communication.

Corrective actions

If the disconnection is unexpected and unexplained, examine the alarm summary, network communication nodes, network connectors and network cabling for the source of the network fault.

Time to respond

Immediate.

DIAG - CPU Free Low Alarm

Applies to C300.

Potential causes

When the available CPU resource falls below the limit set in the C300 Controller FB parameter CPULOLM, this alarm is generated at Low priority.

Consequence of inaction

May cause frequent overruns.

Corrective actions

Reduce values for items such number of blocks, adjusting period, phase, and order of execution.

Time to respond

As early as possible.

DIAG - CPU Low Low Resources

Applies to C300.

Potential causes

When the available CPU resource falls below 5% this diagnostic alarm is generated at High priority.

Consequence of inaction

Multiple phase overruns may occur and the controller response time might be impacted. There is also the possibility of a watchdog timer crash.

Corrective actions

Reduce values for items such number of blocks, adjusting period, phase, and order of execution.

Time to respond

As early as possible.

DIAG - DAC Voltage Deviation

Potential causes

The electrode driver voltage deviation is greater than 3% of measured voltage.

Consequence of inaction

Incorrect PV.

Corrective actions

- Check electrodes for conductive films.
- Check transmitter probe cable connections for a possible short at the transmitter input terminals.
- Check transmitter operation offline with a different probe to determine if the fault is caused by the probe or the transmitter.

Time to respond

DIAG - Daughter Board Fail

Potential causes

The FIM daughter board has failed.

Consequence of inaction

Loss of synchronization. Potential loss of process data/loss of control.

Corrective actions

1. Use the NDM generated Point ID (for example, Driver Name : RM0203) and the given slot number in the description to identify the FIM with the daughter board failure.
2. Restart the module.
3. If the problem persists, replace the FIM hardware.

Time to respond

Immediate.

DIAG - Debug Flag Enabled

Applies to FIM4, FIM8, C300, and PGM .

Potential causes

From the EPIC Program Analyzer tool – the Debug Flag is set.

Consequence of inaction

If the user performs unprivileged debug operations from the CTOOL/EPA tool, the on-process system might be disturbed.

Corrective actions

When the Epic Program Analyzer tool is connected to an on-process controller, deselect the Debug Flag in the EPA tool.

Time to respond

As soon as possible.

DIAG - Debugger Is Running

Applies to CEEACEFB, CEEC200EFB, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

A check for Visual Studio remote debuggers is done during the transition from IDLE->RUN. This alarm is raised if debuggers are found running, and the transition is disallowed.

Consequence of inaction

The CEE cannot transition from IDLE to RUN while a debugger is running.

Corrective actions

Turn off the debugger (VC++).

Time to respond

When possible.

DIAG - Device Fail

Potential causes

The device has failed or is not operating correctly.

Consequence of inaction

DNet Interface Module will no longer be able to communicate with the failed device. Affects many device blocks.

Corrective actions

Replace the device.

Time to respond

Immediate.

DIAG - Device/Firmware Mismatch

Potential causes

Sensor board firmware error. The software did not pass verification tests. The sensor firmware does not match the device type.

Consequence of inaction

Device offline.

Corrective actions

Replace sensor module.

Time to respond

DIAG - Device Idle

Potential causes

The EXECSTATE of the device is INACTIVE.

Consequence of inaction

Causes a break in the communication between device blocks and the DeviceNet network.

Corrective actions

Set the block execution status of the DNET_IM block to ACTIVE.

Time to respond

Immediate.

DIAG - Device Index Setting Does Not Match Displayed Value

Applies to FIM4, FIM8, C300, and PGM .

Potential causes

1. Someone changed the setting on the binary-coded decimal rotary switches on the IOTA.
2. The Primary or non-redundant Series C FIM is defective.
3. The redundant or non-redundant IOTA is defective.
4. There is a software problem.

Consequence of inaction

With the next reboot, the system will take up a different IP address.

Corrective actions

1. Change binary-coded decimal rotary switches to correct setting.
2. Replace the Primary or non-redundant Series C FIM. If the Device Index switch setting matches the Device Index number in the 4-character display upon Series C FIM power up, the removed Series C FIM is defective.
3. Replace the IOTA. If the Device Index switch setting matches the Device Index number in the 4-character display upon Series C FIM power up, the removed IOTA is defective.
4. Contact Honeywell Solution Support Center (SSC) for assistance.

Time to respond

Immediate.

DIAG - Device Index Switches Changed

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

Device address is set using jumpers before booting the controller. If this is modified during run time, this alarm is raised.

Consequence of inaction

With the next reboot, the system will take up a different IP address.

Corrective actions

Verify if the Device Index switch setting is correct, reset if necessary. If failure persists, the IOTA may be defective. Replace the IOTA.

Time to respond

Immediate.

DIAG - Device Index Value Is Zero Upon Power Up

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

1. Binary-coded decimal rotary switches are set to zero on IOTA.
2. The Primary or non-redundant Series FIM4 (or FIM8) is defective.
3. The redundant or non-redundant IOTA is defective.

Consequence of inaction

With the next reboot, the system will not acquire the appropriate IP address and it will not boot up.

Corrective actions

1. Change the binary-coded decimal rotary switches to the correct setting.
2. Replace the Primary or non-redundant Series C FIM. If the Device Index switch setting matches the Device Index number in the 4-character display upon Series C FIM power up, the removed Series C FIM is defective.
3. Replace the IOTA. If the Device Index switch setting matches the Device Index number in the 4-character display upon Series C FIM power up, the removed IOTA is defective.

Time to respond

As soon as possible.

DIAG - Device Mismatch

Potential causes

The configuration of the device in RSNetWorx is not the same as the data received by the DNet Interface.

Consequence of inaction

Device data split between assemblies may not match.

Corrective actions

1. Disable DNet interface.
2. Recheck the device configuration in the RSNetWorx and reload.

Time to respond

Immediate.

DIAG - Device Not Configured

Potential causes

PROFIBUS network is not configured with a device with the specified Station/module numbers.

Consequence of inaction

Fails to identify the PBIM block that will serve its I/O data.

Corrective actions

Configure the PROFIBUS device to identify the associated PBIM blocks that serve the I/O data.

Time to respond

Immediately.

DIAG - Device Offline

Potential causes

The slave device is absent or returning errors on the PROFIBUS network.

Consequence of inaction

The slave remains offline with the active master. The master actively updates the slave, producing a faulty message, increasing the retries count each time.

Corrective actions

1. Check the device and reconfigure the slave device.
2. Replace the device if required.

Time to respond

Immediate.

DIAG - Device Registration Error

Potential causes

The device block could not be registered with the appropriate DNET_IM block.

Consequence of inaction

Device load error due to failed communication between the device block and one or more than one DeviceNet IM.

Corrective actions

Ensure a matching configuration between DNET_IM table and IOM block, including device address and data offsets that correspond to the data expected by the block.

Time to respond

Immediate.

DIAG - DeviceNet IM Comm Error

Potential causes

1. Power is disrupted to the remote chassis in which the DNB-1756 resides.
2. The DNB-1756 is removed under power.
3. The controller to DNet Interface ControlNet communication path (assuming remote I/O) is broken.

Consequence of inaction

Controller and the DNet Interface are no longer able to transfer data between each other resulting in incomplete/ outdated information on the Status tab.

Corrective actions

1. Check the I/O Module to make sure it is not faulted or unpowered.
2. Check the chassis power supply, in which the Dnet Interface module resides and restore power supply if unpowered.

Time to respond

Immediate.

DIAG - DeviceNet_IM Disabled

Potential causes

The DNET_IM block is DISABLED.

Consequence of inaction

When in Disable mode the DNB will not make an attempt to communicate on the network. The message “Network Disabled” is displayed on the front of the DNB.

Corrective actions

Rectify the system error detected by the application logic and enable the communication of the device net block on the DeviceNet network by restoring the status to RUN.

Time to respond

Immediate.

DIAG - DeviceNet IM Duplicate Address

Potential causes

The DNet interface is attempting to go online on a DeviceNet network with the same node number as an existing device on the network.

Consequence of inaction

DNet device fails to operate.

Corrective actions

Check the DNet interface module address and ensure it matches the actual device net address. Ensure that no duplicate device addresses exist.

Time to respond

Immediate.

DIAG - DeviceNet IM Faulted

Potential causes

The DNET_IM is in FAULTY state.

Consequence of inaction

When in Fault mode the DNB will not make an attempt to communicate on the network. The message “Network Faulted” will be displayed on the front of the DNB.

Corrective actions

Rectify the system error detected by the application logic and then enable the communication by restoring the device status to RUN.

Time to respond

Immediate.

DIAG - DeviceNet IM Idle

Potential causes

The DNET_IM is in IDLE state.

Consequence of inaction

When in IDLE mode, the DNB block will not receive inputs from devices on the network, and will not send active output data to the devices.

Corrective actions

Rectify the system error detected by the application logic and restore the device status to RUN.

Time to respond

Immediate.

DIAG - DeviceNet IM Not Active

Potential causes

DNET_IM block is INACTIVE.

Consequence of inaction

I/O data is not transferred between the DNET_IM block and the DNet Interface module, i.e. it causes a break in the communication between device blocks and the DeviceNet network. Fail-safe data is returned to client input blocks.

Corrective actions

Set the block execution status of the DNET_IM block to Active. Any load, reload or snapshot restore initializes the block status to INACTIVE.

Time to respond

Immediate.

DIAG - DeviceNet IM Not Specified

Potential causes

Invalid or missing DNET_IM reference.

Consequence of inaction

DNET_IM serves the device's I/O data. Invalid reference indicates loss of I/O data and fails to detect the device location.

Corrective actions

Reconfigure the DNET_IM (device net interface module) block reference and reload.

Time to respond

Immediate.

DIAG - DeviceNet IM Power Fail

Potential causes

The DNet Interface cannot detect any power on the DeviceNet most likely due to removing power from the DeviceNet Network.

Consequence of inaction

DNet Device fails resulting in communication problems.

Corrective actions

1. Check the power cord or the cable connection to the chassis containing the DNet Interface.
2. Alternatively check if the network connection was not terminated properly.

Time to respond

Immediate.

DIAG - DI Input Fail Alert

Potential causes

Cold junction failure.

Consequence of inaction

Incorrect PV.

Corrective actions

Check the connectors on the terminal board and the sensor module. If necessary, replace the terminal board.

Time to respond

DIAG - Different Amount of Devices

Potential causes

Primary and secondary FIMs detect a different number of devices on the link. Possible RTP or cable failure.

Consequence of inaction

Loss of synchronization. Potential loss of process data and/or loss of control.

Corrective actions

1. Verify Primary FIM detects all devices on the network.
2. Check RTP and cabling.
3. Check segment signal quality.

Time to respond

Immediate.

DIAG - Drive Alarm

Potential causes

A alarm condition (usually a warning) occurs on the associated device .

Consequence of inaction

An alarm is a condition that, if left untreated, may stop the drive. Drive alarms are usually warnings. The FAULTED parameter indicates major drive faults.

Corrective actions

The action to be taken depends on the cause of the alarm (e.g. Analog in Loss, Bipolar conflict, Brake Slipped, power loss). For more information see the Allen-Bradley drive documentation.

Time to respond

Immediate.

DIAG - Drive Fault

Potential causes

A fault condition occurs on the associated device.

Consequence of inaction

Stops the drive operating.

Corrective actions

The action to be taken depends on the cause of the fault (e.g., Analog in Loss, Anlg Cal Chksum, Auto tune aborted). For more information see the Allen-Bradley drive documentation.

Time to respond

Immediate.

DIAG - Duplicate Node Address On Link

Applies to H1 Link.

Potential causes

A second node is on the H1 Link at the same address as the FIM. Typically two FIMs are connected to the same H1 network.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.

Time to respond

Immediate.

DIAG - Electrode Open Circuit or LPR Mode Error

Potential causes

Input open or probe not in solution.

Consequence of inaction

Incorrect PV.

Corrective actions

Check the probe cable for a loose or defective (open) connection to the electrodes or transmitter terminals.

Time to respond

DIAG - Electrode Short Circuit

Potential causes

An input has shorted.

Consequence of inaction

Incorrect PV.

Corrective actions

Check the probe electrodes for conductive films or a defective (shorted) cable. Check the transmitter probe cable connections for a possible short at the transmitter input terminals.

Time to respond

DIAG - Electronics Failure

Potential causes

An electronics failure is detected on the sensor board, as determined by any of the following diagnostic status indicators:

- NVM Fault
- RAM Fault
- Program Memory Fault
- A/D Failure

Consequence of inaction

Device offline.

Corrective actions

Restart both the radio and the sensor. If the condition persists, replace the sensor module.

Time to respond

DIAG - Excess Calibrated Range

Potential causes

The selected calibration points used for upper and lower trim are outside the characterized range of the transmitter.

Consequence of inaction

Incorrect PV.

Corrective actions

Check that the upper and lower trim points are both within the characterized range of the transmitter and re-attempt upper and lower trim calibration.

Time to respond

DIAG - Excess Calibration Correction

Potential causes

User calibration trim point exceeds operational range of probe.

Consequence of inaction

Incorrect PV.

Corrective actions

Re-calibrate using trim points within the operational range of the probe.

Time to respond

DIAG - Excess Span Calibration

Potential causes

The calibrated upper and lower trim has produced a span that is greater than 5% of the characterized span of the transmitter.

Consequence of inaction

Incorrect PV.

Corrective actions

- Clear calibration; or
- Set factory calibration; or
- Check the applied trim points and re-attempt lower and upper (trim) calibration.

Time to respond

DIAG - Excess Zero Calibration

Potential causes

The selected zero offset or the lower calibration trim point is beyond 5% of the lower end of the characterized range of the device.

Consequence of inaction

Incorrect PV.

Corrective actions

Clear calibration.

Time to respond

DIAG - Excessive H1 Link Communication Errors

Applies to H1 Link.

Potential causes

Malformed packets were detected on the H1 link, typically due to faulty wiring or hardware.

Consequence of inaction

Increased latency, stale data or in extreme cases loss of Control, loss of view, loss of synchronization.

Corrective actions

If persistent, verify all wiring and components on the link. Replace or correct the source of the errors.

Time to respond

Immediate

DIAG - Factory Data Error

Applies to FIM4, FIM8, and C300.

Potential causes

Factory Data is programmed into the C300 Controller Flash memory at the time of manufacture. The C300 Controller incorporates a run-time diagnostic to check that this data block is not corrupted. If it is corrupted this alarm is raised.

Consequence of inaction

Loss of control.

Corrective actions

Contact the Honeywell Technical Assistance Center (TAC) to arrange for replacement of the module.

Time to respond

Immediate.

DIAG - Fatal FF Communication Error

Applies to H1 Link.

Potential causes

Occurs on Fieldbus Interface Module (FIM)2 only. Indicates that a fatal exception has occurred on the FIM2 communication co-processor.

Consequence of inaction

Loss of control if non-redundant; loss of synchronization if redundant.

Corrective actions

Contact your Honeywell Technical Assistance Center to diagnose, verify installation, and replace the FIM.

Time to respond

Immediate.

DIAG - Fieldbus devices not communicating or intermittent

Potential causes

Noise, voltage, power supply.

Consequence of inaction

Loss of communication.

Corrective actions

1. Solution 1: Route field signal cables through conduit and at a distance from power cables.
2. Solution 2: Check the power supply. Use a conditioned power supply; ordinary power supply is not suitable.

Time to respond

Immediate.

DIAG - FIM Cable Failure, FIM or RTP Slot

Potential causes

Disconnection or failure of RTP cable or RTP assembly.

Consequence of inaction

Loss of synchronization. If non-redundant, loss of process data and/or loss of control.

Corrective actions

1. Check RTP cabling and assembly.
2. Replace RTP or cable if problems persist.

Time to respond

Immediate.

DIAG - FIM Is Not Primary Link Master

Applies to H1 Link.

Potential causes

The Fieldbus Interface Module (FIM) is not acting as primary link master. Note that FIM is configured to be primary link master by default.

Consequence of inaction

Loss of control.

Corrective actions

Verify that the primary FIM has regained Link Master responsibility.

Time to respond

Immediate.

DIAG - FIM Not Responding

Potential causes

Fieldbus Interface Module (FIM) does not accept downloads. FIM does not show previous configuration.

Consequence of inaction

Loss of communication.

Corrective actions

Clear FIM memory by temporarily placing FIM on a different slot. The change will be detected and the memory reset.

Time to respond

Immediate.

DIAG - FIM Lost Sync

Potential causes

FIM loss of sync.

Consequence of inaction

Loss of synchronization.

Corrective actions

Review the redundancy history on the RM to determine cause of loss of sync.

Time to respond

Immediate.

DIAG - FIM Schedule Error, Not Executing Slot

Potential causes

Function block schedule not executing.

Consequence of inaction

Loss of process data and/or loss of control.

Corrective actions

1. 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.
2. Restart module.
3. If the problem persists, replace FIM hardware.

Time to respond

Immediate.

DIAG - FIM SLOT: XX { Tag Identifier } (Err XX)

Potential causes

Problem with the device listed in the Tag ID.

Consequence of inaction

Loss of synchronization. Potential loss of process data and/or loss of control.

Corrective actions

1. 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.
2. Check segment health to verify signal quality is within the Foundation Fieldbus specifications.
3. Replace the device if problems persist.

Time to respond

Immediate.

DIAG - Firm Ware Error1

Potential causes

ControlNet cable disconnected and/or defective.

Consequence of inaction

Loss of communication.

Corrective actions

1. 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.
2. Restart module.

Time to respond

Immediate.

DIAG - Firm Ware Error2

Potential causes

Buffers not allocated.

Consequence of inaction

Loss of communication.

Corrective actions

1. 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.
2. Restart module.

Time to respond

Immediate.

DIAG - FTA A Communication Error

Potential causes

Loss of communication with the FTA .

Consequence of inaction

Transaction between the IOP and FTA is interrupted.

Corrective actions

Reset the IOP receive buffer index.

Time to respond

Immediate.

DIAG - FTA B Communication Error

Potential causes

Loss of communication with the FTA .

Consequence of inaction

Transaction between the IOP and FTA is interrupted.

Corrective actions

Reset the IOP receive buffer index.

Time to respond

Immediate.

DIAG - FTE Port A Receive Fault

Applies to FIM4, FIM8, C300, FTEB, and PGM.

This alarm is generated specifically and only for an FTE receive path fault on the IOTA, C300, or FIM itself. Disconnection of FTE Cable A or Cable B from the C300 does NOT generate this alarm. Rather a cable disconnection is alarmed by the FTE Status Monitor when it sees no messages transmitted from the C300 on the port from which the cable has been removed.

Potential causes

This alarm is generated specifically and only for an FTE receive path fault. Disconnection of FTE Cable A or Cable B from the C300 is alarmed by the FTE Status Monitor when it sees no messages transmitted from the C300 on the port from which the cable has been removed.

Consequence of inaction

Loss of communication with the controller.

Corrective actions

Unless you suspect that one of the causes described above exists and is resulting in a spurious indication, you should replace the Control module exhibiting this diagnostic as soon as possible.

Time to respond

As soon as possible.

DIAG - FTE Port B Receive Fault

Applies to FIM4, FIM8, C300, FTEB, and PGM.

This alarm is generated specifically and only for an FTE receive path fault on the IOTA, C300, or FIM itself. Disconnection of FTE Cable A or Cable B from the C300 does NOT generate this alarm. Rather a cable disconnection is alarmed by the FTE Status Monitor when it sees no messages transmitted from the C300 on the port from which the cable has been removed.

Potential causes

This alarm is generated specifically and only for an FTE receive path fault. Disconnection of FTE Cable A or Cable B from the C300 is alarmed by the FTE Status Monitor when it sees no messages transmitted from the C300 on the port from which the cable has been removed.

Consequence of inaction

Loss of communication with the controller.

Corrective actions

Unless you suspect that one of the causes described above exists and is resulting in a spurious indication, you should replace the Control module exhibiting this diagnostic as soon as possible.

Time to respond

As soon as possible.

DIAG - Function Block Error

Potential causes

Function Block Schedule not executing.

Consequence of inaction

Loss of synchronization. Potential loss of process data and/or loss of control.

Corrective actions

1. 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.
2. Restart the FIM.
3. Replace the FIM if problems persist.

Time to respond

Immediate.

DIAG - GPS Failed

Applies to C300.

Potential causes

An external GPS-based source is the current master reference for C300 System Time. This event is generated when this GPS source fails.

Consequence of inaction

N/A

Corrective actions

GPS is not yet implemented. So this alarm will not be raised.

Time to respond

N/A

DIAG - H1 Link Communication Error Detected

Applies to H1 Link.

Potential causes

A single malformed packet was detected on the H1 link, typically due to faulty wiring or hardware.

Consequence of inaction

Increased latency or stale data. If not corrected, excessive H1 Link Error alarms may be reported.

Corrective actions

If persistent, verify all wiring and components on the link. Replace or correct the source of the errors.

Time to respond

Immediate.

DIAG - H1 Link Power Failure

Applies to H1 Link.

Potential causes

The Fieldbus Interface Module (FIM) detects incorrect or missing power from an integrated power conditioner. If external power conditioners are used, this diagnostic should be disabled.

Consequence of inaction

Failure of H1 link operations.

Corrective actions

If integrated power conditioners are used, check that the power conditioner is connected to the FIM2 RTP or FIM4/FIM8 IOTA. Integrated power conditioners typically have alarming modules that will detect and report power diagnostics. If external power conditioners are used, this diagnostic should be disabled.

Time to respond

Immediate.

DIAG - Hardware Temperature Exceeded The Threshold

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The temperature of the hardware has exceeded the defined temperature limit in the OVERTEMPTHLD parameter.

Consequence of inaction

May damage some part of the hardware and/or reduce the life time of the controller.

Corrective actions

Check if the parameter value has been lowered from the default and if so, set a more appropriate limit. Also check the cabinet temperature, and whether the cabinet fans and cooling mechanisms are working effectively.

Time to respond

Will vary depending on the threshold limit configured in the OVERTEMPTHLD parameter.

DIAG - Harmonic Distortion Mode Not Possible

Potential causes

No valid 3rd harmonic component available to calculate the B value PV.

Consequence of inaction

Incorrect B value.

Corrective actions

Check for formation of surface films having redox behavior, such as sulfides, which can prevent the electrode from becoming polarized. Check for a diffusion-limiting corroding system.

Time to respond

DIAG - Heap Memory Not Available

Potential causes

Heap allocation failure. Software has detected that there is a heap memory shortage.

Consequence of inaction

Some communication packets may have been dropped.

Corrective actions

Clear by warm restart of device. If the condition persists, contact the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

DIAG - HW Rev Below Acceptable Minimum — Upgrade Required

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The CPLD version in the C300 controller module is not compatible with operations using the current C300 firmware image.

Consequence of inaction

The controller might not work as intended.

Corrective actions

Replace the controller module with a module that meets current hardware specifications.

Time to respond

DIAG - ICP QSend Error

Applies to C200E, CPMC200, LIOM, FIM, IOLIM, and FTEB.

Potential causes

The ICP Driver was unable to pass a message to the next layer. This is an unexpected overload of unknown cause but could include hardware corruption or traffic overload.

Consequence of inaction

Intermittent data access and control data.

Corrective actions

Investigate ControlNet, FTE, I/O and peer traffic loads. Swap roles to see if the problem moves with the chassis. Replace modules one at a time, ending with the chassis itself.

Time to respond

Next maintenance shift.

DIAG - ICP Unrecognized CMD

Applies to C200E, CPMC200, LIOM, FIM, IOLIM, and FTEB.

Potential causes

The ICP ASIC received a command from the backplane that it did not recognize. This indicates hardware corruption.

Consequence of inaction

Eventual system failure.

Corrective actions

Swap roles to see if the problem moves with the chassis. If non-redundant, power cycle the chassis (and reload if necessary). Replace modules one at a time, ending with the chassis itself.

Time to respond

Next maintenance shift.

DIAG - Illegal CLear DEVADDR Attempt On Link

Applies to H1 Link.

Potential causes

An attempt was made to clear the FIM's Device Address. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one Fieldbus Interface Module (FIM) or redundant FIM pair is on the same H1 link. Verify no other FF host device is on the H1 network. If the problem persists, reboot the secondary FIM.

Time to respond

Immediate.

DIAG - Illegal Clear PD_TAG Attempt On Link

Applies to H1 Link.

Potential causes

An attempt was made to clear the Fieldbus Interface Module (FIM)'s Physical Device Tag. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link. Verify no other FF host device is on the H1 network. If the problem persists, reboot the secondary FIM.

Time to respond

Immediate.

DIAG - Illegal Set DEVADDR Attempt On Link

Applies to H1 Link.

Potential causes

An attempt was made to set the Fieldbus Interface Module (FIM)'s Device Address. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link. Verify no other FF host device is on the H1 network. If the problem persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - Illegal Set PD_TAG Attempt On Link

Applies to H1 Link.

Potential causes

An attempt was made to set the Fieldbus Interface Module (FIM)'s Physical Device Tag. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link. Verify no other FF host device is on the H1 network. If the problem persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - Illegal Unknown SM Event On Link

Applies to H1 Link.

Potential causes

An unknown System Management indication was processed by the Fieldbus Interface Module (FIM).

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link. Verify no other FF host device is on the H1 network. If the problem persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - Input 1 Calibration Failure

Potential causes

Input 1 calibration data invalid.

Consequence of inaction

No PV.

Corrective actions

User calibration required.

Time to respond

DIAG - Input 2 Calibration Failure

Potential causes

Input 2 calibration data invalid.

Consequence of inaction

No PV.

Corrective actions

User calibration required.

Time to respond

DIAG - Input 3 Calibration Failure

Potential causes

Input 3 calibration data invalid.

Consequence of inaction

No PV.

Corrective actions

User calibration required.

Time to respond

DIAG - Input 1 Failure

Potential causes

Input 1 error.

Consequence of inaction

No PV.

Corrective actions

- Check input 1 connection and wiring.
- Check input contacts.
- Restart the sensor.

If the condition persists, replace the sensor module.

Time to respond

DIAG - Input 2 Failure

Potential causes

Input 2 error.

Consequence of inaction

No PV.

Corrective actions

- Check input 2 connection and wiring.
- Check input contacts.
- Restart the sensor.

If the condition persists, replace the sensor module.

Time to respond

DIAG - Input 3 Failure

Potential causes

Input 3 error.

Consequence of inaction

No PV.

Corrective actions

- Check input 3 connection and wiring.
- Check input contacts.
- Restart the sensor.

If the condition persists, replace the sensor module.

Time to respond

DIAG - Input 1 T/C Warning

Potential causes

Input 1 thermocouple faulty, resistance is excessive.

Consequence of inaction

No PV.

Corrective actions

Check input 1 connection and wiring. Replace the thermocouple.

Time to respond

DIAG - Input 2 T/C Warning

Potential causes

Input 2 thermocouple faulty, resistance is excessive.

Consequence of inaction

No PV.

Corrective actions

Check input 2connection and wiring. Replace the thermocouple.

Time to respond

DIAG - Input 3 T/C Warning

Potential causes

Input 3 thermocouple faulty, resistance is excessive.

Consequence of inaction

No PV.

Corrective actions

Check input 3 connection and wiring. Replace the thermocouple.

Time to respond

DIAG - Input Failure

Potential causes

Input error.

Consequence of inaction

No PV.

Corrective actions

May need to replace the meter body sensor.

Time to respond

DIAG - Intermittent Comm Failure

Potential causes

The NDM cannot communicate to one or more devices because either the specified device has been removed, or there is 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 hosting the NDM and the device(s).

Consequence of inaction

Loss of communication.

Corrective actions

Scan the Event journal for any recent Comm Failure and/or Card Removed system info events to determine which devices are not able to communicate with the NDM. Be aware that removal of a device (e.g. PCIC) required for communication with other “downstream” devices will result in the NDM reporting communication errors against the other “downstream” devices. Repair or 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).

Time to respond

Immediate.

DIAG - Invalid Keeper

Potential causes

A Keeper-capable ControlNet resident device (for example, CNI) does not indicate the Master Keeper status or Backup Keeper status. Either there is no Master Keeper on the affected ControlNet segment, or the specified device's programmed ControlNet parameters disagree with the ControlNet parameters being asserted by the Master Keeper.

Consequence of inaction

Loss of communication.

Corrective actions

Utilize the Network Tools application to reprogram the ControlNet parameters for the entire ControlNet segment or just the specified device.

Time to respond

Immediately.

DIAG - IOLink(1) Soft Fail Error

Applies to C300.

Potential causes

IOLINK 1 interface is in soft fail.

Consequence of inaction

The consequence depends on the actual soft fail reported on IO LINK configuration form. It could be any of the following:

- Duplicate IOL address
- IOL channel failure
- IOL max errors exceeded
- Not active supervisor
- IOLIM daughter card failure
- Partner not visible on IOL
- Partner mismatch on IOL
- IOL process data cycle overruns
- UM51 diagnostics exceeded time threshold
- UM51 diagnostic overrun

Corrective actions

View the Main tab of the configuration form for the IOLINK block for soft failures specific to the IO LINK interface and corresponding cause/solution.

Time to respond

Depends on actual alarm reported on IOLINK form.

DIAG - IOLink(2) Soft Fail Error

Applies to C300.

Potential causes

IOLINK 2 interface is in soft fail.

Consequence of inaction

The consequence depends on the actual soft fail reported on IO LINK configuration form. It could be any of the following:

- Duplicate IOL address
- IOL channel failure
- IOL max errors exceeded
- Not active supervisor
- IOLIM daughter card failure
- Partner not visible on IOL
- Partner mismatch on IOL
- IOL process data cycle overruns
- UM51 diagnostics exceeded time threshold
- UM51 diagnostic overrun

Corrective actions

View the Main tab of the configuration form for the IOLINK block for soft failures specific to the IO LINK interface and corresponding cause/solution.

Time to respond

Depends on actual alarm reported on IOLINK form.

DIAG - JagXtreme Communication Error

Potential causes

The associated JAGXTERM function block loses communication with the JX terminal.

Consequence of inaction

Communication failure alarms are generated for connected terminal I/O module blocks.

Corrective actions

Check the wiring and wiring terminations.

Time to respond

Immediate.

DIAG - JX Instrument Alarm

Potential causes

A alarm condition (usually a warning) occurred on the associated instrument.

Consequence of inaction

An alarm is a condition that, if left untreated, may stop the drive. Drive alarms are usually warnings.

Corrective actions

Check the instrument.

Time to respond

Immediate.

DIAG - JX Instrument Fault

Potential causes

A fault condition occurred on the associated instrument .

Consequence of inaction

Stops the drive operating.

Corrective actions

Check the instrument.

Time to respond

Immediate.

DIAG - KTC Failure

Potential causes

The presence of a KTC “tombstone” event implicitly indicates KTC card failure.

Consequence of inaction

Loss of communication.

Corrective actions

Restart the RSLinx service, which indirectly resets the KTC.

Time to respond

Immediate.

DIAG - Loss Of Batch Event

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

The Sequence Id of the event requested by server during event recovery is not available.

Consequence of inaction

The loss of string data, but the process will continue as is.

Corrective actions

Set the Batch Event Memory value to "Large". Make use of multiple Phase blocks to retrieve all string data needed.

Time to respond

As early as possible.

DIAG - Loss Of Batch Event Data

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

Occurs during generation of Formula or Report events of Datatype String more than 12 , 24 , 72, with the batch event memory configuration of “Small”, “Medium”, or “Large” respectively in a single execution cycle.

Consequence of inaction

The loss of string data, but the process will continue as is.

Corrective actions

Set the batch event memory to "Large". Make use of multiple Phase blocks to retrieve all string data needed.

Time to respond

As early as possible.

DIAG - Lost Sync

Potential causes

FIMs dropped synchronization for any reason.

Consequence of inaction

Loss of synchronization.

Corrective actions

Review the Redundancy History on the RM to determine cause of Loss of Sync.

Time to respond

Immediate.

DIAG - Low Battery

Potential causes

The device battery voltage is below 4.15V and critically low. The batteries should be replaced within 2-4 weeks.

Consequence of inaction

Device will go offline.

Corrective actions

Replace the batteries within 2–4 weeks.

Time to respond

DIAG - Low External Power

Potential causes

External power critically low.

Consequence of inaction

The device may go offline.

Corrective actions

Check the external 24V power supply.

Time to respond

DIAG - Low Power

Potential causes

External power critically low.

Consequence of inaction

Device may go offline.

Corrective actions

Check external 24V power supply.

Time to respond

DIAG - Local Hardware Fault

Potential causes

Short-circuit or wire-off condition.

Consequence of inaction

Break in field wiring or equipment damage.

Corrective actions

1. Check the power supply and connections.
2. Check the field wiring and replace if worn.

Time to respond

Immediate.

DIAG - Low Redundancy

Potential causes

Transmitter has connected with only one Multinode or FDAP.

Consequence of inaction

No redundant connection to the network.

Corrective actions

No action required. The Transmitter will periodically look for a second Multinode or FDAP in order to form a redundant connection to the network.

Time to respond

DIAG - Max Number Of Devices Exceeded

Applies to H1 Link.

Potential causes

More than 16 devices with non-visitor addresses are connected to the H1 link.

Consequence of inaction

Cannot commission new devices.

Corrective actions

Disconnect non-commissioned devices from the link

Time to respond

During device commissioning.

DIAG - MDM Service Is Running

Applies to CEEC300.

Potential causes

If the Machine Debug Manager (MDM) service is installed and running on a node which hosts on-process ACE, either in a cut-over scenario or inadvertently, the ACE process determines the state of the service both at startup and periodically, and prevents the CEE transition to RUN. An urgent priority system diagnostic alarm is generated.

Consequence of inaction

If the MDM service is running and the user accidentally attaches the debugger to the ACE process then the ACE application will crash.

Corrective actions

If you try to give the CEECOMMAND as 'RUN' when MDM service is running an error message is thrown indicating "CEE can't be activated when the MDM service is running". In this case stop the MDM service and retry the CEECOMMAND 'RUN'. If this alarm is raised when the ACE controller is in a “Run” state, stop the MDM service in the ACE Machine. This will return the alarm to normal

Time to respond

As soon as possible.

DIAG - Memory Limit Exceeded

Applies to C200E, CPMC200, LIOM, SIMC200E, CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

This alarm is generated by the CPM block when the user memory (control strategy) has been exhausted.

Consequence of inaction

Migration is not possible.

Corrective actions

Either disable this error flag, or delete sufficient control strategy from the user pool to make and FREEMEM parameter value a positive number.

Time to respond

As soon as possible.

DIAG - Missing Keeper

Potential causes

A ControlNet segment does not have a Master Keeper. 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.

Consequence of inaction

Loss of Communication.

Corrective actions

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.

Time to respond

Immediate.

DIAG - Module Hardware Fault

Potential causes

Critical module hardware failure detection due to following causes:

1. A detected fault in the I/O device hardware.
2. Opened or shorted leads to the sensor.
3. A faulted remote transmitter.

Consequence of inaction

All channels are marked as bad. PV reports NAN and disrupts process.

Corrective actions

1. Check the leads to the sensor.
2. Replace the device.

Time to respond

Immediate.

DIAG - No Field Power Detected

Potential causes

Loss of field power for a particular channel. Current flow is not present at any channel.

Consequence of inaction

Lack of power resulting in output state change.

Corrective actions

Check the power supply to each channel and associated connections.

Time to respond

Immediate.

DIAG - No Load Detected

Potential causes

The output current draw falls below the threshold or a hardware output failure occurs. Detection only works when the output is in the OFF state.

Consequence of inaction

No load is detected on this channel.

Corrective actions

Check the I/O device and replace hardware, if required.

Time to respond

Immediate.

DIAG - No PBIM Reference

Potential causes

Invalid or missing PBIM reference.

Consequence of inaction

PBIM serves the devices I/O data to each of its associated blocks. Invalid reference indicates loss of I/O data and fails to detect the device location.

Corrective actions

Reconfigure the PBIM block reference and reload.

Time to respond

Immediate

DIAG - No Sensor Board Alert

Potential causes

The Transducer Interface Instrument - X-Band Radar board is disconnected from SmartRadar FlexLine system.

Consequence of inaction

Level detection not possible.

Corrective actions

Check the TII-XR board connections.

Time to respond

DIAG - Non–Volatile Memory Error

Potential causes

Startup diagnostics have detected a defect in the Non-Volatile memory sensor.

Consequence of inaction

The device will go offline.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - Not Using Configured Time Source

Applies to FIM4, FIM8, C300 and PGM.

Potential causes

If the CDA is unavailable or subsequently becomes unavailable, the C300 Controller will continue to run and execute control. In this case, it will use its internal Wall Clock Time (WCT) source (based on a precision oscillator).

Consequence of inaction

The system will continue to use it internal wall clock and will also generate Time Source Changed alarm.

Corrective actions

Verify whether the CDA service is running.

Time to respond

DIAG - Over Range Fault

Potential causes

Indicates the input value is above the valid hardware input range of the channel (e.g. Temp>Tmax).

Consequence of inaction

Disrupts the process. Loss of control.

Corrective actions

Check the input device/transmitter.

Time to respond

Immediate.

DIAG - Over Temperature Alert

Potential causes

The meter body has exceeded the maximum temperature as defined by the meter body characterization data.

Consequence of inaction

Incorrect PV.

Corrective actions

Determine and rectify the cause of the excessive temperature.

Time to respond

DIAG - PCIC Lonely On CNet

Applies to ACE.

Potential causes

1. Cables not connected correctly.
2. Cables not terminated correctly.
3. MAC ID assigned to the PCIC card is incorrect.

Consequence of inaction

When a controller node becomes lonely, it will lose its configuration file and cause errors when it regains access to other nodes.

Corrective actions

1. Check if cables are connected properly on the A & B or just the A ControlNet Supervisory segments. Also check if the terminators of the correct value are installed on both ends of the segment.
2. Check supervisory CNI for A and B network LEDs.
3. Check the MAC ID and assign it correctly.

Time to respond

As soon as possible.

DIAG - Partner Not Visible on FTE

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The Fault Tolerant Ethernet (FTE) communications with redundant controller partner and FTE network are lost due to one of the following reasons:

1. Secondary controller is defective.
2. Secondary IOTA is defective.
3. Primary controller is defective.
4. Primary IOTA is defective.

Consequence of inaction

System redundancy can't be achieved.

Corrective actions

1. Replace the Secondary controller that initiated switchover when fault was detected.
2. Replace the Secondary IOTA that initiated switchover when fault was detected.
3. Replace the Primary controller.
4. Replace the primary IOTA.

Time to respond

As soon as possible.

DIAG - PBIM Communication Error

Potential causes

PBIM communication errors, probably between the PBIM block and the SST-PB3-CLX-HWL (PROFIBUS interface module).

Consequence of inaction

Data loss.

Corrective actions

Investigate the PBIM block's communication status.

Time to respond

Immediate.

DIAG - PBIM Inactive

Potential causes

PBIM block is INACTIVE.

Consequence of inaction

Causes a break in the communication between I/O device/module blocks and the PROFIBUS network. I/O data is not transferred between the PBIM block and the SST-PB3-CLX-HWL (PROFIBUS interface module) card. Fail-Safe data is returned to client input blocks.

Corrective actions

Set the block execution status of the PBIM block to Active. Any adding, removing or reconfiguring one or more slave devices initializes the block status to INACTIVE.

Time to respond

As needed.

DIAG - PBIM Registration Error

Potential causes

Generated if the block is not registered with PBIM block.

Consequence of inaction

Configuration mismatch between this block and the PBIM block with regard to the Station number, Module Number, and Data Offsets that correspond to the data expected by the block.

Corrective actions

Ensure a matching configuration between PBIM table and IOM block, including Station number, Module Number, and Data Offsets that correspond to the data expected by the block.

Time to respond

Immediate.

DIAG - PCIC Failure

Potential causes

The presence of a PCIC “tombstone” event implicitly indicates PCIC card failure.

Consequence of inaction

Loss of communication.

Corrective actions

Restart the RSLinx, which indirectly resets the PCIC.

Time to respond

Immediate.

DIAG - Pressure Overload Alert

Potential causes

The applied pressure has exceeded the limit defined by the meter body characterization data.

Consequence of inaction

Incorrect PV.

Corrective actions

Determine and rectify the cause of the excessive pressure.

Time to respond

DIAG - PROFIBUS Communication Error

Potential causes

The controller to SST-PB3-CLX-HWL communication connection is broken. Causes may be:

1. Power is disrupted to the remote chassis in which the SST-PB3-CLX-HWL resides.
2. The SST-PB3-CLX-HWL is removed under power.
3. The controller to SST-PB3-CLX-HW.

Consequence of inaction

Controller to PROFIBUS interface module communication connection is broken. Results in data loss.

Corrective actions

1. Check the I/O module to make sure it is not faulted or unpowered.
2. Check the chassis PS, in which the PBIM resides and restore, if unpowered.
3. In case of a remote chassis, check the cable connections.

Time to respond

Immediately.

DIAG - PROFIBUS Not In Run

Potential causes

PROFIBUS Run mode is not enabled (on PBIM block).

Consequence of inaction

Disables the communication of output values from the CEE.

Corrective actions

Enable the Profibus Run Mode.

Time to respond

As needed.

DIAG - PROFIBUS Offline

Potential causes

PBIM block is not online with PROFIBUS.

Consequence of inaction

Changes in the PROFIBUS network will not update in the PBIM block.

Corrective actions

Restore the PBIM block status to ONLINE.

Time to respond

As needed.

DIAG - Program Memory Fault

Potential causes

Startup diagnostics detected a defect in the program memory sensor.

Consequence of inaction

Device will go offline.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - PTP Time Source Failed

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

If a PTP/NTP time source is configured and if it becomes unavailable the controller uses its internal wall clock time (WCT), and reports this alarm.

Consequence of inaction

The system will continue to use the CDA time source.

Corrective actions

Check that the PTP time server is running.

Time to respond

Not critical.

DIAG - QiMPACT Communication Error

Potential causes

Communication error within QiMPACT cluster. The IOM Function Block loses communication with its associated QiMPACT terminal.

Consequence of inaction

Communication Failure alarms are generated for connected terminal I/O module blocks.

Corrective actions

Restore the connection to the connected terminal.

Time to respond

Immediate.

DIAG - QiMPACT Instrument Alarm

Potential causes

A alarm condition (usually a warning) occurred on the associated instrument.

Consequence of inaction

An alarm is a condition that, if left untreated, may stop the drive. Drive alarms are usually warnings.

Corrective actions

Check the instrument.

Time to respond

Immediate.

DIAG - QiMPACT Instrument Fault

Potential causes

A fault condition occurred on the associated instrument.

Consequence of inaction

Stops the drive operating.

Corrective actions

Check the instrument.

Time to respond

Immediate.

DIAG - Radio Interprocessor Comm Error

Potential causes

The radio board is not accessible.

Consequence of inaction

Loss of communication to the device.

Corrective actions

Restart both the radio and sensor. If condition persists, replace the sensor module.

Time to respond

DIAG - Radio Status EEPROM SP1 Communication Failure

Potential causes

There has been a radio EEPROM SPI communication failure.

Consequence of inaction

The radio will not be able to perform firmware upgrades but will operate normally using installed code.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - Radio Status Radio Communication Circuitry Failure

Potential causes

The radio processor detected error on internal radio circuitry.

Consequence of inaction

No data acquisition from the field device.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - Radio Status Sensor Radio SP1 Communication Failure

Potential causes

The radio detected a loss of communication with the sensor board over the inter-processor communication link.

Consequence of inaction

No PV.

Corrective actions

Restart both the radio and sensor. If the condition persists, replace the sensor module.

Time to respond

DIAG - Radio Status WDT Reset Occurred

Potential causes

The radio detected a Watch Dog Timer (WDT) timeout.

Consequence of inaction

Device reset.

Corrective actions

Restart both the radio and sensor. If the condition persists, replace the sensor module.

Time to respond

DIAG - RAM Error

Potential causes

Startup diagnostics detected a defect in the sensor RAM.

Consequence of inaction

Device will go offline.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - RAM Fault

Potential causes

Startup diagnostics detected a defect in the processor RAM.

Consequence of inaction

Device will go offline.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - Reconfiguration Fail

Potential causes

IOM reconfiguration status is FAILED.

Consequence of inaction

The reconfiguration terminates in failure.

Corrective actions

1. Check the device status.
2. Restart the device and configure it again.

Time to respond

Immediate.

DIAG - Redun Standby

Applies to C200E, CPMC200, LIOM, and C300.

Potential causes

Both the primary and secondary controllers generate this notification when entering the Standby sync state due to On Process Migration; this is only generated by the C300 controller.

Consequence of inaction

Expected.

Corrective actions

Continue with migration.

Time to respond

N/A

DIAG - Redun Count Exceeded

Applies to CEEACEFB, CEEC200EFB, CEEC300, CEEFB, CEESIMC200FB, and EEFB.

Potential causes

The Redundancy Count Exceeded alarm fires whenever the maximum number of redundancy tracking bytes generated in any CEE-C300 cycle exceeds the value of parameter RDNCNTCYCTP. The maximum is accumulated once every 2 seconds. The alarm clears when the observed maximum for all cycles falls to a value that is more than 10% below the configured trip point.

Consequence of inaction

Possible loss of synchronization.

Corrective actions

Use RTC instrumentation parameters to determine whether the maximum load is spread across all cycles or concentrated on a few cycles. Reset statistics while examining the instrumentation to determine if regular, steady state load produces maxima close to the limit or if, instead, a burst condition tripped the alarm.

Reduce the total configuration being run in the CEE-C300 by deleting CMs. CMs with CAB types would be specifically considered for deletion. Focus on those cycles in which heavy load appears to be concentrated.

Examine, and if needed, modify CAB types deployed within the CEE-C300. CAB types with intensive looping would be specifically considered for modification or for elimination from the configuration.

Increase the trip point of the RTC alarm if absolutely necessary, and if it is safe to do so. This might be done as a stop-gap measure to eliminate Operators having to deal with the alarm noise while an engineering solution is being worked out. It is recommended that if the RTC trip point is increased, it should be done only on a temporary basis. The trip point should be decreased back to the default value after an engineering solution is implemented. If a decision not to reduce the CEE-C300 configuration after an RTC alarm fires is made, and the increased trip point value permanently retained, then the C300 configuration should be considered sealed and complete from that point on, at least for cycles which produce RTC near the trip point. Additional RTC load should not be added to the sensitive cycles.

Time to respond

As soon as possible.

DIAG - Remote Hardware Fault

Potential causes

Remote transmitter is faulted.

Consequence of inaction

Process disruption.

Corrective actions

Replace the transmitter.

Time to respond

Immediate.

DIAG - ROM Application Image Checksum Failure

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The C300 Controller Application Image resides in Flash ROM. This alarm is raised when the C300 Controller run-time diagnostic based on checksum to verify the image fails.

Consequence of inaction

The controller might not boot up in application mode subsequent reboots.

Corrective actions

Try reloading the application image firmware. If this condition persists, contact the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

Immediate.

DIAG - ROM Boot Image Checksum Failure

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The C300 Controller boot Image resides in Flash ROM. This alarm is raised when the C300 Controller run-time diagnostic based on checksum to verify the image fails.

Consequence of inaction

The controller might not boot up in the subsequent reboots.

Corrective actions

Try reloading the boot and application image firmware. If this condition persists, contact the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

As soon as possible.

DIAG - ROM Error

Potential causes

Startup diagnostics detected a defect in the sensor ROM.

Consequence of inaction

Device will go offline.

Corrective actions

Replace the sensor module.

Time to respond

DIAG - RSLinx Failure

Potential causes

The RSLinx service has stopped for an unknown reason.

Consequence of inaction

Loss of communication.

Corrective actions

Restart the RSLinx service.

Time to respond

Immediate.

DIAG - RSLinx Initialization Failure

Potential causes

The NDM is unable to initialize a RSLinx session. Either {1} incompatible version of RSLinx software or {2} RSLinx not running.

Consequence of inaction

Loss of communication.

Corrective actions

Either verify that the appropriate version of RSLinx software is installed for the specific software release in use or restart the RSLinx service.

Time to respond

Immediate.

DIAG - RTP Disconnect

Potential causes

Disconnected RTP cable.

Consequence of inaction

Loss of synchronization. Potential loss of process data/ loss of control.

Corrective actions

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.

Time to respond

Immediate.

DIAG - Runtime Diagnostic Failure

Applies to H1 Link.

Potential causes

Occurs on Fieldbus Interface Module (FIM) 2 only. Indicates that the co-processor has detected a diagnostic failure.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Contact your Honeywell Technical Assistance Center to diagnose, verify installation and replace the FIM.

Time to respond

Immediate.

DIAG - Runtime Diagnostic OVERRUN

Applies to H1 Link.

Potential causes

Occurs on the Fieldbus Interface Module (FIM) 2 only. Indicates that the diagnostic cycle on the co-processor did not complete in the allotted time.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

Contact your Honeywell Technical Assistance Center to diagnose, verify installation and replace the FIM.

Time to respond

Immediate.

DIAG - Runtime Fail on Daughter Board

Potential causes

Run time diagnostic failure of the daughter board.

Consequence of inaction

Loss of synchronization. Potential loss of process data and/or loss of control.

Corrective actions

1. 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.
2. Restart the module.
3. If the problem persists, replace FIM hardware.

Time to respond

Immediate.

DIAG - Secondary Address Overlap

Applies to LIOM SLINK.

Potential causes

An overlap is detected when the starting address of the SIOM plus the slot configuration overlaps with the starting address of the next SIOM. The two SIOMs under consideration can be on one or different links. In such a scenario, only one of the SIOMs comes online and the other SIOM reports an overlap condition on its link.

Consequence of inaction

Only one of the overlapped SIOMs will work; others will not.

Corrective actions

Assign unique addresses for all SIOMs.

Time to respond

As soon as possible.

DIAG - Sensor Alert

Potential causes

Input failure, which can happen for several reasons:

- Wired sensor is not connected to the field device.
- Input range exceeded the limits.
- There is a wire disconnection.

Consequence of inaction

No PV.

Corrective actions

- Check the connection between the wired sensor and field device.
- Check the input signal range.

Time to respond

DIAG - Short Circuit Detected

Potential causes

Short circuit or overload condition.

Consequence of inaction

1. Equipment damage.
2. Damages the device due to excess current drawn for a given channel.

Corrective actions

Check the power supply and associated connections.

Time to respond

Immediate.

DIAG - SIOM Offline

Potential causes

SIOM was taken offline.

Consequence of inaction

Corrective actions

Command "Restart Slinks" from LIOM FB configuration form.

Time to respond

DIAG - SIOM Offline, Communications Ceased

Applies to LIOM SLINK.

Potential causes

When a SIOM goes offline on a serial link, communication on the corresponding serial link, or both serial links, ceases depending on the serial link fault configuration.

Consequence of inaction

All the SIOM on that particular link will not be under control of LIOM.

Corrective actions

Fix the connections or power to the affected SIOM.

Time to respond

Immediately.

DIAG - SIOM Offline, Secondary Communications Ceased

Applies to LIOM SLINK.

Potential causes

When a SIOM goes offline on a serial link, communication on the corresponding serial link, or both serial links, ceases depending on the serial link fault configuration.

Consequence of inaction

All the SIOM on that particular link will not be under control of LIOM.

Corrective actions

Fix the connections or power to the affected SIOM.

Time to respond

Immediately.

DIAG - SM Dupe Node Address

Potential causes

A second node is on the H1 Link at the same address as the FIM. Typically two FIMs are connected to the same H1 network.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.
2. Verify no other FF host device is on the H1 network.
3. If persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - SM Node Address Clear

Potential causes

An attempt was made to clear the FIM's Device Address. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.
2. Verify no other FF host device is on the H1 network.
3. If persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - SM Node Address Set

Potential causes

An attempt was made to set the FIM's Device Address. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.
2. Verify no other FF host device is on the H1 network.
3. If persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - SM Physical Device Tag Clear

Potential causes

An attempt was made to clear the FIM's Physical Device Tag. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.
2. Verify no other FF host device is on the H1 network.
3. If persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - SM Physical Device Tag Set

Potential causes

An attempt was made to set the FIM's Physical Device Tag. There should be no device or system on the H1 link capable of this action.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Verify wiring to ensure only one FIM or redundant FIM pair is on the same H1 link.
2. Verify no other FF host device is on the H1 network.
3. If persists, reboot secondary FIM.

Time to respond

Immediate.

DIAG - SM Unknown

Potential causes

Unrecoverable or unexpected condition detected in System Management.

Consequence of inaction

Unpredictable results including loss of control and loss of view.

Corrective actions

1. Check segment health for network errors, noise, or nonconforming devices.
2. Replace the FIM if problems persist.

Time to respond

Immediate.

DIAG - SNTP Failed

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

If the connection to the configured SNTP time source is broken during normal startup operation, the C300 Controller will continue to run. The loss of connection is detected when no messages from the configured system time source are received over a 90 second interval. If the C300 Controller remains connected to the FTE network and if CDA is available and functioning, the C300 Controller will transition to the use of CDA Time, causing these alarms to be raised.

Consequence of inaction

The system will continue to use CDA time source and will also generate "Time Source Changed" and " Not using configured time source" alarms.

Corrective actions

Check that the SNTP time server is running.

Time to respond

Not critical.

DIAG - Stack Limit Exceeded

Applies to C200E, CPM, CPM200, LIOM, C300, and FIM4.

Potential causes

One or more tasks have exceeded their defined stack limit.

Consequence of inaction

The controller may crash.

Corrective actions

Contact your Honeywell Technical Assistance Center for help with diagnosis.

Time to respond

Immediate.

DIAG - Stale Output Alert

Potential causes

The number of consecutively missed publishes exceeds the stale count limit.

Consequence of inaction

Incorrect output value.

Corrective actions

- Determine the cause of the missed publishes; or
- Check the stale count limit.

Time to respond

DIAG - Sync Checksum Fail

Applies to C200E, CPM, CPM200, LIOM, C300, FIM4, and FIM8.

Potential causes

1. Invalid writes to secondary tracked memory are essentially the same as CRC errors, since invalid writes lead to CRC errors.
2. CRC of the data copied to the Tracked memory of secondary during synchronization is validated, if it fails this alarm is raised.

Consequence of inaction

Loss of redundancy.

Corrective actions

Restart the CPM. If problem persists, replace the CPM.

Time to respond

Immediate.

DIAG - Sync HW Failure

Applies to C200E, CPM, CPM200, LIOM, C300, FIM4, and FIM8.

Potential causes

Synchronization hardware (i.e., Tracker mechanism) failure.

Consequence of inaction

Loss of redundancy.

Corrective actions

- If the CPM is being used in a non-redundant configuration, replace the CPM at the user's earliest convenience.
- If the CPM is currently in the primary redundancy role, attempt switchover to better primary.
- If the CPM is currently in the secondary redundancy role, first restart the CPM. If problem persists, replace the CPM.

Time to respond

Immediate.

DIAG - Task Health Monitoring Warning

Applies to FIM4, FIM8, and C300.

Potential causes

The task being monitored doesn't execute in the monitoring time window.

Consequence of inaction

The controller may fault and take itself offline.

Corrective actions

Make sure that the CPUFREE, Redundancy load, and IOLINK bandwidth usage are within Honeywell recommended limits.

Time to respond

Not critical.

DIAG - Time Jump Greater Than Five Minutes

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

If none of the configured time sources are available controller uses its internal WCT source. As soon as it finds a more precise time source, it will switch to that source and if the time difference greater than 5 minutes, this alarm is generated.

Consequence of inaction

CAB blocks that makes decision based on DELTATIME, TIME and TOD parameters will be impacted.

Corrective actions

Validate whether the time jump is justified.

Time to respond

Not critical.

DIAG - UMAX Exceeded

Potential causes

A ControlNet segment has at least one node that is attempting to send unscheduled traffic and is at a MAC address higher than expected as specified by the UMAX ControlNet network parameter. Either there is no Master Keeper on the affected ControlNet segment, or the ControlNet parameters being asserted by the Master Keeper are not valid.

Consequence of inaction

Loss of communication.

Corrective actions

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).

Time to respond

Immediate.

DIAG - Uncommanded Shutdown

Potential causes

The PCM child process did not set its own exit event and therefore did not exit cleanly.

Consequence of inaction

Loss of communication.

Corrective actions

Time to respond

Immediate.

DIAG - Uncomm Dev Oper Class Changed To Basic

Applies to H1 Link.

Potential causes

Safe device handling has set the Boot Operational Functional Class of the device to BASIC.

Consequence of inaction

None.

Corrective actions

No action required. If configured, the uncommissioned device will be changed to link master when loaded.

Time to respond

During device commissioning.

DIAG - Under Range Fault

Potential causes

Input value is under the valid hardware input range of the channel (e.g. Temp < Tmin).

Consequence of inaction

Disrupts the process. Loss of control.

Corrective actions

Check the input device/transmitter.

Time to respond

Immediate.

DIAG - Unexpected Partner on Redundancy Link

Applies to FIM4, FIM8, and C300.

Potential causes

Only the controller explicitly configured as non-redundant generates this notification if a partner is present on the Redundancy private path. The RDNSYNCSTATE parameter is set to either PARTNERVISBL or INCOMPATIBLE. This notification returns to normal if the controller is subsequently configured as redundant or if the partner is removed from the redundancy link.

Consequence of inaction

No impact.

Corrective actions

This notification returns to normal if the controller is subsequently configured as redundant or if the partner is removed from the redundancy link.

Time to respond

As soon as possible.

DIAG - Verify Lost

Potential causes

Actual state of the output does not match the commanded state.

Consequence of inaction

Loss of control. The commanded-output state is changed and the actual input PVstate does not change accordingly

Corrective actions

Check the field device.

Time to respond

Immediate.

DIAG - Watchdog Timer Error

Potential causes

Sensor Watchdog Timeout. The processor was restarted due to unexpected operation.

Consequence of inaction

Device will be reset.

Corrective actions

Clear by warm restart of device. If condition persists contact Honeywell Technical Assistance Center for support.

Time to respond

DIAG - WDT Refresh Warning

Applies to FIM4, FIM8, C300, and PGM.

Potential causes

The watchdog timer is being refreshed at a rate that is outside acceptable limits. Or the watchdog timer is being refreshed late, but not late enough for it to expire.

Consequence of inaction

Task health monitoring will be disturbed.

Corrective actions

The system CPU usage needs to be reduced if the statistics show very high CPU usage or CPU Overruns. If the CPU usage is reasonable then contact the Honeywell Technical Assistance Center (TAC) for support.

Time to respond

As soon as possible.

DIAG - Wire off Detected

Potential causes

Absence of a field wire (sensor/actuator) or the break in field wiring.

Consequence of inaction

1. Break in field wiring.
2. Loss of data from field and hence control.

Corrective actions

Check the field wiring and replace field wire if worn.

Time to respond

Immediate.

Duplicate Point system alarms

The following topics describe duplicate point-related system alarms and how to respond to them.

Related topics

“Duplicate Point - message/alarm/alert from con <server name> is on a point which is a duplicate of an existing point from con <server name>” on page 270

Duplicate Point - message/alarm/alert from con <server name> is on a point which is a duplicate of an existing point from con <server name>

Potential causes

The local server has notified that two points on different DSA servers have the same item name. The local server has received a point alarm from a DSA server. However, a point of the same name (that references another DSA server), already exists in the system.

Consequence of inaction

Notifications from the duplicate point on the DSA server will not be processed and displayed on this DSA subscriber. Notifications on the existing point will be shown as expected on this DSA subscriber.

Corrective actions

1. Change the ‘item name’ of one of the duplicate points. For more information, see the “Requirements for implementing a DSA system” topic.
2. For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation. For more information, see the “Creating a diagnostic package for TAC” topic.

Time to respond

The corrective action should be initiated immediately to allow alarms from the duplicate point to be seen on this DSA subscriber, especially if operators on this DSA subscriber are responsible for monitoring and control of this point.

EVTARC system alarms

The following topics describe event archiving-related system alarms and how to respond to them.

Related topics

“EVTARC - Event Archive Initialization Failed” on page 272
“EVTARC - Invalid archive directory” on page 273

EVTARC - Event Archive Initialization Failed

Potential causes

The event archiving task has failed to start.

Consequence of inaction

Cannot create an event archive.

Corrective actions

- Call up the **Event Archiving Operations** display.
- For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Immediate.

EVTARC - Invalid archive directory

Potential causes

The event archiving task cannot write to the folder because:

- The specified folder does not exist; or
- Experion does not have permission to write to the specified folder

Consequence of inaction

Cannot create an event archive.

Corrective actions

- Call up the **Event Archiving Configuration** display. Ensure that a valid folder is specified in **Create archive in directory**.
- Allow the MNGR account to write to the specified folder.

Time to respond

Immediate.

HSTARC system alarms

The following topics describe history archiving-related system alarms and how to respond to them.

Related topics

“HSTARC - Disk Full Error” on page 276
“HSTARC - Invalid Pathname For Move” on page 277
“HSTARC - Permission Error” on page 278

HSTARC - Disk Full Error

Potential causes

The drive where history archives are to be moved to does not have enough free space or an error when copying the history archives to the Location to Move.

Consequence of inaction

History archive files not moved. The result is that the drive on which the Experion history archives are stored may become full.

Corrective actions

1. Call up the **History Archiving** display.
2. Check that the History Archiving Disk Limit is configured appropriately.
3. Check that the “Location to Move History Archive to” exists and has enough free space.

For more information, see “Configuring history archives”.

Time to respond

As soon as possible before next history archive management run time (default 7:43AM every day), in case disk runs out of space.

HSTARC - Invalid Pathname For Move

Potential causes

The history archive folder could not be created.

Consequence of inaction

History archive files have not been moved. The drive on which the history archives are stored may fill up (reducing free space).

Corrective actions

1. Call up the **History Archiving** display.
2. Check that the “Location to Move History Archive to” is a valid location.

Time to respond

As soon as possible before next history archive management run time (default 7:43AM every day), in case disk runs out of space.

HSTARC - Permission Error

Potential causes

The history archive folder could not be created.

Consequence of inaction

History archive files have not been moved. The drive on which the history archives are stored may fill up (reducing free space).

Corrective actions

1. Call up the **History Archiving** display.
2. Check that the “Location to Move History Archive to” exists and has enough free space.
3. Check that the MNGR user has permission to create files and directories and write to the “Location to Move History Archive to” folder.

Time to respond

As soon as possible before next history archive management run time (default 7:43AM every day), in case disk runs out of space.

LNK nn system alarms

The following topics describe link-related system alarms and how to respond to them.

Related topics

“LNK nn - Cntrl Stream Upgraded” on page 280
“LNK nn - Peer Server Host Name Cannot Be Resolved” on page 281

LNK nn - Cntrl Stream Upgraded

Potential causes

Server Redundancy network link control stream has been upgraded to a data stream due to change in link availability.

Consequence of inaction

Servers will remain out of synchronization, so the backup server database will not be updated with the changes on the primary (including point configuration, history, events, etc.) and some automatic failover actions will not be triggered.

Corrective actions

Resynchronize the backup and primary servers. For more information, see “.”

Time to respond

The time to respond will depend on availability of other Link (if configured) and an assessment of process/site/operations for criticality/risk of losing synchronization between Servers.

LNK nn - Peer Server Host Name Cannot Be Resolved

Potential causes

Hosts File is not configured correctly on Servers. Host naming rules have not been followed for redundant servers.

Consequence of inaction

Link will become unavailable for redundancy. If only one link configured, or both links unavailable, then it shall not be possible to synchronize the servers.

Corrective actions

1. Acknowledge the alarm.
2. Investigate why the backup server is not operational. Start the backup server and make sure that it is connected to the network.
3. Correct the hosts file on both servers.
4. Verify communications between the Servers using 'ping' command or accessing network shares.
5. Verify that link has been restored on Redundancy Status display, and then resynchronize the backup and primary servers. For more information, see “.”

Time to respond

The time to respond will depend on availability of other Link (if configured) and an assessment of process/site/operations for criticality/risk of losing synchronization between Servers.

No condition system alarms

The following topics describe No condition system alarms and how to respond to them.

Related topics

“Asset Electronic Signature” on page 284
“CStnxx: Server Is Not Available” on page 285
“Disk Space Low: Deleting Old Archives” on page 286
“Disk Space Low: Suspending Event Collection” on page 287
“Event Archiving Reset Failed” on page 288
“Event File Error” on page 289
“Failed logon attempt” on page 290

Asset Electronic Signature

Potential causes

The Electronic Signatures for an asset has been enabled or disabled.

Consequence of inaction

Is an information alarm.

Corrective actions

To enable or disable Electronic Signatures for an asset click the link on the **Electronic Signatures General** display.

Time to respond

There is no recommended response time. However, the amount of time taken to respond varies on whether any corrective action is taken and the type of corrective action.

CStnxx: Server Is Not Available

Potential causes

The numbered Console station has notified that it has lost contact with the server.

Consequence of inaction

At minimum, this alarm signifies the loss of view to non-direct data on the Console Station. At worst, this alarm signifies complete loss of view on the Console Station.

Corrective actions

Check that the Console Station is powered up and connected to the Experion server.

Check the status of the Console Station on the **Console Station Status Detail** display. You can view a detailed status by clicking the down arrow next to **Show details**, and check that all components are OK.

In the case of a network failure, check that the network connection between the server and the Console Station is operational.

Time to respond

Immediate.

Disk Space Low: Deleting Old Archives

Potential causes

The server event manager has notified that the server event buffer is full.

Consequence of inaction

New events could be lost.

Corrective actions

Move old event archives to another disk and delete them from the original disk, or increase the disk size.

1 Choose **View** > **Events** > **Event Archiving**.

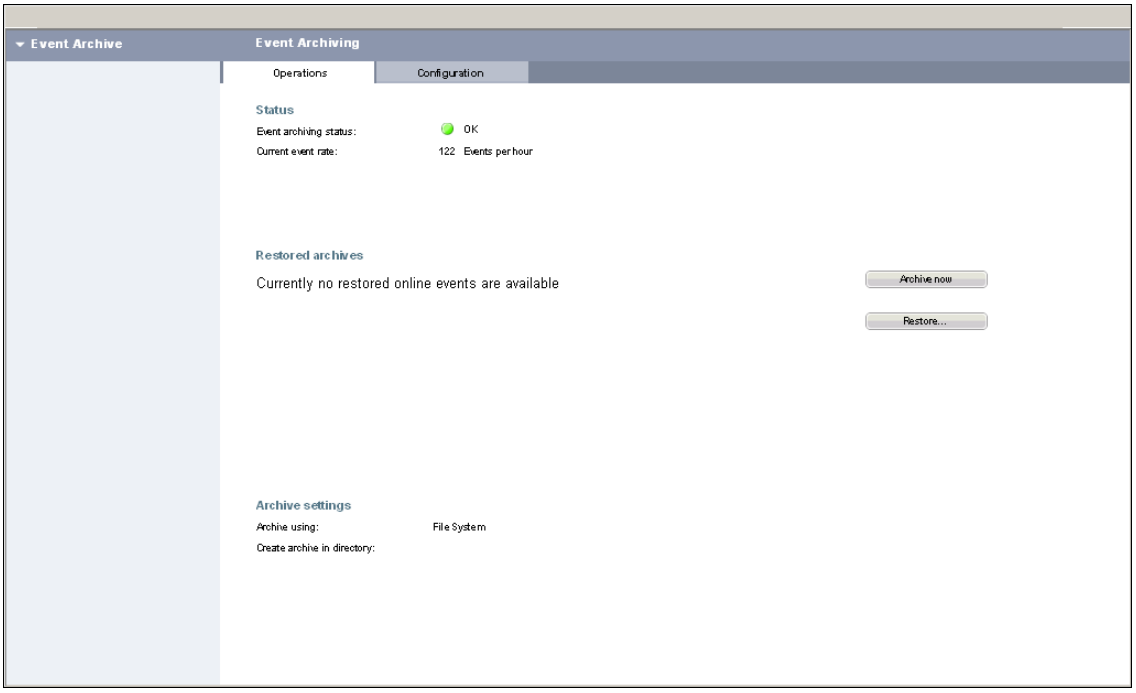

Figure 1: Event Archiving Status Display

2 You can now:

- **a** Archive the events by clicking the **Archive Now** button.
- **b** Check for tampering of event records.
- **c** Restore archived events by clicking the **Restore** button.
- **d** Remove restored archives by clicking the **Remove** button. The **Remove** button appears when you have restored archives.
- **e** View the status of events collection and archiving.

Time to respond

Within 24 hours.

Disk Space Low: Suspending Event Collection

Potential causes

The server event manager is unable to determine free disk space, or disk space is less than configured limit.

Consequence of inaction

New events could be lost.

Corrective actions

1. Call up the **Event Archiving Operations** display.
2. Check disk integrity, archive old events, or increase event disk limit.

Time to respond

Immediate.

Event Archiving Reset Failed

Potential causes

The event archiving reset stored procedure failed to run. Can be caused by various factors.

Consequence of inaction

New events could be lost.

Corrective actions

- Call up the **Event Archiving Operations** display.
- For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Immediate.

Event File Error

Potential causes

The server event manager failed to journal an event to the SQL database.

Consequence of inaction

New events could be lost.

Corrective actions

- Call up the **Event Archiving Operations** display.
- For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Approximately 2 hours.

Failed logon attempt

Potential causes

The logon failed, which could be due to one of the following causes:

1. Operator or Group not configured in Experion.
2. Operator or Group disabled in Experion.
3. Operator disabled in Windows.
4. Incorrect password.
5. Windows domain controller(s) is offline.
6. Experion Operator Management Service not running under an appropriate account.

Consequence of inaction

Is an informational alarm.

If this alarm is received frequently, it could indicate attempted unauthorized use of the system and should be investigated.

Corrective actions

1. Configure the Operator/Group in Experion.
2. Enable the Operator/Group in Experion.
3. Enable the Operator in Windows.
4. Use the correct password.
5. Bring the Windows domain controller(s) online.
6. Run the:
   - Operator Management Service with an account that has appropriate permissions.
   - Operator Management Service on all nodes.

Time to respond

There is no recommended response time. However, the amount of time taken to respond varies on whether any corrective action is taken and the type of corrective action.

NULL system alarms

The following topics describe NULL-related system alarms and how to respond to them.

Related topics

“NULL - Console Fail” on page 292
“NULL - Console Marginal” on page 293
“NULL - Console Station Is Not Available” on page 294

NULL - Console Fail

Potential causes

The server has lost communication with every Console Station and Console Station Extension in a Console.

Note that this alarm can be configured. See “Configuring system alarm priorities”.

Consequence of inaction

This alarm signifies that view has been lost on every Station in the Console.

Corrective actions

Check that the Console is powered up and connected to the Experion Server.

Check that Station is running on each Console Station and each Console Extension Station in the cluster, and that each of these Station instances is connected.

For more information, see “Lost contact with a Console Station”.

Time to respond

Immediately.

NULL - Console Marginal

Potential causes

The server has lost communication with one or more Console Stations or Console Station Extensions in a Console.

Note that this alarm can be configured. For more information, see “Configuring system alarm priorities”.

Consequence of inaction

This alarm signifies that view has been lost on at least one Station, but that view is maintained on at least one other Station. If view is subsequently lost on other Stations, it might be the case that other Stations in the cluster have also lost view, and the Console Fail alarm will be raised.

Corrective actions

Check that the Console or Console Station Extension is powered up and connected to the Experion Server.

Check that Station is running on each Console Station and each Console Extension Station in the cluster, and that each of these Station instances is connected.

For more information, see “Lost contact with a Console Station”.

Time to respond

It depends on whether a failure happens on another Station in the cluster.

NULL - Console Station Is Not Available

Potential causes

The server has lost communication with a Console Station.

Note that this alarm can be configured. For more information, see “Configuring system alarm priorities”.

Consequence of inaction

At minimum, this alarm signifies the loss of view to non-direct data on the Console Station. At worst, this alarm signifies complete loss of view on the Console Station.

Corrective actions

Check that the Console is powered up and connected to the Experion Server. For more information, see “Lost contact with a Console Station”.

Time to respond

Immediate.

ORPHANS system alarms

The following topics describe orphan activity-related system alarms and how to respond to them.

Related topics

“ORPHANS - Orphan Activities Detected” on page 296

ORPHANS - Orphan Activities Detected

Potential causes

A child activity has been created on the server and the parent activity does not exist on that server, possibly due to one of the following:

1. If inter-cluster peer to peer is being used so that the parent and child activities are in different clusters, but the 2 cluster servers are not configured for DSA Alarms and Data.
2. The CEE containing the parent activity has been set to IDLE, while the CEE containing the child activity is still running.

Consequence of inaction

The child (orphan) activity will continue to run until it has reached a terminal state. The activity will then remain in the controller until it is manually removed by an operator. This may have an impact on the overall result of an batch.

Corrective actions

1. Investigate why the parent activity could not be resolved on the server.
2. If the parents cannot be resolved, navigate to the **Orphan Activity Summary** display by double clicking on the alarm, and then manually remove any orphan activities.

Time to respond

Depends on the configuration of the recipe.

Note that only one alarm is raised regardless of the number of orphan activities found.

OTHER system alarms

The following topics describe the OTHER system alarm types and how to respond to them.

Related topics

OTHER - Duplicate IOL Address

Applies to IOLINK.

Potential causes

A duplicate IOLink address has been detected.

Consequence of inaction

May result in "Not Active Supervisor" alarm, one of those module may not be recognized by controller.

Corrective actions

Check the secondary IO Modules for correct physical address.

Time to respond

Immediate.

OTHER - IOL Channel A Failure

Applies to IOLINK.

Potential causes

This alarm is raised when there are cable errors are present.

Consequence of inaction

Loss of communication with IOPs.

Corrective actions

1. Check IOLINK cable A from end to end for proper connections.
2. Check the cable connectors at the IOTAs and fix as needed.
3. Refer to the IOLINK Statistics for the error counts to zero in on the suspect link (primary IOLINK, secondary IOLINK, or IOMs) and replace if necessary.

   Once a problem has been identified and a fix is applied. To verify the fix:

   a. Reset the error counts via the I/O Link Command "RESET_ERRORS" from the Main Tab.
   b. Re-enable the Periodic Cable Swap diagnostic via the I/O Link Command "ENB_PERSWAP" from the Main Tab.
   c. Wait about 2-3 minutes for the alarm to return to normal, otherwise, monitor the error counts and if they are still accumulating, call the Honeywell SSC for support.

Time to respond

Immediate.

OTHER - IOL Channel B Failure

Applies to IOLINK.

Potential causes

This alarm is raised when there are cable errors are present.

Consequence of inaction

Loss of communication with IOPs.

Corrective actions

1. Check IOLINK cable A from end to end for proper connections.
2. Check the cable connectors at the IOTAs and fix as needed.
3. Refer to the IOLINK Statistics for the error counts to zero in on the suspect link (primary IOLINK, secondary IOLINK, or IOMs) and replace if necessary.

   Once a problem has been identified and a fix is applied. To verify the fix:

   a. Reset the error counts via the I/O Link Command "RESET_ERRORS" from the Main Tab.
   b. Re-enable the Periodic Cable Swap diagnostic via the I/O Link Command "ENB_PERSWAP" from the Main Tab.
   c. Wait about 2-3 minutes for the alarm to return to normal, otherwise, monitor the error counts and if they are still accumulating, call the Honeywell SSC for support.

Time to respond

Immediate.

OTHER - IOL Maximum Errors Exceeded

Applies to IOLINK.

Potential causes

The number of IOL Communication and Silence Errors exceeds the MAX limit.

Consequence of inaction

Loss of communication with IOPs.

Corrective actions

Channel A and Channel B errors need to be addressed.

Time to respond

Immediate.

OTHER - IOL Pre-fetch Alarm Overruns

Applies to C300 and IOLIM.

Potential causes

IO Link reports pre-fetch overrun alarm if the C300 Controller's CPU or IOLINK is heavily loaded. This alarm indicates that the C300 Controller is not able to scan input data from the Priority IOMs in a timely manner.

Consequence of inaction

End-to-end response times may be larger than expected.

Corrective actions

If this diagnostic alarm is reported, perform the following actions which may allow recovery:

1. Reconfigure the CMs PHASE to balance the output writes across multiple different phases.
2. Redistribute IOMs between the two IO Links.

Time to respond

ASAP if the alarm persists

If the alarm appears and then returns to normal as a result of a temporary condition such as a checkpoint restore, an IOM load/reload, or an IOM swap over, then it can be ignored.

OTHER - IOL Process Data Cycle Overruns

Applies to IOLINK.

Potential causes

PV scanning from the IOM or IOMs was not completed within the IOM scan rate timeframe.

Consequence of inaction

Increase in response time.

Corrective actions

Reduce the IOM's scan rate or the execution period of the Control Modules containing connections to IO Channels.

Time to respond

As soon as possible.

OTHER - IOL Processor, Diagnostic Cycle Overflow

Applies to C300 and IOLIM.

Potential causes

Internal IOLINK Communication Daughter Card diagnostic detected an internal fault.

Consequence of inaction

Possible loss of communication with the IO.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

OTHER - IOL Processor Diagnostic Exceeded Time Threshold

Applies to IOLINK.

Potential causes

The time allotted for the incremental internal diagnostic has been exceeded.

Consequence of inaction

The UM51 diagnostic may fail.

Corrective actions

Call Honeywell SSC.

Time to respond

Immediate.

OTHER - IOL Processor Diagnostic Failed To Complete

Applies to IOLINK.

Potential causes

The diagnostic task failed to finish.

Consequence of inaction

The hardware may function improperly as at least one of the diagnostics failed to complete.

Corrective actions

Call Honeywell SSC.

Time to respond

Immediate.

OTHER - IOL Processor, Diagnostic Initiation Timeout

Applies to C300 and IOLIM.

Potential causes

Internal IOLINK Communication Daughter Card diagnostic detected an internal fault.

Consequence of inaction

Possible loss of communication with the IO.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

OTHER - IOL Processor, Resumption Of Non-Wait Task

Applies to C300 and IOLIM.

Potential causes

Internal IOLINK Communication Daughter Card diagnostic detected an internal fault..

Consequence of inaction

Possible loss of communication with the IO.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

OTHER - IOL Processor Stack Limit Overflow

Applies to C300 and IOLIM.

Potential causes

Internal IOLINK Communication Daughter Card diagnostic detected an internal fault.

Consequence of inaction

Possible loss of communication with the IO.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

OTHER - IOL Processor Unknown SF

Applies to C300 and IOLIM.

Potential causes

Internal IOLINK Communication Daughter Card diagnostic detected an internal fault.

Consequence of inaction

Possible loss of communication with the IO.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

OTHER - Not Active Supervisor

Applies to IOLINK.

Potential causes

The IOL interface daughter card could not transition into the active supervisor role. Generally this is caused by a partner IOLINK with a conflicting IOLINK Address.

Consequence of inaction

Loss of communication with the IO modules.

Corrective actions

See .

Time to respond

As soon as possible.

OTHER - Partner I/F Mismatch on IOL

Applies to IOLIM and C300.

Potential causes

Only occurs in redundant configurations. The IOLINK cables from the primary (IOLIM/C300) are not connected to the correct controller or the correct Link number (in case of C300 Only).

Consequence of inaction

Loss of controller redundancy.

Corrective actions

Make sure the IOLINK cables are connected to the correct pair.

In case of C300 only, make sure that the cable from IOLINK1 and IOLINK2 of the primary are connected to IOLINK1 and IOLINK2 of the secondary, respectively.

Time to respond

As soon as possible.

OTHER - Partner I/F Not Visible On IOL

Applies to IOLINK.

Potential causes

The Primary IOLINK is unable to view it's redundant partner across the I/O Link.

Consequence of inaction

Loss of redundancy.

Corrective actions

Call Honeywell SSC.

Time to respond

As soon as possible.

Replication system alarms

The following topics describe replication-related system alarms and how to respond to them.

Related topics

“Replication - Events Database Replication Failed” on page 316
“Replication <replication number> failed” on page 317

Replication - Events Database Replication Failed

Potential causes

Redundancy replication of the Events database has failed. Can be caused by various factors.

Consequence of inaction

Events that are collected on the primary server are not journaled on the backup. If the primary server subsequently fails, these events will be lost.

Corrective actions

- Call up the **Event Archiving Operations** display.
- For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

If this alarm is raised, then events will not be journaled on the backup. This should be addressed in case the primary server fails.

Replication <replication number> failed

Potential causes

File replication did not replicate to all destinations.

Consequence of inaction

Files on some computers will not be updated.

Corrective actions

1. Call up the **File Replication Settings** display.
2. Click **View Report**.
   The file replication report for further detail on the cause of failure.
3. Check that the replication destination computers are online and available.

Time to respond

Immediately.

Scripting system alarms

The following topics describe scripting-related system alarms and how to respond to them.

Related topics

“Scripting - Script Engine Error” on page 320

Scripting - Script Engine Error

Potential causes

An undefined error has occurred with a script engine. It may be due to syntax, runtime or a timeout error.

Consequence of inaction

This alarm can be seen under the following scenarios:

1. There is a system failure in the script engine. If this happens then no scripts will run in the failed script engine.
2. There is a run time error in a script. If this happens the erroneous script will be disabled, but other scripts in the script engine will continue to execute.

Corrective actions

1. Call up the **Script Engines** display. This will identify which script engine is in error.
2. Examine the server log to identify which script engine is in error and what kind of error is it.
3. Debug and test the script so the problem no longer occurs.

Time to respond

Immediate.

Series C and Process Manager I/O System Alarms

The following topics describe the Series C Process Manager I/O system alarms and how to respond to them.

Related topics

A/D Conversion Data Overflow - 5v Supply to Application board failure

Potential causes

Overflow bit is ON in the received analog input channel data.

Consequence of inaction

The PV is set to NaN for that particular Analog Input Channel.

Corrective actions

1. In the case of non-redundant, there is a loss of view for the affected channel.
2. In the case of redundant, control goes to HEALTHY and SYNCHRONIZED PARTNER.

Time to respond

Immediate.

A/D Conversion Data Overflow - A/D Conversion Data Overflow

Potential causes

Overflow bit is ON in the received analog input channel data.

Consequence of inaction

The PV is set to NaN for that particular analog input channel.

Corrective actions

1. If non-redundant, there is a loss of view for the affected channel.
2. If redundant, control goes to HEALTHY and SYNCHRONIZED PARTNER.

Time to respond

Immediate.

A/D Conversion Incomplete - A/D Conversion Incomplete

Potential causes

Analog to digital conversion of the input channel is incomplete.

Consequence of inaction

The PV is set to NaN for that particular analog input channel.

Corrective actions

1. If non-redundant, there is a loss of view for the affected channel.
2. If redundant, control goes to HEALTHY and SYNCHRONIZED PARTNER.

Time to respond

Immediate.

ADC Register Write Failure - ADC Register Write Failure

Potential causes

ADC register write command failed.

Consequence of inaction

ADC SPI Interface is not working properly.

Corrective actions

Replace the AI IOM.

Time to respond

If non-redundant, replace immediately, otherwise replace within 8 to 24 hours.

ADC Supply Voltage Failure - ADC Supply Voltage failure

Potential causes

ADC chip is not working 100% efficiently.

Consequence of inaction

Replace the AI IOM.

Corrective actions

Replace the AI IOM.

Time to respond

If non-redundant, replace immediately, otherwise replace within 8 to 24 hours.

ADOUTUDF_042 - ADC VALUE UNDERFLOW(APPLY TO DATA I/P'S)

Potential causes

A/D slot conversion on AIM slot underflowed minimum allowed count (HLAI only).

Consequence of inaction

The device connected to that slot will no longer be under Experion control.

Corrective actions

Power cycle the I/O module and if the alarm persists then replace the I/O module.

Time to respond

Immediate.

ADPCOMFL_027 - NO COM TO ADP OR OTHER MICRO PROCSR AM

Potential causes

Communication with ADP or other microprocessor is lost.

Consequence of inaction

Analog to digital conversion process by ADP processor halts.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

ADRAMADR_01 - ADP PRIVATE RAM ADDRESSING FAILURE

Potential causes

ADP private RAM addressing failed.

Consequence of inaction

Analog to digital conversion process by ADP processor halts.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

ADRAMCNT_011 - ADP PRIVATE RAM CONTENTS FAILURE

Potential causes

ADP (Analog to Digital Processor) private RAM contents error.

Consequence of inaction

Analog to digital conversion process by ADP processor halts.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

ADROMERR_016 - ADP EPROM CHECKSUM FAILURE

Potential causes

ADP EPROM checksum failure.

Consequence of inaction

Analog to digital conversion process by ADP processor halts.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

ADSTRTUP_018 - ADP START UP FAILURE

Potential causes

ADP startup failure.

Consequence of inaction

Analog to digital conversion process can no longer be performed as ADP is not started.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

AI Channel Not Calibrated - AI IOM is out of calibration

Potential causes

If the IOMs are out of calibration and the measured/output value of these modules will not be accurate.

Consequence of inaction

Measured/output value of these IOM/IOP will not be accurate.

Corrective actions

Field calibration of these IOM/IOP needs to be performed.

Time to respond

Immediately.

AO Channel Not Calibrated - AO IOM is out of calibration

Potential causes

If the IOMs are out of calibration, the measured/output value of these modules won't be accurate.

Consequence of inaction

Measured/output value of these IOMs/IOPs will not be accurate.

Corrective actions

Field calibration of these IOMs/IOPs needs to be performed.

Time to respond

Immediate.

AO Channel Not Calibrated - SVP-IOM/SP-IOM AO channels not calibrated

Potential causes

Calibration data is not present in the Flash device.

Consequence of inaction

Fails to load the calibration data.

Corrective actions

Recalibrate the AO channels

Time to respond

Immediate.

BADADPER_017 - BAD ERROR CODE DETECTED IN ADP

Potential causes

1. ADP has failed in communications with IOLP.
2. Application processor (LLAI or STI) has a communication failure with the high-performance I/O Link card.

Consequence of inaction

ADP process cannot progress.

Corrective actions

If the error persists, replace the IOP card.

Time to respond

Immediate.

BADADPJP_034 - BAD BRANCH TAKEN IN ADP ROM EXECUTION

Potential causes

Bad branch taken during ADP ROM execution.

Consequence of inaction

The ADP processed values are faulty.

Corrective actions

Replace the LLAI IOP card for the LLAI FTA.

Time to respond

Immediate.

BADCALRF_039 - CALIBRATION REFERENCE OUTSIDE LIMITS

Potential causes

Inaccurate reference voltage provided during field calibration.

Consequence of inaction

The value measured at the ADC/DAC will be inaccurate.

Corrective actions

1. If the field calibration fails, a factory calibration is needed.
2. Alternatively, replace the IOM/IOP.

Time to respond

Immediate.

BADFLREG_044 - AO FAILURE SELECTION REGISTER IS BAD

Potential causes

AO module failure selection register is bad.

Consequence of inaction

AO module will not work as expected.

Corrective actions

Replace IOP card.

Time to respond

Immediate.

BADPLUGM_029 - BAD PLUG-IN MODULE IN FTA

Potential causes

Bad input or bad FTA plug-in module.

Consequence of inaction

The connected device using that FTA cable will no longer be under EPKS control.

Corrective actions

Test that the slot is wired correctly. If it is, replace the FTA plug-in module.

Time to respond

Immediate.

BADRESUM_003 - RESUME OF NON-WAITING TASK

Potential causes

IOP executive resumed a non-waiting task - software bug indicated.

Consequence of inaction

Unexpected behavior.

Corrective actions

Contact TAC for assistance.

Time to respond

Immediate.

BADRJVAL_033 - REFERENCE JUNCTION VALUE BAD

Potential causes

AIH,LLAI reference junction value is bad.

Consequence of inaction

The data received through that port is faulty, resulting in unexpected behavior.

Corrective actions

Check that the reference junction wire or jumper (P1) is correctly implemented on the FTA.

Time to respond

Immediate.

BADSECRG_022 - SECONDARY REGULATOR NOT OK

Potential causes

DO IOP card secondary regulator is not functioning.

Corrective actions

Replace the DO IOP card.

Time to respond

Immediate.

BDOUTBFR_046 - Bad Output Buffer

Potential causes

Output disable buffer failure.

Consequence of inaction

Disrupts process.

Corrective actions

Replace the IOP. Use Standby Manual device if IOP is non-redundant.

Time to respond

Immediate.

BDSNDLTC_045 - Bad Secondary Latch

Potential causes

Secondary latch fails or bad secondary latch.

Consequence of inaction

Disrupts process.

Corrective actions

Replace the IOP. Use a standby manual device if IOP is non-redundant.

Time to respond

Immediate.

CABLE DISCONNECT, RTP - No RTP connection

Potential causes

RTP cable has been disconnected or has failed.

Consequence of inaction

Communication loss between the field devices.

Corrective actions

Use the NDM generated Point ID and the FIM slot number in the description field to find the FIM with the disconnected RTP cable.

Time to respond

Immediate.

CALBABRT_038 - CALIBRATION SEQUENCE ABORTED

Potential causes

Calibration of an IOP card has been aborted during the calibration procedure, due to a failure.

Consequence of inaction

Calibration error.

Corrective actions

Check the precision voltage/resistance source for accuracy. Also, make sure that the correct calibration procedure is being followed.

Time to respond

Immediate.

Channel Not Field Calibrated - SVP-IOM/SP-IOM Channel not field calibrated

Potential causes

Valve position calibration status is not complete. Sensor type is LVDT or RVDT.

Consequence of inaction

Fails to load the calibration data; disrupts the process.

Corrective actions

Complete calibration.

Cold Start - Device Cold Start

Potential causes

A power failure or device reset.

Consequence of inaction

Fails to initialize the device.

Corrective actions

Check the power supply to the device and device status.

Time to respond

Immediate.

COMMS - No IOLP access to shared RAM

Potential causes

IOLP cannot gain access to shared RAM.

Consequence of inaction

Input conversion will be prohibited.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

Configuration Changed - Device Configuration Changed

Potential causes

An operation was performed that changed the device's configuration.

Corrective actions

No action may be required. Flag may be cleared.

Device Malfunction - Field Device Malfunction

Potential causes

The device detected a serious error or failure.

Consequence of inaction

IOP/IOM issues a Command 48 which requests the device specific status and conditions. Depending on the type of fault, the analog value and/or the digital variables may be set to the BAD state (unusable data). The channel remains in this mode until the fault is resolved.

Corrective actions

Resolve the detected fault. Replace the device.

Time to respond

Immediate.

DIAGCTFL_026 - AI Input-Output loopback failure

Potential causes

This soft failure is generated due to a hardware failure in the AI channel of the I/O module.

Consequence of inaction

Loss of data.

Corrective actions

Replace the faulty I/O module.

DIAGCTFL_026 - DI Input-Output loopback failure

Potential causes

This soft failure is generated due to a hardware failure in the AI channel of the I/O module.

Consequence of inaction

Loss of data.

Corrective actions

Replace the faulty I/O module.

DIAGCTFL_026 - IOM diagnostic circuit failure

Potential causes

This soft failure is generated due to a hardware failure in the AI channel of the I/O module.

Consequence of inaction

Loss of data.

Corrective actions

Replace the faulty I/O module.

DIAGOFLO_005 - ENTIRE DIAG CYCLE OVERFLOW

Potential causes

Entire diagnostic cycle overran the 2 minute allocated time in which diagnostics have to run to completion.

Consequence of inaction

1. IOP failure.
2. Loss of control.

Corrective actions

1. Investigate control point mix/strategy for an excessive load.
2. Otherwise, a possible I/O Link problem exists. Check I/O Link card, the I/O Link cable, and the IOP cards.

Time to respond

Immediate.

DIAGTMOT_004 - ONE DIAG INITIATION TIMED OUT

Potential causes

Diagnostics not run in at least 5 seconds. Processing overload.

Corrective actions

1. Investigate control point mix/strategy for an excessive load.
2. Otherwise, a possible I/O Link problem exists. Check the I/O Link card, the I/O Link cable, and the IOP cards.

Time to respond

Immediate.

DO Relay Extn Board Missing - Relay Extension Board Missing

Potential causes

Relay extension board missing.

Consequence of inaction

IOP cannot communicate to the output device. Outputs non-operational.

Corrective actions

Ensure relay board is properly installed.

Time to respond

Immediate.

DTPATHFL_069 - DATA PATH FAILURE

Potential causes

Data path failure.

Corrective actions

Replace the FTA when convenient.

DTPATHTO_070 - DATA PATH TIME OUT

Potential causes

Data path time.

Corrective actions

Replace the FTA when convenient.

EECKSMER_007 - EEPROM CHKSUM ERROR

Potential causes

EEPROM (used to hold calibration information in Analog Output IOPs) checksum failure. It usually means an Analog Output IOP is not calibrated properly.

Consequence of inaction

Improper AO calibration. Output operations accuracy is lost.

Corrective actions

1. Calibrate the Analog Output IOP card.
2. If the error persists, replace the HLAI or the AO.

Time to respond

Immediate.

EECNTERR_008 - EEPROM counter error - too many writes

Potential causes

EEPROM counter error. The number of writes to EEPROM has exceeded the safe number (10,000). This could indicate the IOP has not been calibrated, because a virgin EEPROM will fail this test.

Consequence of inaction

- Too many writes or unformatted EEPROM
- Loss of calibration data
- Less accuracy
- Process disruption.

Corrective actions

1. Calibrate the Analog Output IOP card.
2. If the error persists, replace the HLAI or the AO IOP card, or the FTA.

Time to respond

Immediate.

EEFAILED_040- EEPROM UPDATE FAILED DUE TO EEPROM BUSY

Potential causes

EEPROM update failed due to EEPROM busy.

Consequence of inaction

Calibration data may be lost.

Corrective actions

If an HLAI or AO, replace the IOP. If a LLAI, replace the affected plug-in module.

Time to respond

Immediately.

EEFLAGER_009 - EEPROM INCOMPLETION ERROR

Potential causes

Incomplete EEPROM write resulting in uncalibrated IOM.

Consequence of inaction

Uncalibrated I/O module. Process disruption.

Corrective actions

1. Calibrate the AI or AO card.
2. If the error persists, replace the HLAI or the AO IOP card, or the FTA.
3. Check EEPROM.

Time to respond

Immediate.

Feedback Inputs failure - Resolver Feedback Inputs Failure

Potential causes

This soft failure is generated when the Resolver is not connected to the field terminals. SVP_AI channel reports this soft failure when it is configured as “Resolver”.

Consequence of inaction

SVP_AI Channel PV will not be shown properly.

Corrective actions

Ensure that the wiring connection between the Resolver and the SVPM IOTA field terminals are correct.

Time to respond

Immediately.

FTA 1 Calibration Failure - FTA 1 CALIBRATION FAIL

Potential causes

FTA 1 calibration failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

Recalibrate the FTA.

Time to respond

Immediate.

FTA1 Comm Failure - FTA 1 COMMUNICATION FAIL

Potential causes

FTA 1 communication failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check the connection from the Power Adapter to FTA 1.
2. If the FTA is missing, install the FTA.
3. If the FTA is present, replace the FTA.

Time to respond

Immediate.

FTA 1 Fail - LLMUX FTA1 HAS A FAILURE

Potential causes

LLMUX or RHMUX FTA 1 has a soft failure.

Consequence of inaction

Loss of data from field.

Corrective actions

- LLMUX or RHMUX: Check FTA 1
- SI: Correct the error condition at the device connected to FTA 1.

Time to respond

Immediate.

FTA 1 Identification Error - FTA 1 IDENT ERROR

Potential causes

LLMUX FTA 1 identification failure.

Consequence of inaction

Data mismatch.

Corrective actions

Verify/correct the FTA pinning.

Time to respond

Immediate.

FTA1 Not Calibrated - FTA 1 IS NOT CALIBRATED

Potential causes

- LLMUX: FTA 1 is not calibrated
- SI: FTA 1 write buffer overflow.

Consequence of inaction

Inaccurate process values.

Corrective actions

- LLMux or RHMUX: Calibrate FTA 1
- SI: Reduce the number of writes to the FTA.

Time to respond

Immediate.

FTA 1 Ref Voltage Failure - FTA 2 VREF FAIL

Potential causes

FTA 1 reference voltage failure.

Consequence of inaction

Loss of process data/loss of control

Corrective actions

Replace the FTA.

Time to respond

Immediate.

FTA 2 Calibration Failure - FTA 3 CALIBRATION FAIL

Potential causes

FTA 2 calibration failure.

Consequence of inaction

Loss of process data/ loss of control.

Corrective actions

Recalibrate the FTA.

Time to respond

Immediate.

FTA 2 Comm Failure - FTA 2 COMMUNICATION FAIL

Potential causes

FTA 2 communication failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check the connection from the Power Adapter to FTA 2.
2. If the FTA is missing, install the FTA.
3. If the FTA is present, replace the FTA.

Time to respond

Immediate.

FTA2 Fail - LLMUX FTA2 HAS A FAILURE

Potential causes

LLMUX or RHMUX FTA 2 has a soft failure.

Consequence of inaction

Loss of data from field.

Corrective actions

1. LLMUX or RHMUX: Check FTA 2
2. SI: Correct the error condition at the device connected to FTA 2.

Time to respond

Immediate.

FTA 2 Identification Error - FTA 2 IDENT ERROR

Potential causes

LLMUX FTA 2 identification failure.

Consequence of inaction

Data mismatch.

Corrective actions

Verify/correct the FTA pinning.

Time to respond

Immediate.

FTA 2 Not Calibrated - FTA 2 IS NOT CALIBRATED

Potential causes

1. LLMUX: FTA 2 is not calibrated.
2. SI: FTA 2 write buffer overflow.

Consequence of inaction

Inaccurate process values

Corrective actions

1. LLMux or RHMUX: Calibrate FTA 2.
2. SI: Reduce the number of writes to the FTA.

Time to respond

Immediate.

FTA 2 Ref Voltage Failure - FTA 2 VREF FAIL

Potential causes

FTA 2 reference voltage failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

Replace the FTA.

Time to respond

Immediate.

FTA 3 Calibration Failure - FTA 3 CALIBRATION FAIL

Potential causes

LLMUX FTA 3 calibration failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check FTA calibration.
2. Recalibrate the FTA.

Time to respond

Immediate.

FTA 3 Comm Failure - FTA 3 communication failure

Potential causes

LLMUX FTA 3 communication failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check the connection from the Power Adapter to FTA 3.
2. If the FTA is missing, install the FTA.
3. If the FTA is present, replace the FTA.

Time to respond

Immediate.

FTA 3 Fail - AI-MUX FTA3 HAS A FAILURE

Potential causes

LLMUX: FTA 3 has a soft failure. E.g. FTA cable unplugged.

Consequence of inaction

Loss of data from field.

Corrective actions

Check FTA 3.

Time to respond

Immediate.

FTA 3 Identification Failure - FTA 3 identification failure

Potential causes

LLMUX FTA 3 identification failure.

Consequence of inaction

Data mismatch.

Corrective actions

Verify/correct the FTA pinning.

Time to respond

Immediate.

FTA 3 Not Calibrated - FTA 3 IS NOT CALIBRATED

Potential causes

FTA reference voltage is kept to zero.

Consequence of inaction

Inaccurate process values.

Corrective actions

Increase the reference voltage to 100mV.

Time to respond

Immediate.

FTA 3 Ref Voltage Failure - FTA 3 reference voltage failure

Potential causes

LLMUX FTA 3 reference voltage failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

Replace the FTA.

Time to respond

Immediate.

FTA 4 Calibration Failure - FTA 4 CALIBRATION FAIL

Potential causes

LLMUX FTA 4 calibration failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check FTA calibration.
2. Recalibrate the FTA.

Time to respond

Immediate.

FTA 4 Comm Failure - FTA 4 communication failure

Potential causes

LLMUX FTA 4 communication failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

1. Check the connection from the Power Adapter to FTA 4.
2. If the FTA is missing, install the FTA.
3. If the FTA is present, replace the FTA.

Time to respond

Immediate.

FTA4 Fail - AI-MUX FTA4 HAS A FAILURE

Potential causes

LLMUX: FTA 4 has a soft failure. E.g. FTA cable unplugged.

Consequence of inaction

Loss of data from field.

Corrective actions

Check FTA 4.

Time to respond

Immediate.

FTA 4 Identification Error - FTA 4 identification failure

Potential causes

LLMUX FTA 4 identification failure.

Consequence of inaction

Data mismatch.

Corrective actions

Verify/correct the FTA pinning.

Time to respond

Immediate.

FTA 4 Not Calibrated - FTA 4 IS NOT CALIBRATED

Potential causes

FTA reference voltage is kept to zero.

Consequence of inaction

Inaccurate process values.

Corrective actions

Increase the reference voltage to 100mV.

Time to respond

Immediate.

FTA 4 Ref Voltage Failure - FTA 4 reference voltage failure

Potential causes

LLMUX FTA 4 reference voltage failure.

Consequence of inaction

Loss of process data/loss of control.

Corrective actions

Replace the FTA.

Time to respond

Immediate.

FTA Power Failure - FTA Power Failure

Potential causes

LLMUX IOM is not able to power the FTAs.

Consequence of inaction

Loss of field data and process disruption.

Corrective actions

Replace the IOM.

Time to respond

Immediate.

FTAMISSG_006 - FTA or power adapter missing

Potential causes

- If from an LLMUX or RHMUX IOP, the power adapter is missing
- If from a Series C DO IOM the relay extension board is missing
- If from any other IOP the FTA is missing.

Consequence of inaction

Loss of field data and process disruption.

Corrective actions

1. Install the FTA or relay adapter.
2. If an FTA is present, replace the FTA or check the FTA cable.

Time to respond

Immediate.

FTAMSMCH_031 - FTA type mismatch with point configuration

Potential causes

FTA type mismatch with slot configuration.

Consequence of inaction

Loss of field data and process disruption.

Corrective actions

Reconfigure the FTA type or replace the FTA.

Time to respond

Immediate.

HART Comm Failure - HART Communication Fail

Potential causes

1. Faulty wiring
2. non-HART device on the wire
3. significant electrical noise on the wires
4. problems with the device or IOM.

Consequence of inaction

The IOM stops communicating with the HART device.

Corrective actions

1. Check the wiring.
2. Verify the device type.
3. If the problem persists replace the device or IOM, whichever is faulty.
4. Press RESETHCOMERR button to reset HNCOMERR to zero.

Time to respond

Immediate.

HART Diagnostic Underrun - HART PROCESSOR DIAGNOSTIC TASK UNDER-RUN

Potential causes

HART processor diagnostic task under-run.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HART Modem 1 Error - HART hardware error detected against DUART channel 1 or modem 1

Potential causes

HART hardware error detected against DUART channel 1 or modem 1.

Consequence of inaction

Disrupts the process.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HART Modem 2 Error - HART hardware error detected against DUART channel 2 or modem 2

Potential causes

HART hardware error detected against DUART channel 2 or modem 2.

Consequence of inaction

Disrupts the process.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HART Modem 3 Error - HART hardware error detected against DUART channel 3 or modem 3

Potential causes

HART hardware error detected against DUART channel 3 or modem 3.

Consequence of inaction

Disrupts the process.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HART Modem 4 Error - HART hardware error detected against DUART channel 4 or modem 4

Potential causes

HART hardware error detected against DUART channel 4 or modem 4.

Consequence of inaction

Disrupts the process.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HART Stack High - HSTACKHI

Potential causes

HART processor program stack above 90% usage level.

Consequence of inaction

Loss of data.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

HWFIFOFL_064 - HARDWARE FIFO FAILURE

Potential causes

Hardware FIFO buffer diagnostic failed.

Consequence of inaction

PVs of all points are set to BAD.

Corrective actions

Replace the IOP.

Time to respond

Immediate.

INPTFAIL_021 - INPUT POINT FAILURE

Potential causes

Input point failure.

Consequence of inaction

No channel PV scanning.

Corrective actions

Check which input is failing, then check the fuse on IOTA and field wiring.

Time to respond

Immediate.

IOL Address Diag Failure - IOL Address Diag Failure

Potential causes

IOL address diagnostic failure.

Consequence of inaction

Disrupts process.

Corrective actions

1. Check IOM number at device index switch.
2. Ensure correct assignment.
3. If not correct, reset to correct device index number.
4. Reset IOM.

Time to respond

Immediate.

IOM or IOTA HART Chan Failure - IOM or IOTA HART Channel Failure

Potential causes

IOM or IOTA HART channel failure

Consequence of inaction

Initializes the HART live database and discontinues all HART scanning for this channel.

Corrective actions

Replace the IOM.

Time to respond

Immediate.

IOPSWITCHOVER - IOP Switchover Occurred

Potential causes

1. Synchronized redundant module failure
2. Operator Command
3. Primary module was detected fault.

Consequence of inaction

Depending on the cause of switchover, consequences vary. Possible loss of redundancy.

Corrective actions

Check for the failures reported by the previous primary module. If no fault it may have been forced by operator.

Time to respond

Immediate.

LOSTSYNC_058 - LOSTSYNC

Potential causes

Secondary module lost synchronization with its primary.

Consequence of inaction

Loss of redundancy. Secondary fails to follow up with the primary and cannot assume the primary state on switch-over.

Corrective actions

1. If the primary module status is OK, re-sync with the START command.
2. If the primary module status is IDLE, re-sync with the IDLE command.

Time to respond

Immediately.

LVDT Core Fallout - LVDT Core Fallout

Potential causes

This alarm is generated if the LVDT core is out of LVDT.

Consequence of inaction

Bad PV generated by AI channel that will cause loss of control.

Corrective actions

Check the LVDT wiring connections.

1. Check if the LVDT core is inside the LVDT, and correct the position of the LVDT core.
2. Check the wiring to ensure that there is no open or short circuit in the LVDT cable connection.

Time to respond

Immediately.

MBCHKMER_015 - MBCHKMER

Potential causes

LLAI shared ROM checksum error. LLAI only - no AI conversion.

Consequence of inaction

Results in IOP failure, disrupting the process.

Corrective actions

Unplug IOP card and plug it back in to reset device.

Time to respond

Immediate.

MBRAMADR_014 - MBRAMADR

Potential causes

LLAI shared ROM address error. LLAI only - no AI conversion.

Consequence of inaction

Disrupts the process.

Corrective actions

Reset the IOP.

Time to respond

Immediate.

MBRAMCNT_013 - MBRAMCNT

Potential causes

LLAI shared ROM contents failure. LLAI only - no AI conversion.

Consequence of inaction

Disrupts the process.

Corrective actions

Reset the IOP

Time to respond

Immediate.

MLTINPFL_060 - MLTINPFL

Potential causes

Multiple input failure detected.

Consequence of inaction

Disrupts the process. May result in indeterminate outputs.

Time to respond

Immediate.

Module Not Calibrated - ADC OUT OF CALIBRATION

Potential causes

This SF pertains to both PM HLAI and Series C AI modules. It could a result of:

1. a bad internal reference voltage
2. an internal multiplexer failure
3. the module being badly out of calibration.

Consequence of inaction

The values read from the field device could be inaccurate or reported for the wrong channel.

Corrective actions

Recalibrate the module. If the problem persists replace the module.

Time to respond

Immediate.

More Status Available - More Status Available

Potential causes

Reading additional status information.

Consequence of inaction

Generates an additional device status alarm or event.

Corrective actions

The measurements may still be correct and suitable for use by the control system. This alarm merely indicates that Command 48 contains diagnostic information that is useful to the host.

No Response

Potential causes

1. I/O module hard failure due to a fatal fault (malfunction) either in the hardware or software.
2. IOLINK failure
3. Power loss to I/O module.

Consequence of inaction

1. Loss of control and loss of view
2. In the event of an IOLINK failure: for output modules, depending on the fault option configuration (in channel) the O/P value will be driven.

Corrective actions

1. In the case of module hard fail, reset the I/O module using user reset contacts (do not do power cycle)
2. Record the last hardware failure status code, I/O firmware and hardware revisions
3. Extract controller internal logs and IO internal logs
4. Report to TAC with all of the above information.

Time to respond

Immediate.

NOACLINE_028 - NOACLINE

Potential causes

No external AC line in the LLAI - input conversions continue.

Consequence of inaction

May continue to operate but at lesser degree of accuracy.

Corrective actions

1. Check optical coupler and associated fuse on the back panel.
2. Check that the primary (left-side) power supply module in the power system is installed and functional.

Time to respond

Immediate.

NTUSED62_062 - Data bus failure

Potential causes

Unused on I/O Link interface.

Consequence of inaction

Disrupts process.

Corrective actions

Replace the IOP.

Time to respond

Immediate.

OP Fail in Circuit/Field Wire - Failure in output circuit/field wiring detected by AO or DO

Potential causes

1. Failure in output circuit/field wiring detected by AO or DO.
2. May also indicate failure of loopback test.

Consequence of inaction

Outputs non-operational.

Corrective actions

Check field wiring and the fuses on the IOTA. If it is good, try replacing the IOTA and/or the appropriate IOM card.

Time to respond

Immediate.

Open Wire Detected - Open wire/sensor detected

Potential causes

Open wire/sensor detected in the field device connection.

Consequence of inaction

The sensor data cannot be read or the data may not be written to field device.

Corrective actions

Check the field wiring and IOTA connections.

Time to respond

Immediate.

Output Short Circuit Detected - DO channel detected a short circuit or over current situation

Potential causes

1. DO channel detected a short circuit or over current situation.
2. Wiring faults.

Consequence of inaction

Overcurrent or DO channel draws more current than is permitted. It may spoil the DO device.

Corrective actions

The shorted device or shorted wiring must be corrected. Check the field wiring and IOTA connections.

Time to respond

Immediate.

PIFAULTY_072 - FIELDBUS - FAULTY personality image

Potential causes

Personality image in F-ROM is faulty.

Corrective actions

1. Ensure that you have the correct revision of the personality software.
2. Reload the personality image.
3. If the error appears again, contact TAC.

Time to respond

Immediate.

PRVRAMFL_065 - Private RAM diagnostic failed

Potential causes

Private RAM diagnostic failed.

Consequence of inaction

PVs of all the points are set to BAD. Disrupts the process.

Corrective actions

Unplug IOP card and plug it back in to reset device.

Time to respond

Immediate.

PV Out of Limits - Primary Variable Out Of Limits

Potential causes

The PV going beyond its operating limit.

Time to respond

Immediate.

PVVALDFL_067 - PV validation diagnostic failed

Potential causes

PV validation diagnostic failed. Possibly either IOM hardware failure or bad input scan circuitry.

Consequence of inaction

PVs of all points are set to BAD. Disrupts the process.

Corrective actions

1. Unplug IOP card and plug it in back to reset device.
2. If the same alarm persists replace IOP card.

Time to respond

Immediate.

Readback Register Diag Failure - Readback Register Diagnostic Failure

Potential causes

Value read from bank registers of CPLD at startup is compared to values at run time. If they are not the same this alarm is reported.

Consequence of inaction

Disrupts the process.

Corrective actions

Internal hardware problem. Replace the IOM.

Time to respond

Immediate.

REDNDIAG_061 - REDNDIAG

Potential causes

If IOM is in SYNCD state and both wiggle bits in REDDATA are set, then this alarm is posted.

Consequence of inaction

Disrupts the process.

Corrective actions

1. If an AO, force the IOP A to be the primary then replace the FTA's plug-in module.
2. If an HLAI, synchronize the database, then replace the IOPs one at a time.

Time to respond

Immediate.

Redundancy Hardware Failure - Redundancy Hardware Failure

Potential causes

Inhibit output is faulted or partner not controlling the screws and asserting backup request.

Consequence of inaction

Loss of redundancy and hence loss of data and control.

Corrective actions

Check the redundant partner.

Time to respond

Immediate.

REQOFLOW_002 - IOP task request overflow - excessive IOL activity

Potential causes

1. Excessive IOL activity.
2. Any one task taking excessive time because of events or alarms.

Consequence of inaction

IOL time-out errors and link fault.

Corrective actions

1. Check IOL activity.
2. Contact TAC for assistance.

Time to respond

Immediate.

SCANORUN_019 - SCANORUN

Potential causes

1. Input module scan overrun. Excessive IOL activity to this IOP. Inputs have been lost.
2. Intermittently bad I/O link hardware.

Consequence of inaction

Faulty input values. Affects process.

Corrective actions

1. Check for a chattering DI point.
2. Investigate the faulty I/O link hardware.

Time to respond

Immediate.

Servo Current Driver Shutdown - Servo Current Driver Shutdown

Potential causes

This soft failure is generated due to a hardware failure on the servo driver interface.

Corrective actions

Replace the faulty I/O module.

Time to respond

Immediate.

SOECLKFL_066 - SOECLKFL

Potential causes

The SOE clock failed.

Consequence of inaction

PVs of all the points are set to BAD. Disrupts the process.

Corrective actions

Replace the IOP.

Time to respond

Immediate.

SOECNTFL_068 - SOECNTFL

Potential causes

SOE counter diagnostic failed.

Consequence of inaction

PVs of all the points are set to BAD. Disrupts the process.

Corrective actions

Replace the IOP.

Time to respond

Immediate.

Speed Channel - No Pulse Input - Speed Channel - No Pulse Detected

Potential causes

No speed probe is connected to the Speed channel terminals or there is a field open wire condition for the speed probe. This soft failure can also be generated when there is a zero speed condition in the field.

Consequence of inaction

Speed Channel PV will not be shown properly.

Corrective actions

Check the field wiring and correct if there are any improper connections to the Speed channel.

Time to respond

Immediately.

Speed RCAP Ref Clock Failure - Speed RCAP Ref Clock Failure

Potential causes

This soft failure is generated if there is a hardware failure in the Speed channel hardware.

Consequence of inaction

Speed Channel PV will not show correctly.

Corrective actions

Replace the faulty IO module.

Time to respond

Immediately.

STCKLIM_024 - STCKLIM

Potential causes

IOM stack usage is dangerously close to its limit.

Consequence of inaction

Module shutdown.

Corrective actions

1. Reduce activity on this IOM.
2. Reduce scan rate or move points to a different IOP.
3. Contact TAC for assistance.

Time to respond

Immediate.

STCOVRUN_001 - Sample time clock overrun

Potential causes

Sample time clock overrun greater than 2 x period.

Consequence of inaction

Affects the process.

Corrective actions

1. Investigate a possible I/O link problem or excessive IOL activity.
2. Check C300 IOL cards, cables, IOMs and IOL budgets.
3. Contact TAC if the alarm persists or repeatedly occurs.

Time to respond

Immediate.

STMACHFL_071 - STMACHFL

Potential causes

State machine diagnostic indicates a failure in the SOE hardware engine on a DISOE IOP.

Consequence of inaction

PVs of all points are set to BAD. Disrupts the process.

Corrective actions

Replace the IOP.

Time to respond

Immediate.

SupIna - Not Active Supervisor

Potential causes

The IOL interface daughter card could not transition into the active supervisor role. Generally this is caused by a partner IOLINK with a conflicting IOLINK Address.

Consequence of inaction

The real time data transmission is lost.

Corrective actions

Check for duplicate IOL Address.

Time to respond

Immediate.

Uncertain Pulse Input - Uncertain Pulse Input

Potential causes

This soft failure is generated in the following conditions:

1. Issues in field wiring of speed probes.
2. Excessive frequency variation in the pulse input.

Corrective actions

Check the field wiring and correct any improper connections to the speed channel.

Time to respond

Immediate.

Unstable Input - Resolver Unstable Input

Potential causes

This soft failure is generated when a Resolver angle cannot be determined due to excessive variation in the Resolver signal.

Consequence of inaction

PV will be fluctuating and there will be no stable PV.

Corrective actions

Ensure that the Resolver connection with the SVPM IOTA is correct.

Time to respond

Immediately.

Variable Out Of Limits - Non-Primary Variable Out Of Limits

Potential causes

A device variable not mapped to the PV going beyond its operating limits.

VDT ADC Selection Failure - LVDT ADC Channel Selection Failure

Potential causes

LVDT ADC channel selection failure.

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Time to respond

Immediate.

VDT Critical Signal Failure - LVDT Channel Critical Signal Failure

Potential causes

LVDT channel critical control signal failure i.e. ADC critical signals failures.

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Corrective actions

Check if LVDT is enabled for diagnostics to run.

Time to respond

Immediate.

VDT Exctn Freq Drift - LVDT Excitation Frequency Drift Greater than 100Hz

Potential causes

LVDT Excitation Frequency Drift Greater than 100Hz. This soft fail can be generated due to one of the following:

1. Wiring fault in the excitation voltage terminals (for instance, L1X+ / L1X- on the IOTA).
2. Excitation frequency generated by the external source is not within limits of the calibrated frequency.

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Corrective actions

1. Verify and correct any wiring problems at the excitation terminals.
2. Check if the excitation frequency supplied by the external source is correct.

Time to respond

Immediate.

VDT Extn Volt Out of Range - LVDT Excitation Voltage out of calibrated Range

Potential causes

LVDT Excitation Voltage out of calibrated Range. This soft failure is generated due to one of the following:

1. Wiring fault in the excitation voltage terminals (for LVDT channel, L1X+ / L1X- on the IOTA).
2. Excitation voltage generated by the external source is not within limits of the calibrated voltage.

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Corrective actions

1. Verify and correct any wiring problems at the excitation terminals.
2. Check if the excitation voltage supplied by the external source is correct.

Time to respond

Immediate.

VDT Fb A Volt Out of Range - LVDT Feeback Channel A Voltage out of calibrated Range

Potential causes

LVDT Feeback Channel A Voltage out of calibrated range. This soft failure can be generated due to faulty wiring in the feedback A voltage terminals. (For LVDT channel 1 it is L1A+ / L1A- on the IOTA).

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Corrective actions

Check if there is any faulty wiring at the feedback A voltage terminals and correct the faulty wiring.

Time to respond

Immediate.

VDT Fb B Volt Out of Range - LVDT Feeback Channel B Voltage out of calibrated Range

Potential causes

LVDT Feeback Channel B Voltage out of calibrated range. This soft failure can be generated due to faulty wiring in the feedback B voltage terminals. (For LVDT channel 1 it is L1B+ / L1B- on the IOTA).

Consequence of inaction

Field diagnosis fails resulting in process disruption.

Corrective actions

Check if there is any faulty wiring at the feedback B voltage terminals and correct the faulty wiring.

Time to respond

Immediately.

VREFFAIL_041 - Reference voltage out of range

Potential causes

In AI, the internal 5V reference is out of range. This SF pertains to both PM HLAI and Series C AI modules. This could be caused by:

1. A bad internal reference voltage.
2. An internal multiplexer failure.
3. The module being out of calibration.

Consequence of inaction

The values read from the field device could be inaccurate or reported for the wrong channel.

Corrective actions

Recalibrate the module. If the problem persists replace the module

Time to respond

Immediately.

VTESTFAI_030 - VTESTFAI

Potential causes

Test voltage reference >5% out of range - PVAUTO to NAN.

Consequence of inaction

The PV is set to NAN by the IOP.

Corrective actions

Replace the IOP card.

Time to respond

Immediate.

VZERO_FL_032 - VZERO_FL

Potential causes

Zero Reference voltage out of range in AI and AO IOMs. Zero reference failure.

Consequence of inaction

The PV is set to NAN, by the IOP for AI.

Corrective actions

Replace the PMIO.

Time to respond

Immediate.

WRITENBL_059 - WRITENBL

Potential causes

AO or DO write enable protection failure.

Consequence of inaction

IOP failure can result in indeterminate outputs.

Corrective actions

Replace the IOP at the earliest convenience.

Time to respond

Immediate.

WRONG_HW_063 - WRONG_HW

Potential causes

I/O redundancy configured on non-supported hardware revision.

Consequence of inaction

I/O redundancy is lost.

Corrective actions

Replace the IOP with an IOP that supports redundancy (proper hardware revision).

Time to respond

Immediate.

SYNC system alarms

The following topics describe synchronization-related system alarms and how to respond to them.

Related topics

“SYNC - Backup Point Database Larger” on page 454
“SYNC - Backup Inconsistency Detected” on page 455
“SYNC - Backup Server Error Starting” on page 456

SYNC - Backup Point Database Larger

Potential causes

The synchronization of the primary and backup server cannot be completed as the backup point database is larger than the primary point database.

Consequence of inaction

Corrective actions

Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.

For assistance in resolving the problem, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Synchronization is lost immediately when this alarm occurs. Time to respond will depend on assessment of process/site/operations for criticality/risk of losing synchronization.

SYNC - Backup Inconsistency Detected

Potential causes

The backup server has detected a request that if processed, would corrupt its database.

Consequence of inaction

Server synchronization has failed, so the backup server database will not be updated with the changes from the primary server (including point configuration, history, events, etc.), and some automatic failover actions will not be triggered.

Corrective actions

Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.

Repeat synchronization attempt. If repeated attempts fail, capture a diagnostic package and send it to your Honeywell Technical Assistance Center (TAC) for investigation.

Time to respond

Synchronization is lost immediately when this alarm occurs. Time to respond will depend on assessment of process/site/operations for criticality/risk of losing synchronization.

SYNC - Backup Server Error Starting

Potential causes

The backup server failed to restart correctly after synchronizing with the primary server.

Consequence of inaction

Backup Server (and therefore server redundancy) is not available. The system shall continue to run on Primary, but without redundancy.

Corrective actions

Check the backup server status on the **System Status** display. For more information, see “Checking the status of redundant servers”.

1. Set the backup server status to Database Only.
2. Set the backup server status to System Running.
3. Resynchronize the backup and primary servers. For more information, see “Synchronizing the server databases”.

Time to respond

When the alarm is raised, Backup is already unavailable. The time to respond will depend on assessment of process/site/operations for criticality running without the backup server being available.

Systems Management system alarms

The following topics describe Systems Management-related system alarms and how to respond to them.

Related topics

ACE:CDA-SP : Experion PKS CDA-SP Service stopped

The System Health Monitor has detected that a crucial service is not running. The CDA-SP service allows OPC communication from the Control Data Access – to - supervisory platform (CDA-sp).

Potential causes

1. The service failed to auto-start after a reboot due to a configuration error.
2. A user manually stopped the service.
3. The running service failed.

Consequence of inaction

Potential loss of view.

Corrective actions

From the services panel, start the “Experion PKS CDA-SP Service” service.

If the service does not start, note the failure condition cited in the error message, correct the condition, and try again to start the service.

Time to respond

The condition should be addressed immediately.

CAS: Component Admin Service is not running

The System Health Monitor has detected that a crucial service is not running. The system management Component Admin Service manages HCI Servers that choose to be managed. It provides event notifications to WMI clients like the System Management Display and Redirection Manager.

Potential causes

1. The service failed to auto-start after a reboot due to a configuration error.
2. A user manually stopped the service.
3. The running service failed.

Consequence of inaction

Without the CAS service, the status of components is unknown.

Corrective actions

From the services panel, start the service “sm-Component Admin Service”.

If the service does not start, note the failure condition cited in the error message, correct the condition, and try again to start the service.

Time to respond

The condition should be addressed immediately.

CAS: was unable to Checkpoint component <component name> Error = <error num>:<error string>

Potential causes

The various causes of this alarm are described in the alarm <error num> and <error string>.

Consequence of inaction

The checkpoint file for the component is not current. If the component were to be reloaded at this time it would be loaded with data from the last successful checkpoint. If that checkpoint file is current (that is, no component configuration changes were made since the file was created) there would be little or no consequence should the component need to be reloaded. However, if that checkpoint is obsolete (that is, component configuration changes have occurred since the checkpoint file was created) the configuration data will be lost if the component is reloaded. For example, if the component should fail at a time when the checkpoint file is obsolete, and then get reloaded from the obsolete file, all configuration changes made since the last successful checkpoint would be lost.

Corrective actions

The solution varies for each cause. For known causes, the error string will likely provide enough information to correct the problem. If the error string does not provide sufficient information (and for unknown causes) the component log file must be examined. The alarm comes from CAS, but CAS is just reporting the error returned from the component so further investigation must be done on the specific component. The solution may require enabling logging on the component, initiating a checkpoint again, and then examining the log file for the cause.

Time to respond

Current checkpoints should be maintained so that components can be reliably restarted at any time. Correct the problem and create a checkpoint as soon as possible.

<Component Name>: Component state changed from <previous state> to Communication Failure

Component cannot communicate with underlying device. This is comparable to “component failed”.

Potential causes

1. The state of the component's underlying device (or devices) has changed from a running state to a state that renders the component failed.
2. Unknown.

Consequence of inaction

Loss of redundancy. This component has essentially failed and redundancy has been lost.

Potential loss of view. If the redundant partner is not running or should stop, view will be lost.

Corrective actions

1. Restart any failed devices. Search proximate alarms for indication of the cause of the device failure.
2. Attempt to restart the component. Note the failure time and look in the event viewer application log for an entry pertaining to the failure. Look also in the event viewer system event log.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

<Component name>: Component state changed from <previous state> to Failed

Component failed.

Potential causes

1. The state of the component's underlying device (or devices) has changed from a running state to a state that renders the component failed.
2. Unknown.

Consequence of inaction

Loss of view. The component has failed and view to the device is lost.

Corrective actions

1. Restart any failed devices. Search proximate alarms for indication of the cause of the device failure.
2. Attempt to restart the component. Note the failure time and look in the event viewer application log for an entry pertaining to the failure. Look also in the event viewer system event log.

Time to respond

The condition should be addressed immediately.

<Component name>: Component state changed from <previous state> to Warning

Component state changed to warning.

Potential causes

1. The state of the component's underlying device (or devices) has changed from a running "OK" state to a state less than OK.
2. The component is starting up and the warning state is just a step in the progression from “Stopped”, “Failed”, or “Off”.

Consequence of inaction

Potential loss of redundancy. An underlying device may be failed or partially failed.

Potential loss of view. If the redundant device is not running, or should stop, view will be lost.

Corrective actions

1. Restart any failed devices. Search proximate alarms for indication of the cause of the device failure.
2. Monitor state to ensure that it proceeds to “OK” or “Running”.

Time to respond

For loss of redundancy, the condition should be addressed as soon as possible.

For loss of view, the condition should be addressed immediately.

<Component Name>: Device state changed from <previous state> to Communication Failure

Some devices communicate with “sub-devices”. Failure in that communication is comparable to “device failed”, which has the description “There is an error in the device or in the communications channel to the device”.

For example, TPNServer_Boiler1: Device state changed from Running to Communication Failure

Potential causes

1. Device failed.
2. Watchdog timeout. The device has not reported status or data to the component for some time.
3. The device is starting up and the warning state is just a step in the progression from “Stopped”, “Failed”, or “Off”.

Consequence of inaction

Loss of redundancy. This device has essentially failed and redundancy has been lost.

Potential loss of view. If the redundant device is off or should fail, loss of view will occur.

Corrective actions

1. Attempt to re-start the device. Use device specific information in the message to troubleshoot the device.
2. Look at performance indicators for the device and the opponent-to-device network status. For some devices and channels, this information is available on the component's auxiliary status display. Double-click the alarm in System Status Display to get to the detail page of the node. Use the components tab to navigate to the component and then select the aux. display button. Note that not all component types have an auxiliary display.
3. Monitor state to ensure that it proceeds to “OK” or “Running”.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

<Component name>: Device state changed from <previous state> to Failed. Device Info: <device info>

There is an error in the device or in the communications channel to the device.

Potential causes

1. Device failed.
2. Watchdog timeout. The device has not reported status or data to the component for some time.
3. The device is starting up and the warning state is just a step in the progression from “Stopped”, “Failed”, or “Off”.

Consequence of inaction

Loss of redundancy. This device has failed and redundancy has been lost.

Potential loss of view. If the redundant device is off or should fail, loss of view will occur.

Corrective actions

1. Attempt to restart the device. Use device specific information in the message to troubleshoot the device.
2. Look at performance indicators for the device and the opponent-to-device network status. For some devices and channels, this information is available on the component's auxiliary status display. Double-click the alarm in System Status Display to get to the detail page of the node. Use the components tab to navigate to the component and then select the aux. display button. Note that not all component types have an auxiliary display.
3. Monitor state to ensure that it proceeds to “OK” or “Running”.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

<Component name>: Device state changed from <previous state> to Warning. Device Info: <device info>

There is an error in the device or in the communications channel to the device.

Potential causes

1. Device error.
2. Watchdog timeout. The device has not reported status or data to the component for some time.
3. The device is starting up and the warning state is just a step in the progression from “Stopped”, “Failed”, or “Off”.

Consequence of inaction

Potential loss of redundancy. Depending on the device and the warning information, loss of redundancy may occur.

Potential loss of view. Depending on the state of the redundant device, loss of view may occur.

Corrective actions

1. Attempt to re-start the device. Use device specific information in the message to troubleshoot the device.
2. Look at performance indicators for the device and the component-to-device network status. For some devices and channels, this information is available on the component's auxiliary status display. Double-click the alarm in System Status Display to get to the detail page of the node. Use the components tab to navigate to the component and then select the aux. display button. Note that not all component types have an auxiliary display.
3. Monitor state to ensure that it proceeds to “OK” or “Running”.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Control Firewall <device name> (address <Fw address>) port <port ID> excessive TX_PAUSE change. Cur:<Tx Pause Val> Last:<Last Tx Pause Val>

The Control Firewall detected a possible network loop in the system. Typically, a loop is created by having extra crossover cables between switches or CF9s resulting in an infinite path for multicast traffic.

Potential causes

This is caused by a network loop in the system.

Consequence of inaction

Potential loss of redundancy. A loop may cause devices to block.

If both channels become blocked, loss of view will occur.

Corrective actions

Evaluate the network for misplaced cables or possibly dual homed nodes. If unable to immediately identify the loop, contact TAC/Network Services to have a network survey done.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Control Firewall <Fw name> (address <Fw address>) has blocked ports

The Control Firewall is blocking the ports due to a possible network loop in the system. If the Control Firewall sees messages from multiple MACs on a downlink port, it will enter the blocking mode. Typically, a loop is created by having extra crossover cables between switches or CF9s resulting in an infinite path for multicast traffic.

Attention
This event is generated only in Control Firewall.

Potential causes

This is caused by a network loop in the system.

Consequence of inaction

For non-redundant devices, a loss of view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss of view will occur.

Corrective actions

Evaluate the network for misplaced cables or possibly dual homed nodes. If unable to immediately identify the loop, contact TAC/Network Services to have a network survey done.

Time to respond

The condition should be addressed as soon as possible.

Control Firewall <Fw Name> (address <Fw address<) is no longer being heard by FTE

A WMI instance deletion event was received for the firewall.

Potential causes

1. The Control Firewall uplink cable has failed or has been disconnected.
2. The Control Firewall has been powered down or otherwise lost power.

Consequence of inaction

For non-redundant devices, a loss-of-view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss-of-view will occur.

Corrective actions

1. Re-connect or replace the uplink cable.
2. Power up the Control Firewall.

Time to respond

The condition should be addressed as soon as possible.

Control Firewall <Fw Name> (address <Fw Address>) port <port index> link status is Down

The Polling Timer detected a link status change and the link is down.

Potential causes

This alarm indicates that the device connected to the port has failed (or been powered down) or that the connection from the port to the device has failed (cable failure or disconnect). Double-click on the alarm to see the Detail Display and navigate to the ports tab for additional information.

1. The device connected to the port has failed or been powered down.
2. The cable from the port to the device has failed or been disconnected.

Consequence of inaction

For non-redundant devices, a loss-of-view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss-of-view will occur.

Corrective actions

1. Check and correct the power and status of the device. Replace the device if necessary.
2. Check and correct the cables from the port to the device. Replace the cable if necessary.

Time to respond

The condition should be addressed as soon as possible.

Control Firewall <Fw name> (address<Fw address>) uplink RX_OCTETS has stalled. Check for intermittent cable

The Control Firewall (CF) has not acknowledged receiving a status request within the timeout period.

Attention
Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

Potential loss of redundancy.

The paths to the devices (through this CF) may no longer be functional. If redundancy is lost and other paths to the devices are unavailable, loss of view will occur.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Control Firewall <Fw name> (address<Fw address>) uplink TX_OCTETS has stalled. Check for intermittent cable

The switch (Control Firewall) has not reported a status request within the timeout period.

Attention
Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

Potential loss of redundancy.

The paths to the devices (through this Control Firewall) may no longer be functional. If redundancy is lost and other paths to the devices are unavailable, loss of view will occur.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Excessive Disk Paging: memory resource issue is causing excessive disk paging

Potential causes

Paging is the process of moving fixed size blocks of code and data from RAM to disk using units called pages in order to free memory for other uses. Although some paging is acceptable because it enables the use of more memory than actually exists, constant paging is a drain on system performance. Reducing paging will significantly improve system responsiveness.

Consequence of inaction

Insufficient resources can compromise the entire node.

Corrective actions

1. Make sure the node meets Honeywell's minimum memory requirements for the node type.
2. Use the task manager to identify any non-Honeywell processes that are using large amounts of memory. Stop those processes if reasonable to do so.
3. If only Honeywell processes are running and excessive paging persists, call TAC. There are a number of Microsoft recommendations to alleviate excessive disk paging (setting page file size, splitting page file onto multiple disks, and so on) but these should be supervised by TAC.

Time to respond

The condition should be addressed immediately.

FTE device <device name> (Device Index: <device index>) has detected a duplicate

The device index is used more that once within the multicast group.

Potential causes

Configuration error when assigning FTE device names.

Consequence of inaction

Potential loss of view, potential alarm inconsistencies. Duplicate indexes cause indeterminate problems.

Corrective actions

Use the FTE event log to identify the duplicate index. Follow the steps in the "Verify duplicate device indexes were not assigned" topic in the "Troubleshooting FTE" section of the *Fault Tolerant Ethernet Installation and Service Guide*. The duplicate status can also be seen in the FTE Heartbeat Node Status Display.

In the Honeywell FTE Mux-IM Protocol Driver Properties page, resolve any duplicates. Follow the steps in the "Modify FTE settings" topic in the "Operating and servicing FTE" section of the *Fault Tolerant Ethernet Installation and Service Guide*.

Time to respond

The condition should be addressed immediately.

FTE device <device name> disjoined FTE community (no longer being heard)

The FTE driver is no longer receiving messages from the device.

The device is no longer being heard on either the A or the B interface. This could be due to a problem in the device itself or in the loss of redundant communication paths (redundant cable failures or redundant switch failures). In this state the device will not appear in the FTE Status Display.

Potential causes

1. The FTE device failed or was powered down.
2. Look in the System Status for numerous, proximate alarms, for other devices disjoining. If there is NO indication of numerous other devices that have disjoined simultaneously, and if it is known that the device is powered up, it is likely that both cables have failed.
3. Look in the System Status for numerous, proximate alarms, for other devices disjoining. If there are numerous devices that have disjoined simultaneously, it may indicate a common point of failure such as a switch.
4. In the case of duplicate device index, FTE effectively turns off, but the node may still be able to communicate if there are no faults in the network (since redundancy is lost).

Consequence of inaction

Loss of view. View to the device has been lost.

Corrective actions

1. Power up the device.
2. Check and correct all cables in the path from the device.
3. Check and correct all switches in the path from the device.
4. Correct device index.

Time to respond

The condition should be addressed immediately.

FTE Device <device name> interface <A/B> status is SILENT

The 1-second status monitor detected a change. For the current cycle, no status update was received from the device on the stated interface.

For more information about monitoring FTE devices, see the “Monitoring nodes in an FTE network” topic, in the “Operating and Servicing FTE” section of the *Fault Tolerant Ethernet Installation and Service Guide*.

Potential causes

1. DISJOIN: Look for a proximate event stating the device has “disjoined FTE community (no longer being heard)”. If the DISJOIN event exists, address that event first because when the device is no longer being heard, it will not appear in the FTE Status Display that is used to diagnose the “SILENT” event.
2. Cable fault: Open the FTE Status Display and locate the device in the PDTag column. If there are relatively few devices that are SILENT, it is likely that each SILENT represents a cable fault.

   The cause is that a cable has failed (or been disconnected) in the path that connects the device to the system.
3. Switch Failure: Open the FTE Status Display. If there are numerous devices that are SILENT, it may indicate a common point of failure such as a switch.

   The cause is that a switch that connects the device to the system has failed or has been powered down.
4. Link speed/duplex: Open the FTE Status Display. If the device is toggling between “OK” and “SILENT” it may indicate a configuration error in the “Link speed / Duplex” setting of a network adapter or switch port. This may also manifest as appearing/disappearing in the FTE Status Display when both adapters or both ports, are in error.

   The cause is a link speed/duplex configuration error.
5. Switch Uplink Error: Open the FTE Status Display. If there are numerous devices disconnected on either A or B, it may indicate a switch uplink cable error.

   The cause is an uplink cable, on a lower level switch, has failed or been disconnected.

Consequence of inaction

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss-of-view will occur.

Corrective actions

1. Look for a proximate event stating the device has a “disjoined FTE community (no longer being heard)”. If the DISJOIN event exists, address that event first, as the device is no longer being heard and it will not appear in the FTE Status Display to be able to diagnose the “SILENT” event.
2. Check and correct all of the cables from the device to the system by observing LED status at each connection.
3. Check and correct the power and status of all switches in the path that connects the device to the system.
4. Check “Link speed / Duplex” setting of the device’s network adapters and their connected switch ports. It is advisable to check the link speed and duplex settings of all network adapters and switch ports.
5. Check and correct the uplink cables of all switches in the path that connects the device to the system.

Time to respond

The condition should be addressed as soon as possible.

FTE/Heartbeat network packet delivery to application layer is being delayed. Node is experiencing Disk/CPU resource utilization issues

Potential causes

1. High CPU usage.
2. High disk access: This could be low RAM causing page faults, a misbehaving app, or even a virus scan.

Consequence of inaction

Potential loss of view. Insufficient resources can compromise the entire node.

Corrective actions

1. Use task manager to locate applications that are using excessive CPU. Use application-specific troubleshooting guidelines to reduce the amount of CPU used by those applications. Restart those applications if necessary.
2. Close any non-critical applications and attempt to identify applications that are using excessive resources. Track page faults in performance monitor. Assistance from TAC is recommended for this.

Time to respond

The condition should be addressed immediately.

FTE STATUS: Device state changed from <previous state> to Failed. Device Info: <device information string>

Potential causes

The cause of the failure is included in the “Device Info”, the device information string of the alarm.

Consequence of inaction

Loss of redundancy. This device has failed and redundancy has been lost.

Potential loss of view. If the redundant device is off or should fail, loss of view will occur.

Corrective actions

1. If the <device information string> is “This FTE Node has a Crosslink Failure”, check and correct the crosslink cables in the path from the device to the system.
2. If the <device information string> is “This device info heartbeat provider has stopped. FTE status cannot be determined”, check the SM-Heartbeat Provider service and start it if it is not running. Ensure that the service starts. The executable for this service is named *fteprovider.exe*.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

FTEProvider: FTE Provider is not running

The System Health Monitor has detected that a crucial service is not running. The system management FTE Provider service relays information from the FTE driver to the various applications that use FTE for system communications and it provides an “I’m alive” heartbeat.

Potential causes

1. The service failed to auto-start after a reboot due to a configuration error,
2. A user manually stopped the service,
3. The running service failed.

Consequence of inaction

FTE Provider is a crucial link in both FTE and non-FTE node communication.

Corrective actions

From the services panel, start the service “sm-Component Admin Service”.

If the service does not start, note the failure condition cited in the error message, correct the condition, and try again to start the service.

Time to respond

The condition should be addressed immediately.

HCINS: Alias name: <component alias name> exists on two nodes in the same TPSDomain. You must remove or rename one of them to solve this problem

Two components exist that have the same alias name but different definitions. That is, either the PROGID or the ACCESS (component type) of one component is different from that of the other component.

Potential causes

This can be caused by configuring or adding a component while some node in the system is down (For example, adding or configuring “AliasNameX” while “Node1” is down). When Node1 restarts, it replicates the names in its repository. If AliasNameX was already in Node1’s repository, and if that definition is different from the new definition, then the duplicate condition exists and the event is logged.

Consequence of inaction

Potential alarm and data inconsistencies.

Corrective actions

You must remove or rename one of the components to solve this problem. Local components can be deleted using the “Name Service Configuration” tool in the System Management Display. Domain components can only be deleted (or renamed) using the “HCI Component Configuration” tool which is also accessed through System Management Display.

Time to respond

The condition should be addressed immediately.

HCINS: Alias name: <component alias name> from the component alias file conflicts with the one in the repository - You must remove Alias name from the component alias file to solve this problem

A component alias file is being imported and it contains a definition that conflicts with a component already in the repository.

Potential causes

This occurs during the import of a component alias file which contains a component by the same name (but different definition) as a component already in the repository. Allowing the import would result in a duplicate alias name condition so the import is blocked.

Consequence of inaction

Inability to configure the system.

Corrective actions

Remove the alias definition from the file or remove the alias name from the repository.

Time to respond

The condition must be addressed before configuration can proceed.

Modbus/TCP Firewall <Fw Name>(address <Fw Address>) port <port index> link status is Down

The Polling Timer detected a link status change and the link is down.

For more information, see the “Modbus TCP Firewall faceplate and detail displays” topic in the “Monitoring Modbus TCP Firewall” section of the *Honeywell Modbus TCP Firewall User Guide*.

Potential causes

The MODBUS/TCP Firewall (MBTCP) has two ports, secure and unsecure. The secure port connects to the FTE network. The unsecure port connects to a Modbus device network switch or, less commonly, directly to a Modbus device.

If the unsecure connection goes down there is a proximate alarm noting this event. If the secure connection goes down, or if the firewall fails, there is a proximate alarm noting the firewall is “no longer heard”. That alarm does not distinguish between interface, device, switch, or cable failure.

Possible causes for this event are these:

1. The MBTCP has been powered off or otherwise failed.
2. The cable that connects to the port has been disconnected or has otherwise failed.
3. The switch to which the port connects has been powered down or otherwise failed.

Attention

The MBTCP uses a generic 9 port faceplate but statistics are only available for the Uplink port and Port 1. Port 2 through Port 8 display bad-quality data.

Consequence of inaction

For non-redundant devices, a loss-of-view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss-of-view will occur.

Corrective actions

1. Check and correct the power and status of the MODBUS/TCP Firewall.
2. Check and correct the power and status of the Modbus device network switch that connects to the unsecure port.
3. Check and correct the power and status of the switch that is connected to the secure port.

Time to respond

The condition should be addressed as soon as possible.

Modbus/TCP Firewall <Fw name> (address<Fw address>) uplink RX_OCTETS has stalled. Check for intermittent cable

The switch (Modbus/TCP Firewall) has not acknowledged receiving a status request within the timeout period. The paths to the devices (through this FW) may no longer be functional.

Attention
Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

For non-redundant devices, a loss of view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss of view will occur.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Modbus/TCP Firewall <Fw name> (address <Fw address>) uplink TX_OCTETS has stalled. Check for intermittent cable

The switch (Modbus/TCP Firewall) has not reported a status request within the timeout period. The paths to the devices (through this firewall) may no longer be functional.

Attention
Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

For non-redundant devices, a loss of view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss of view will occur.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

Modbus/TCP <Fw Name> (address <Fw address>) is no longer being heard by FTE

A WMI instance deletion event was received for the switch.

Potential causes

When this alarm is reported, it does not distinguish between interface, device, switch, or cable failure.

Possible causes for this event are:

1. The Modbus/TCP Firewall has failed or been powered down.
2. The cable, that connects to the secure port, has failed or been disconnected.
3. The switch, connected to the secure port, has failed or been powered down.

Consequence of inaction

For non-redundant devices, a loss of view has occurred.

For redundant devices, redundancy is lost. If the other path to the device is unavailable, a loss of view will occur.

Corrective actions

1. Power up the Modbus/TCP Firewall.
2. Check and correct the cable that connects the secure port to the switch.
3. Power up the switch.

Time to respond

The condition should be addressed as soon as possible.

One-Wireless Firewall <Fw Name> (address <Fw address>) is no longer being heard by FTE

A WMI instance deletion event was received for the switch.

Potential causes

When this alarm is reported, it does not distinguish between interface, device, switch, or cable failure.

Possible causes for this event are as follows:

1. The OneWireless Firewall has failed or been powered down.
2. The cable, that connects to the secure port, has failed or been disconnected.
3. The switch, connected to the secure port, has failed or been powered down.

Consequence of inaction

Loss of view has occurred.

Corrective actions

1. Power up the OneWireless Firewall.
2. Check and correct the cable that connects the secure port to the switch.
3. Power up the switch.

Time to respond

The condition should be addressed immediately.

One-Wireless Firewall <Fw Name>(address <Fw Address>) port <port index> link status is Down

The Polling Timer detected a link status change and the link is down.

Potential causes

The OneWireless Firewall (OWFW) has two ports, secure and unsecure. The secure port connects to the FTE network. The unsecure port connects to the wireless network.

If the unsecure connection goes down there is a proximate alarm noting this event. If the secure connection goes down, or if the firewall fails, there is a proximate alarm noting the firewall is “no longer heard”. That alarm does not distinguish between interface, device, switch, or cable failure.

Possible causes for this event are these:

1. The OWFW has been powered off or has otherwise failed.
2. The cable that connects to the port has been disconnected or has otherwise failed.
3. The switch to which the port connects has been powered down or has otherwise failed.

Consequence of inaction

A loss-of-view has occurred.

Corrective actions

1. Check and correct the power and status of the OWFW.
2. Check and correct the power and status of the wireless network that connects to the unsecure port.
3. Check and correct the power and status of the switch that is connected to the secure port.

Time to respond

The condition should be addressed as soon as possible.

One-Wireless Firewall <Fw name> (address <Fw address>) uplink RX_OCTETS has stalled. Check for intermittent cable

The switch (OneWireless Firewall) has not acknowledged receiving a status request within the timeout period. The paths to the devices (through this firewall) may no longer be functional.

Attention

Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

Loss of view has occurred.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

The condition should be addressed immediately.

One-Wireless Firewall <Fw name> (address <Fw address>) uplink TX_OCTETS has stalled. Check for intermittent cable

The switch (OneWireless Firewall) has not reported a status request within the timeout period. The paths to the devices (through this firewall) may no longer be functional.

Attention
Intermittent cables include partially failed cables where the link may still be active, but TX or RX wire pairs have failed.

Potential causes

The path from the uplink port to the system, which had previously passed data, has failed.

Consequence of inaction

Loss of view has occurred.

Corrective actions

Check and correct the uplink cable and connections. Check and correct all cables and connections in the upstream from the uplink cable.

Time to respond

The condition should be addressed immediately.

OPC Event Source: <node name>. Proxy ARP agent found. Check router configuration

Potential causes

By default router interfaces run a proxy ARP agent. In cases where devices are not on the same subnet as the routed interface (common with controllers under best practices) the router will respond to ARP requests for the controllers MAC address with its own MAC address, potentially causing loss of view to the controller. This can be intermittent depending on which ARPs from the controller and the router for the controller IP address reach the other nodes. The AddRoute service periodically checks to see if the router is performing the proxy ARP function and logs this event if the router responds with a proxy ARP.

Consequence of inaction

See “Potential causes” above.

Corrective actions

Add the “no ip proxy-arp” command to the routed interfaces connected to an FTE network.

Time to respond

The condition should be addressed immediately.

SNMP Trap: - <IP Address> Type - AuthenticationFailure

Generated when the sending device receives a message that is not properly authenticated. For example, an incorrect login attempt. An AuthenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that does not have proper authentication.

Potential causes

This trap occurs when a network management system (NMS) polls the device with the wrong community string.

Consequence of inaction

Potential loss of redundancy. The device reporting path (through this switch) may be lost.

If both reporting paths (through both switches) is lost, loss of view will occur.

Potential no-impact. This could be a configuration issue that does not impact view.

Corrective actions

The IP address in the trap indicates the origin of the message. Investigate there for authentication errors.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

SNMP Trap: - <IP Address> Type - ColdStart

Trap signifies that the sending device is re-initializing itself and may have been altered.

Potential causes

Switch is powered up.

Consequence of inaction

Not applicable.

Corrective actions

No action required.

Time to respond

Not applicable.

SNMP Trap: - <IP Address> Type - LinkDown; Index - <Index>

The sending device recognizes the failure of a communication link.

Potential causes

1. Switch is powered down or failed.
2. Cable is disconnected or failed. This includes the cross cable.
3. Device is powered down or fails.
4. Control Firewall is powered down or fails.
5. Control Firewall uplink port is disconnected or fails.

Consequence of inaction

Loss of redundancy. The device reporting path (through this switch) has been lost.

If the device reporting path (through the other switch) is lost, loss of view will occur.

Corrective actions

1. Power up the switch. Replace or repair switch if necessary.
2. Examine physical path to device and connect all cables. Replace or repair cables if necessary.
3. Power up the device. Replace or repair device if necessary.
4. Power up the Control Firewall. Replace or repair the Control Firewall.
5. Reconnect Control Firewall uplink port. Replace or repair Control Firewall if necessary.

Time to respond

For loss of view, the condition should be addressed immediately.

For loss of redundancy, the condition should be addressed as soon as possible.

SNMP Trap: - <IP Address> Type - WarmStart

Trap signifies that the sending device is re-initializing itself and has not been altered.

Potential causes

Switch reset.

Consequence of inaction

Not applicable.

Corrective actions

No action required.

Time to respond

Not applicable.

SRP(syncrep.exe): FTE Status cannot be determined. Restart FTE Status server. <error message>

Various errors are funneled into this event.

Potential causes

FTEStatus got an error while executing a WMI query.

Consequence of inaction

Device reporting state cannot be determined.

Corrective actions

From the System Status Display, restart the FTEStatus server.

Time to respond

The condition should be addressed immediately.

SRP(syncrep.exe): SRP has not heard expected traffic for an excessive period. Reconnecting Receive socket

The SRP multicast receive message handler timed out (2 minutes) while waiting for an input message. This means that the node has not even received its own message that is sent periodically from the SRP multicast send message handler. This can indicate an error in the configuration or network adapter binding order, or it can indicate an error in the configuration of network adapter link speed/duplex.

Potential causes

1. Typically this does not occur in FTE nodes because the FTE installation sets the binding order automatically. For non-FTE nodes, the user must configure this manually.
2. Typically this does not occur in FTE nodes because the FTE installation sets the binding order automatically. For non-FTE nodes, the user must configure this manually.

Consequence of inaction

Loss of alarms on this node.

Corrective actions

1. Make sure the primary and secondary adapters are at the top of the preference order under network adapter advanced settings.
2. Make sure the link-speed duplex settings are correct so that the network card does not lose connection. Typically this needs to be set to 100MB/Full duplex, but check the release-specific specifications.

Time to respond

The condition should be addressed immediately.

Synchronization requests were not answered by node(s): <node list>

Potential causes

1. Network configuration is preventing Synchronized Repository Provider (SRP) communication between nodes.
2. Synchronized Repository Provider (SRP) configuration is preventing SRP communication between nodes.

Consequence of inaction

Nodes are out of sync with respect to the state of the various system alarms and events within the multicast scope - an accurate view of system events is not available. Failure to receive and display an alarm could make an operator unaware of a critical event.

Corrective actions

1. Verify that adapters and corresponding switch ports are set to 100MB/Full duplex. Verify network interfaces are configured correctly with respect to IP configuration.
2. Verify that SRP multicast addresses are correct adapters and corresponding switch ports are set to 100MB/Full duplex.

Time to respond

This should be addressed immediately.

SysEvtProv: System Event Provider is not running

The System Health Monitor has detected that a crucial service is not running. The system management System Event Provider service captures windows events into a common synchronized repository of events. A filter file is used to identify window events to be produced into the synchronized repository.

Potential causes

1. The service failed to auto-start after a reboot due to a configuration error.
2. A user manually stopped the service.
3. The running service failed.

Consequence of inaction

Potential loss of alarms and potential loss of events. Without this service, system events and alarms are not maintained.

Corrective actions

From the services panel, start the “sm-System Event Provider” service.

If the service does not start, note the failure condition cited in the error message, correct the condition, and try again to start the service.

Time to respond

The condition should be addressed immediately.

The system detected an address conflict for IP address <IP Address> with the system having <network> hardware address <hdw address>. <Message>

Where:

- for Event ID 4198, <Message> is “The local interface is being disabled.”
- for Event ID 4199, <Message> is “Network operations on this system may be disrupted as a result.”

Potential causes

The assigned Static IP displays 0.0.0.0 (for event ID 4198).

Windows detected a duplicate media access control (MAC) address on the network. The system detected an address conflict for the <IP address> with the system having the <hdw address>. The local interface has been disabled. Both the adapter and the other device are using the hardware address specified. Each device should have a unique address.

Media access control addresses are pre-assigned and permanently burned into the network interface card (NIC). These addresses under normal circumstances are always unique, however, rare errors made during the manufacturing process can cause duplicate media access control addresses to be used and cause this problem. Another source of duplicate media access control addresses can occur if you are assigning locally administered media access control addresses (LAA), in which case you are overriding the burned-in address in favor of the locally assigned media access control address. With some drivers, LAA media access control addresses are possible, usually Token Ring adapter drivers.

Consequence of inaction

Potential loss of view. All network connectivity over TCP/IP to this computer has ceased until the conflict is resolved and the system is restarted.

Corrective actions

To troubleshoot this problem, you have to determine which other computer on the network is using the same media access control address. Several tools that ship with the Microsoft TCP/IP stack can be used to locate the duplicate addressed computer. To isolate the duplicate media access control address, perform the following steps:

The example below uses IP address 129.0.0.1, and hardware address 02:A0:8C:DE:00:FD. For your troubleshooting, use the addresses from the alarm message.

From a working TPC/IP based client:

1 Ping the TCP/IP address found in the event log entry from a command prompt by typing the following:
PING 129.0.0.1

You should get replies back similar to these from the duplicate addressed computer:

```
Pinging 129.0.0.1 with 32 bytes of data
Reply from 129.0.0.1: bytes=32 time=10ms ttl=128
Reply from 129.0.0.1: bytes=32 time=<10ms ttl=128
Reply from 129.0.0.1: bytes=32 time=<10ms ttl=128
Reply from 129.0.0.1: bytes=32 time=<10ms ttl=128
```

2 To verify the computer's media access control address is the duplicate, type the following at a command prompt:
ARP -a 129.0.0.1

You should get a reply back as follows:

```
Internet Address Physical Address
129.0.0.1 02:A0:8C:DE:00:FD <-- matches the event log entry
```

3 We can now use NBTSTAT to get the NetBIOS (friendly) name of the duplicate computer by typing the following at a command prompt:

NBTSTAT -A 129.0.0.1

You should get a reply back with the NetBIOS name of the computer. Use this NetBIOS name to determine who the owner of the computer is so you can locate it on your network.

```
NAME            TYPE        STATUS
-----------------------------------------------
NTSERVER1       <00>        Unique
DOMAN-NAME      <00>        GROUP
NTSERVER1       <03>        Unique

Media access control address = 02-A0-8C-DE-00-FD
```

If you get a message:

HOST NOT FOUND.

This would indicate that the duplicate computer is not a NetBIOS enabled computer, like a Novell server, Unix server, Router, or perhaps a Jet Direct Printer.

4 Once you find the duplicate addressed computer, you can either replace its network card, or if a locally administered media access control address (LAA), change it to be unique on the network.

Change the LAA:

1 In the Windows Control Panel, double-click the Network icon.

2 While displaying the properties of the installed network adapter, change the properties or configuration of the installed Network Adapters LAA to use a unique LAA.

Time to respond

The condition should be addressed immediately.

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) listed in the “Support and other contacts” section of this document.

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.

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 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.

Index