



GE VERNOVA

PROFICY® SOFTWARE & SERVICES

PROFICY iFIX HMI/SCADA

Enhanced Failover

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, GE Vernova assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of GE Vernova. Information contained herein is subject to change without notice.

© 2024 GE Vernova and/or its affiliates. All rights reserved.

Trademark Notices

“GE VERNOVA” is a registered trademark of GE Vernova. The terms “GE” and the GE Monogram are trademarks of the General Electric Company, and are used with permission.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:
doc@ge.com

Table of Contents

Enhanced Failover	1
For New Users of Enhanced Failover:	1
For Existing Users of Enhanced Failover:	1
Terms You Should Know When Working with Enhanced Failover and LAN Redundancy	1
Components of Enhanced Failover	3
Active SCADA	3
Standby SCADA	3
Logical SCADA Name	3
iClient Connections	4
SCADASync.exe	4
SCADARoleMgr.exe	4
SCADASyncMonitor.exe	4
iFIXNotificationFG.exe and iFIXNotificationBG.exe	4
SCADASync.log and ScadaRoleMgr.log Files	5
Network Status Display (NSD) Tag	5
Enhanced Failover Runtime Information (SCADASync) Tags	5
What is Enhanced Failover?	6
What is my SCADA Role?	7
Summary of When Role Changes Occur	7
Introduction to Enhanced Failover	8
Differences Between Enhanced Failover and Failover in Previous iFIX Releases	8
Changes in iFIX 2023	8
Updated Licensing	9
Enhanced Failover and Legacy Client Compatibility	9
More Robust and Efficient Processing	9
Support for Database Synchronization	9
True Standby Node Support	9
Dedicated SCADA-to-SCADA Network for Improved Communications	10
Automatic Switching to Active SCADA	10

New NSD Tag Fields	10
Alarm Acknowledgement Synchronization Change	10
New Enhanced Failover Runtime Information Fields	11
Limitations of Enhanced Failover	11
General Limitations	11
Unsynchronized Items	12
Database Synchronization for Enhanced Failover	13
Synchronized Items	13
Items that Affect Database Synchronization Performance	13
File Synchronization	13
Alarm Management for Enhanced Failover	14
Choosing a Communications Protocol for SCADA Synchronization	14
Understanding Enhanced Failover	16
Security Checks Used with Enhanced Failover	16
Security Area for Enhanced Failover	17
To assign a security area for Enhanced Failover:	17
What Happens when a Failover Occurs?	17
Alarm Handling for SCADA Servers	18
Logical Node Names	18
I/O Drivers and Enhanced Failover	19
Considerations for Using IGS vs. Other Drivers with Enhanced Failover	19
Alarm ODBC Service and Enhanced Failover	21
Considerations When Working with Configuration Hub	22
Using Configuration Hub with iFIX Enhanced Failover	22
Deleting Servers or Groups	22
Notes on Certificate Management	23
Special I/O Addresses	23
Proficy Historian and Enhanced Failover	23
Customizing the Synchronization Process with SCADASync.ini	24
Key Descriptions of SCADASync.ini	25
iFIX Notification and Enhanced Failover	30

Description of the Fields in the Notification Table	31
When iFIX Notification Displays the Message	31
How Notification Works, in More Detail	31
Configuration Examples: Enhanced Failover	32
Recovery Examples: Enhanced Failover Behavior	33
Scenario 1: Primary SCADA Unavailable	34
Scenario 2: Secondary SCADA Unavailable	34
Scenario 3: Both Primary and Secondary SCADA Unavailable	35
Scenario 4: iFIX Network to Primary SCADA from the Client Unavailable	36
Scenario 5: iFIX Network to Secondary SCADA from the Client Unavailable	37
Scenario 6: Dedicated Network Between Primary and Secondary Unavailable	37
Scenario 7: Complete Network Failure	38
Configuring a SCADA Server Pair for Enhanced Failover	39
Configuring Computers for Enhanced Failover	39
Preparation Checklist for Enhanced Failover	40
Checklist for Enhanced Failover Configuration	41
Configuring Computers for Enhanced Failover	42
Preparation Checklist for Enhanced Failover	43
Assigning Physical and Logical Node Names	44
To define your local and logical node names on the primary SCADA:	45
To define your local and logical node names on the secondary SCADA:	45
Enabling Enhanced Failover	45
To enable Redundancy and configure pairs on the primary SCADA:	47
To enable Redundancy and configure pairs on the secondary SCADA:	47
Configuring Data Sync Transports for Enhanced Failover	47
Data Sync Transport Options Dialog Box	51
Steps to Configure the Data Sync Transports	53
To define the data sync transports on the primary SCADA:	53
To define the data sync transports on the secondary SCADA:	53
Configuring iClients	53
How the iClient Works in Run Mode	55

Steps to Configure	55
To add the remote node on the iClient:	56
To configure the logical node name (remote node) on the iClient:	56
Disabling the 1914 Error Message	56
To suppress the 1914 message from appearing on screen:	57
Testing Your Enhanced Failover Configuration	57
To test your nodes:	57
Tips for Enhanced Failover Configurations	58
Synchronize the Clocks on the SCADA Servers	59
Identify Factors Affecting Performance	59
Enhanced Failover and VMWare ESX or ESXi Server	59
Configuring Jumbo Frames when Using VMWare	60
Monitoring Network Status	60
Monitoring Network Status	61
Monitoring Enhanced Failover Status and Initiating Manual Failover to the Standby SCADA	61
Enabling/Disabling Drivers on SCADA Pairs	61
Triggering an Event on Failover	62
Network Status Display Fields	62
What is the NSD Tag?	62
How to View NSD Fields in iFIX	62
Zero-based NSD Fields	63
One-based NSD Fields	63
Field Descriptions	63
Example Uses of Network Status Display Fields	67
SCADA Failover	68
LAN Failover	68
Custom Pictures with Logical and Physical Node Names	68
EDA and Network Status Display (NSD) Fields	69
Troubleshooting Enhanced Failover	69
Troubleshooting Checklist for Enhanced Failover Configuration	72
More Information on Network Card Usage	74

Tips for working with NICs	74
Tools for Troubleshooting	75
Log Files for Enhanced Failover	75
SCADASync.log	76
ScadaRoleMgr.log	76
Command Line Parameters	76
System Messages for Enhanced Failover Activity	77
Error Messages for Enhanced Failover in iFIX	77
Monitoring SAC in Mission Control	81
More Information on Drivers and SAC	83
Enhanced Failover Diagnostics with the SCADA Sync Monitor	84
To open the SCADA Sync Monitor:	86
Toolbar for SCADA Sync Monitor	86
Overview of the SCADA Node Synchronization History	87
Database Synchronization Status	87
Communication Status	88
Debug Log for Troubleshooting	89
Overall System Health	90
Global Memory Synchronization Status	91
Runtime Information Fields for Enhanced Failover	91
What are SCADASync Tags?	92
How to Use and View SCADASync Tags in iFIX	92
SCADASync[0]	92
SCADASync[1]	93
Field Descriptions	93
Field Formats	100
Example Uses of Runtime Information Fields for Enhanced Failover	100
Example 1: Monitor the Status of the Primary Node	101
Example 2: Monitor the Status of the Secondary Node	101
Example 3: Determine the Version of iFIX Running on a Specified Node	101
Example 4: Display the Logical Node	101

Example 5: Display the Primary Node Name	101
Example 6: Display the Secondary Node Name	101
Example 7: Display the Available System Disk	102
Frequently Asked Questions about Enhanced Failover	102
Maintenance Mode	104
Enabling or Disabling Maintenance Mode	105
Maintenance Mode Steps	106
Maintenance Mode from Remote iClients	107
.....	108
Enabling or Disabling Maintenance Mode from a Remote iClient	108
Maintenance Mode Synchronization	109
Alarm Acknowledgement Synchronization	110
Simulation Register Synchronization	110
Database Manager in Maintenance Mode	110
Disabling Maintenance Mode Synchronization	111
To disable alarm acknowledgment synchronization:	111
To disable simulation register synchronization:	111
Simulation Register Synchronization Timeout Parameter	111
Client Operations	113
Viewing Alarms on iClients	113
Reading Data in iFIX Pictures on iClients	113
Network Failure Detection on the iClient	114
Example of the iFIX Notification Window Under Normal Conditions	115
Example of the iFIX Notification Window when a Change Occurs	115
SCADAs with Enhanced Failover Detection on the iClient	115
Index	117

Enhanced Failover

The Enhanced Failover e-book is intended for process control engineers, integrators, and developers responsible for designing and creating operator displays, and configuring the development and run-time environments. The manual assumes familiarity with the process database, the iFIX WorkSpace, and the System Configuration Utility (SCU).

For New Users of Enhanced Failover:

This e-book contains the following sections to help you work with and understand the iFIX Enhanced Failover features:

- [Terms for Working with Enhanced Failover](#)
- [Components of Enhanced Failover](#)
- [What is Enhanced Failover?](#)
- [What is my SCADA Role?](#)
- [Introduction to Enhanced Failover](#)
- [Understanding Enhanced Failover](#)
- [Security Checks Used with Enhanced Failover](#)
- [Configuring a SCADA Server Pair for Enhanced Failover](#)
- [Monitoring Network Status](#)
- [Troubleshooting Enhanced Failover](#)
- [Client Operations](#)
- [Maintenance Mode](#)

For Existing Users of Enhanced Failover:

If you are upgrading from a version of iFIX (before iFIX 5.0) with the previous Failover solution, be sure to refer to the [Differences Between Enhanced Failover and Failover in Previous iFIX Releases](#) section in this e-book and [Enhanced Failover and Upgrading](#) section in the Getting Started with iFIX e-book before you begin configuring or using the Enhanced Failover feature.

A configuration checklist is provided in the [Checklist for Enhanced Failover Configuration](#) section as overview. If you are familiar with iFIX, this should get you started quickly in making your updates.

The only changes between iFIX 5.0 and the current version of iFIX are the addition of the Enhanced Failover Runtime Information (SCADASync) tags, and various server enhancements (that do not require any configuration changes). For more information on the SCADASync tags, refer to the [Runtime Information Fields for Enhanced Failover](#) section.

Terms You Should Know When Working with Enhanced

Failover and LAN Redundancy

Before you begin working with Enhanced Failover in iFIX you should familiarize yourself with the following terms:

Term	Description
Enhanced Failover	The process of switching the active SCADA node from a waiting, standby SCADA node, when the active SCADA node becomes unavailable for processing data.
Active SCADA	The fully functioning SCADA node in run mode. The active node sends the process database to standby node. All iClients retrieve their data and alarms from the active SCADA. The active SCADA generates alarms.
Standby SCADA	The “Idle” SCADA node in run mode. Updates to the standby SCADA are based on database synchronization updates pushed from the active node. The standby node replaces the concept of the backup node in previous versions of iFIX, prior to iFIX 5.0.
Physical Node	The physical node (also called the local node) is the local iFIX node name, and should be unique within your iFIX network.
Logical Node	A logical node is a pair of SCADA nodes configured to use Enhanced Failover. A client using a logical node obtains data from the active SCADA node in the pair.
Primary SCADA	The first node that you configure in your primary and secondary pair in configure mode. This is the node that goes active when you start iFIX, but may not always be the active node.
Secondary SCADA	The second node that you configure in your primary and secondary pair.
Synchronization	<p>A process that occurs on the active SCADA node, where the iFIX process database and all files in the PDB folder changed from the last update are copied to the standby node.</p> <p>The actual process name of the iFIX application that performs the database synchronization is SCADASync.exe. The ScadaRoleMgr.exe works in tandem with the SCADASync.exe, and assigns the roles during failover.</p>
iFIX Client node	<p>Operators view process data received from a SCADA Server using a client (SCADA or iClient node).</p> <p>The client obtains data and alarms from the active SCADA node:</p> <ul style="list-style-type: none">• A client automatically switches over to the newly active SCADA when a failover occurs.• Any VBA script on the client continues to execute when a failover occurs. If the VBA script is reading data while the failover occurs, the VBA script may return an error.• The Alarm Summary shows the same number of alarm and acknowledge states after a failover occurs. The real-time

trend shows some gap in the line chart.

Components of Enhanced Failover

Enhanced Failover is the capability to switch over automatically to a standby SCADA Server when a failure occurs. The switchover from the active to the standby SCADA Server occurs without user interaction, unless it is manually triggered. There are certain components that need to be configured and running to allow this switchover to occur.

The following components are included in the iFIX Enhanced Failover configuration:

- [Active SCADA](#)
- [Standby SCADA](#)
- [Logical SCADA](#)
- [iClient Connections](#)

The running components of iFIX Enhanced Failover system also include:

- [SCADASync.exe Process](#)
- [SCADARoleMgr.exe Process](#)
- [SCADASyncMonitor.exe](#)
- [iFIXNotificationFG.exe and iFIXNotificationBG.exe Applications](#)
- [SCADASync.log and ScadaRoleMgr.log Files](#)
- [Network Status Display \(NSD\) tag](#) (optional)
- [Enhanced Failover Runtime Information \(SCADASync\) tags](#) (optional)

Active SCADA

The Active SCADA scans its database, communicates with the PLCs, and generates alarms. Periodically, it sends its database to the standby SCADA over the dedicated SCADA Synchronization network.

Standby SCADA

The Standby SCADA is ready to take the place of the Active node if the need arises. SAC does not poll the database or generate alarms on this node. Instead, the Standby SCADA receives database and alarm information from the Active node.

Logical SCADA Name

A logical node is a pair of SCADA nodes configured for use with Enhanced Failover. A logical pair consists of a **Primary** and a **Secondary** node. A client uses the logical node name to obtain data from the

Active SCADA node in the pair, and to communicate with the Active SCADA node. Each Enhanced Failover SCADA node (both Primary and Secondary) is defined by a unique physical name and a common logical name.

The SCADA pair consists of a Primary node which is the preferred node in the pair, and a Secondary node which is the backup node in the pair, each having a role/status. When Enhanced Failover is enabled, one node will be Active, and the other node will be in Standby. The Active node functions as a normal SCADA node. SAC is processing the database and alarms are being generated on the Active node. Additionally, the Active SCADA node periodically sends database and alarm information to its partner, the Standby node.

iClient Connections

iClient nodes allow operators to obtain data and alarms from the Active SCADA node. Clients must be connected to the SCADA in “Active” mode to change data, acknowledge alarms, or write data to the PLC.

It is required that you have a dedicated network connection for SCADA synchronization and a separate connection for iFIX Client connections. iFIX Clients follow the Active SCADA. When a failover occurs, the Clients are notified to connect to the new active SCADA. For more information on configuring iClients, refer to the [Configuring iClients](#) sections.

SCADASync.exe

SCADASync.exe is the process name of the iFIX application that performs the synchronization.

For more information on this process, refer to the [What is Enhanced Failover?](#) and [What Happens when a Failover Occurs?](#) sections.

SCADARoleMgr.exe

SCADARoleMgr.exe is a process that decides if the SCADA node will be active or standby.

For more information on this process, refer to the [What is Enhanced Failover?](#) and [What Happens when a Failover Occurs?](#) sections.

SCADASyncMonitor.exe

The SCADA Sync Monitor (SCADASyncMonitor.exe) displays information about the primary and secondary SCADA Servers. You can use it for viewing diagnostic information about your Enhanced Failover configuration, or for troubleshooting issues with your Enhanced Failover configuration. For more information on this application, refer to the [Enhanced Failover Diagnostics with the SCADA Sync Monitor](#) section.

iFIXNotificationFG.exe and iFIXNotificationBG.exe

iFIX Notification (iFIXNotificationFG.exe and iFIXNotificationBG.exe) notifies a user on a Client that it is only able to communicate with a standby SCADA node. You cannot write to a standby SCADA node, and a standby SCADA node does not generate any alarms. Since this limits what the operator can do, a

modal message box appears informing the user about the condition until the active node becomes available again. For more information, refer to the [iFIXNotification.exe and Enhanced Failover](#) section.

SCADASync.log and ScadaRoleMgr.log Files

For Enhanced Failover, there are two additional log files available for troubleshooting. The SCADASync.log includes messages that occur during the SCADA synchronization process. The ScadaRoleMgr.log includes messages that occur during the active to standby node switchover. For more information on these log files, refer to the [Log Files for Enhanced Failover](#) section.

Network Status Display (NSD) Tag

The Network Status Display tag is a special tag residing on each networked node that displays diagnostic, failover, and network information. Networking in the SCU must be enabled to view this tag, which can be added to your custom iFIX pictures. This tag also provides fields for manually triggering failovers: A_SWITCHSCADAROLE and F_SWITCHSCADAROLE. For more information, refer to the [Network Status Display Fields](#) section.

Enhanced Failover Runtime Information (SCADASync) Tags

The SCADASync tags are special tags consisting of runtime information for your Enhanced Failover configuration. Enhanced Failover must be enabled in the SCU to view these tags. The SCADASync tags are very helpful for troubleshooting your Enhanced Failover configuration, and can be added to your custom iFIX pictures. Many of these fields can be viewed from within the SCADA Sync Monitor; however, there are more SCADASync fields than what is displayed in the SCADA Sync Monitor. Use these tags to obtain additional information, for instance, regarding your data synchronization transports. For more information on these tags, refer to the [Runtime Information Fields for Enhanced Failover](#) section.

What is Enhanced Failover?

Enhanced Failover is the ability to define two SCADA nodes to function as one logical node. The logical node provides data and alarms to its clients even if one of the SCADA nodes becomes inoperable. When you start iFIX on both nodes, one SCADA will be your active node, and the other will be your standby node.

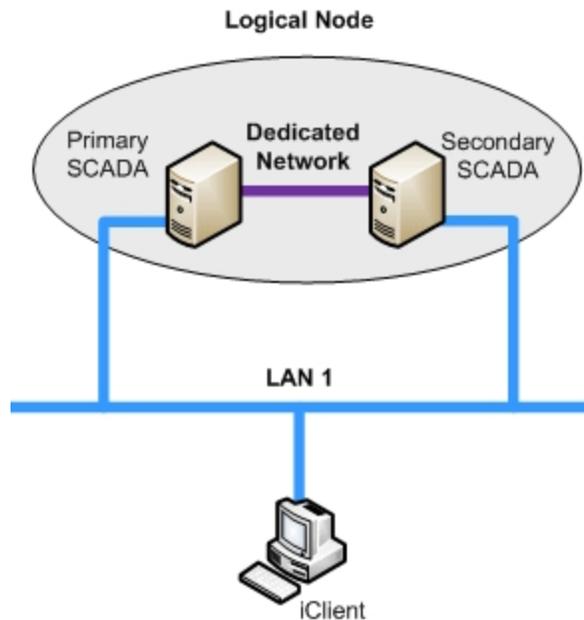
The active node continuously pushes a copy of the memory-based process database (PDB) to the standby node. This process is called synchronization, by which real-time data such as setpoints, the tag database, and alarms are synchronized between the SCADA node pair. The active node synchronizes its process database with the standby node. SCADASync.exe is the iFIX application that performs the synchronization. SCADARoleMgr.exe is the iFIX application that decides if the SCADA node is active or standby.

SCADASync.exe will use any available network connection for the synchronization; however, you should prioritize network usage to separate your real-time iFIX network from the SCADA synchronization network.

IMPORTANT: It is *strongly recommended* that you use a dedicated network connection between the primary and secondary SCADA nodes.

When the SCADA nodes are physically close to each other, a crossover cable can be used. Additionally, it is further recommended that the network components (LAN adapters, hubs, switches, cables, etc.) used for synchronization of the SCADA pair support a minimum 1 Gigabit Ethernet.

The following figure shows an example of an Enhanced Failover configuration that includes two networks: a dedicated network for SCADA synchronization and a second network, LAN 1, which is for iFIX networking.



Simple Enhanced Failover Example: One LAN and One Dedicated Network

Operators view the process data received from a SCADA Server using an iClient. Should the active SCADA Server become unavailable, process data will become unavailable to the operator at the iClient workstation. Enhanced Failover increases the chance that data will continue to be available to the iClient, despite a failure in the active SCADA node component.

Enhanced Failover allows you to connect an iClient to both the primary and secondary SCADA Servers that are connected to the same PLC(s). The iClient establishes and maintains the connections to both the primary and secondary SCADA Servers, either of which can be the active server or the standby server. When the active SCADA Server fails and the standby becomes active, the iClient nodes automatically fail over to the newly active SCADA Server.

You can use Enhanced Failover and LAN Redundancy either individually or together. For more information, see the [Examples of LAN Redundancy Used with Enhanced Failover](#) section.

A standby SCADA will automatically take over the active role from its partner SCADA when any of the following conditions occur on the active SCADA node:

1. SAC stops processing blocks due to an application exception (crash).
2. The computer runs out of disk space.
3. Loss of the synchronization link with the partner SCADA node. In this case, both SCADAs take on the active role.
4. Loss of all iFIX network connections.
5. A user requests that a role change occurs (manual failover).
6. Maintenance Mode is enabled. This case occurs on the primary SCADA node.

What is my SCADA Role?

Each node in an Enhanced Failover SCADA pair has a role: **Active** or **Standby**. In normal operations, one SCADA assumes the Active role, and the other SCADA assumes the Standby role.

If a SCADA node cannot communicate or detects a problem with its partner, it becomes the Active node. If both SCADA nodes are Standby or both nodes are Active, the Primary node becomes Active. When using Maintenance Mode, both SCADAs will be Active.

Roles can also be changed manually by changing values of the NSD (network status display) tag: A_SWITCHSCADAROLE or F_SWITCHSCADAROLE. The NSD tag provides the ability to force a SCADA to a particular role or to display information about the SCADAs or Clients.

Summary of When Role Changes Occur

A SCADA role automatically changes when:

- SAC stops processing blocks due to an application exception (crash).
- The computer runs out of disk space.
- All synchronization links between the two nodes are unavailable.
- A user requests that a change occurs (manual failover).

- iFIX connectivity is unavailable. For instance, this scenario occurs when disconnecting the iFIX networking cable on the SCADA computer. Be aware that a SIM is needed to support this functionality.

NOTE: SCADA roles do not change as a result of bad Driver to PLC communication.

Introduction to Enhanced Failover

When Enhanced Failover is enabled, two SCADA Servers (a primary and secondary) provide increased availability in case of a failure. This section describes how Enhanced Failover works and how to configure it. It includes the following sections:

- [Differences Between Enhanced Failover and Failover in Previous iFIX Releases](#)
- [Limitations of Enhanced Failover](#)
- [Database Synchronization for Enhanced Failover](#)
- [Alarm Management for Enhanced Failover](#)

Differences Between Enhanced Failover and Failover in Previous iFIX Releases

The Enhanced Failover configuration and architecture provided in iFIX 5.0 and greater is different compared to previous iFIX versions. If you are a new customer or a customer upgrading from a previous version of iFIX, be sure to allot some time to understand these changes and implement the new configuration.

Some of the Enhanced Failover features provided in iFIX 5.0 and greater include:

- [Updated Licensing](#)
- [Enhanced Failover and Legacy Client Compatibility](#)
- [More Robust and Efficient Processing](#)
- [Support for Database Synchronization](#)
- [True Standby Node Support](#)
- [Dedicated SCADA-to-SCADA Network for Improved Communications](#)
- [Automatic Switching to Active SCADA](#)
- [New NSD Tag Fields](#)
- [Alarm Acknowledgement Synchronization Change](#)
- [New Enhanced Failover Runtime Information Fields](#)

Changes in iFIX 2023

Some of the changes introduced in iFIX 2023 for Enhanced Failover include:

- If the Primary SCADA fails over to the Secondary due to a shutdown or connection loss, the Secondary will remain active when the Primary comes back online. To make the Primary the active SCADA again, you must execute a manual failover using one of the SWITCHSCADAROLE fields of the Network Status Display (NSD) tag.

Updated Licensing

Enhanced Failover is a keyed option in iFIX 5.0 and greater. New and upgrade customers must ensure this option is enabled on your key before starting iFIX. You can check if this option is enabled through the License Viewer.

Enhanced Failover and Legacy Client Compatibility

An iFIX network that contains iFIX version 5.8 Enhanced Failover SCADA nodes and also contains older iFIX client nodes may not be supported:

- An iFIX client node, installed with iFIX version 5.5 or later, is fully compatible with iFIX version 5.8 Enhanced Failover SCADA nodes.
- An iFIX client node, installed with iFIX version 5.1 and updated with iFIX51_Pulse10_Workspace_019 SIM (Software Improvement Module), is fully compatible with iFIX version 5.8 Enhanced Failover SCADA nodes.
- An iFIX client node, installed with iFIX version 5.1 and is not updated with iFIX51_Pulse10_Workspace_019 SIM is **not** compatible with iFIX version 5.8 Enhanced Failover SCADA nodes.
- An iFIX client node, installed with iFIX version 5.0 or earlier, is **not** compatible with iFIX version 5.8 Enhanced Failover SCADA nodes.

IMPORTANT: In an Enhanced Failover pair, both SCADA nodes must have the same iFIX version installed with all SIMs.

More Robust and Efficient Processing

Enhanced Failover is more robust than in earlier versions before iFIX 5.0. For instance, in previous releases, the two SCADA systems acted independently of one another. Now, the active and standby nodes stay synchronized and the detection of failure occurs more quickly.

Before iFIX 5.0, generated alarms could vary based on differences in timing of the two independent nodes. This process was improved, so that such inaccuracies are minimized.

Support for Database Synchronization

Enhanced Failover includes database synchronization between the active and standby SCADA pair.

If you are upgrading from a previous iFIX release, prior to iFIX 5.0, make sure you read the section of the iFIX Getting Started guide, for a complete list of items that you should evaluate.

True Standby Node Support

In the iFIX releases prior to 5.0, each node in a pair was active all the time. It was left to the customer to create a scheme that simulated an active and a standby node. With Enhanced Failover, the secondary node is a dedicated standby node. As such, the standby node is in an inactive state:

- The SAC database processing task is in standby mode, and no longer processing the database.
- Outputs are not being written to the PLC.
- Interactive or programmatic process database changes are not allowed, as they would be overwritten by the synchronization process.
- The Alarm ODBC client is not writing messages to the relational database.

This means that you can no longer use your standby node (which used to be called a backup node) as your development node, if you did so in the past.

Dedicated SCADA-to-SCADA Network for Improved Communications

Between the active and standby nodes, iFIX now supports (and GE strongly recommends) a dedicated connection between them – a dedicated SCADA-to-SCADA network. This requires that you install new hardware, if you are upgrading from a previous release, as well as that you update your SCU configuration. The use of a dedicated network creates a fast, reliable, efficient connection between the two SCADA nodes for use with synchronization traffic. A dedicated network allows you to eliminate synchronization traffic from your iClient network, eliminate a single point of failure, and improve performance.

Automatic Switching to Active SCADA

All iClient nodes automatically switch to the active SCADA. Connection failover can be manually initiated using the CURACTIVENODE field of the NSD tag, but an iClient is automatically switched back to the active SCADA node.

New NSD Tag Fields

New fields for Network Status Display (NSD) tag are available for use in iFIX pictures and applications. You can only access this tag when TCP/IP networking is enabled. The new Network Status Display (NSD) fields include:

- **A_SCADASTATUS, F_SCADASTATUS** – The status of the SCADA node: ACTIVE (1) or STANDBY (2).
- **A_SWITCHSCADAROLE, F_SWITCHSCADAROLE** – Use this to request a change in state: ACTIVE (1) or STANDBY (2).
- **F_SCADAREDUN** – This field is set to 1 if Enhanced Failover is enabled; it is set to 0 if it is disabled.

For more information on the NSD fields, refer to the [Network Status Display Fields](#) section.

Alarm Acknowledgement Synchronization Change

In the iFIX releases prior to 5.0, the failover feature attempted to keep alarms synchronized using the ALM_SYNC process. Now, with Enhanced Failover, this feature is part of the database synchronization process. ALM_SYNC is therefore obsolete and no longer required to keep alarms synchronized.

New Enhanced Failover Runtime Information Fields

The runtime information fields for Enhanced Failover reside within SCADASync tags (also known as Enhanced Failover tags). These fields are very helpful for troubleshooting your Enhanced Failover configuration. SCADASync tags contain diagnostic and network information pertaining to your Enhanced Failover configurations. These runtime information fields are available in iFIX 5.1 and greater.

For more information on these runtime information fields, refer to the [Runtime Information Fields for Enhanced Failover](#) section.

Limitations of Enhanced Failover

General Limitations

When using Enhanced Failover with iFIX, be aware of the following general limitations:

- If you did not purchase a key that supports Enhanced Failover, you will not be able to use this feature in iFIX. Do not use a standby SCADA Server as a development node. The standby SCADA node must be a dedicated standby node.
- The SCADA pair must be configured identically.
- You cannot make database modifications to the standby node. Data cannot be written to a standby node; you can only read data from the standby node. However, you can use [Maintenance Mode](#) on the primary node to temporarily suspend synchronization between the two SCADA nodes, so that you can make changes to your database while SAC is still running.
- iFIX I/O drivers do not support redundant communication with multiple SCADA nodes. iFIX only supports synchronization of the Simulation (SIM) and Simulation 2 (SM2) I/O drivers. All SIM and SM2 driver information is synchronized between the active and standby nodes.
- I/O drivers (6.x and 7.x versions) reading data between the SCADA pair is not supported. The I/O drivers on the active and standby SCADA nodes run independently of each other (for example, they have separate poll tables). Both SCADAs are reading data from the PLC/RTU network at all times. Therefore, the driver configurations running on both SCADA nodes should be identical.

NOTE: Be aware that if your driver is utilizing [Access Time](#) for its datablock/poll records, on the standby SCADA, these datablock/poll records will time-out.

NOTE: If both SCADAs are communicating to the same PLC, you can reduce the load by disabling a driver or I/O devices under a driver if a SCADA is in Standby mode. For more information, see:

- Disable the IGS Driver on an iFIX Enhanced Failover Standby Scada
- Enable or Disable Datablocks, Devices or Channels in a 7.x Driver Programmatically
- The iFIX OPC data server and the Alarm & Event server running on the SCADA nodes is supported; however, the iFIX OPC servers do not support logical names. OPC clients will not automatically switch to the active node.
- The Proficy Historian collectors should be running on both the active and standby iFIX SCADA nodes and configured in Proficy Historian as redundant collectors. For more information about working with Proficy Historian, refer to the [Proficy Historian and Enhanced Failover](#) section.
- You should not have your Proficy Historian Archiver running on either computer in SCADA pair when using Enhanced Failover or LAN Redundancy.

- If you upgraded from a version of iFIX before iFIX 5.0, and previously used the SCADA Failover feature, you will need to reconfigure some settings in the SCU (the data transport for synchronization) before Enhanced Failover will work. For more information, refer to the [Enhanced Failover and Upgrading](#) section in the iFIX Getting Started guide.
- If you use Terminal Services with iFIX, be aware that a Terminal Server cannot reside on either the primary or secondary iFIX SCADA nodes configured for Enhanced Failover. If the SCADA Server and Terminal Server run on the same machine, that machine becomes a single source of failure.
- The primary and secondary SCADA pair must be the same version (major and minor) of iFIX. For example, if the primary SCADA has iFIX 5.0 installed, the secondary SCADA must have iFIX 5.0 installed. The iClient nodes can be any version of iFIX.
- You can have up to three network cards (a primary, secondary, and tertiary network path) configured for SCADA-to-SCADA communication.
- If you are using UDP, the primary SCADA must have a dedicated network.
- If the iClient cannot access the active node through iFIX networking, but can access the standby SCADA through iFIX networking, the iClient will use the data on the standby node. This will allow the Alarm summary to display the current value, but it won't get any new alarms until it can access the active node.
- Dynamic Connections on the SCADA pair should be disabled for iClients to failover to partner SCADA in a timely fashion.
- If you are using UDP, the primary and secondary SCADA computers must be physically next to each other in the same location/room.

Unsynchronized Items

Enhanced Failover only provides for database and alarm synchronization. The following items are not synchronized between the active and standby node with the Enhanced Failover feature enabled:

- The background scheduler running on both SCADA nodes is not synchronized.
- I/O drivers (other than SM2 and SIM) are not synchronized.
- System Extension Toolkit (STK) modules are not synchronized.
- The alarm printer, file, and history queues are not synchronized.
- The Auto Alarm Manager (AAM) queue is not synchronized.
- Any EDA background programs are not synchronized, unless the program is aware of the redundant SCADA setup.
- iFIX Pictures are not synchronized.
- Background schedules are not synchronized.
- VBA scripting variables.
- The AR (Analog Register) and DR (Digital Register) block values are not synchronized.

NOTE: The AR and DR blocks are not part of SAC processing, and therefore not part of the synchronization of the values between the two databases. The AR and DR blocks on the standby and active nodes reflect the value(s) transmitted by the local driver for the specified I/O address. Be aware

that if the AR and DR blocks are not reading value from the same PLC, it is possible that the active and standby nodes to have different values for the AR and DR blocks in each database.

Database Synchronization for Enhanced Failover

The database synchronization feature automatically copies the memory-resident process database (PDB) from the active SCADA node to the standby node at regular intervals. By default, to ensure that the database on the standby SCADA node is as fresh as possible, database synchronization occurs as fast as possible with very little time between synchronizations. See the [Customizing the Synchronization Process with SCADASync.ini](#) section for more information on how to modify the frequency that database synchronization occurs.

Synchronized Items

iFIX items that are synchronized as part of the database synchronization include the:

- Process Database
- SQL trigger (SQT) tasks
- SIM driver registers
- SIM signal generators and parameters
- SM2 driver registers
- Alarm counters
- Alarm logging to ODBC (relational database)

NOTE: AR and DR blocks are synchronized between nodes, however the data for these blocks resides in the driver's image table. So, during a failover, the available data is supplied by the driver.

Items that Affect Database Synchronization Performance

Items that can affect database synchronization timing include:

- Process database size
- Network speed and non-synchronization traffic
- Speed and bandwidth of hardware components

File Synchronization

In addition to synchronization of the memory-resident parts of iFIX, certain directories and files are monitored for changes. When changes to files are detected, files are copied from the active node to the standby node (never in the other direction). Therefore, any file changes made on the standby will not be synchronized to the active node. If the standby should become active, files will synchronize only if they saved after the node becomes active.

If you never want to synchronize files from the secondary node to the primary node, you can disable file synchronization on the secondary node. For more information, refer to [Customizing the Synchronization Process with SCADASync.ini](#) section.

NOTE: Be aware that if you export a database from the iFIX Database Manager on the standby SCADA or iClient (View) node, the default location will be the PDB directory of the local computer, not the SCADA node that is active.

Alarm Management for Enhanced Failover

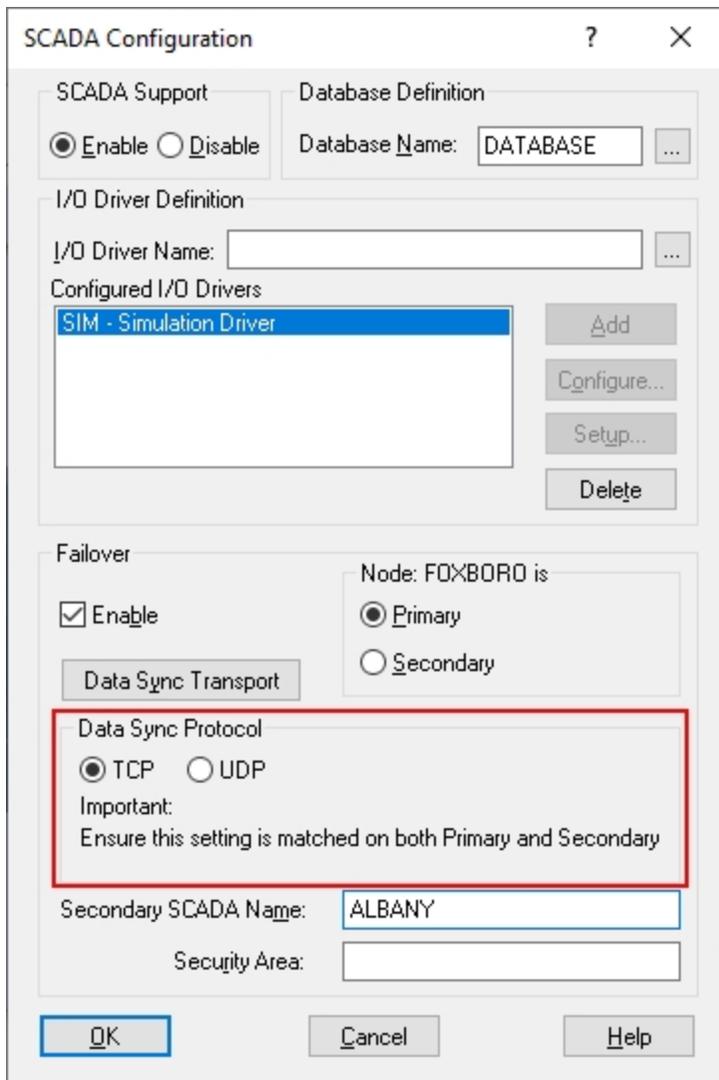
When using the Enhanced Failover feature you should be aware of the following alarm management features:

- The Current Alarm, Alarm Priority, Current Value, Latched Alarm, and Alarm Acknowledgements all reside in the iFIX database. These are included as part of the database synchronization process.
- If you used Alarm Synchronization (Alarm_sync.exe) in an iFIX release prior to 5.0, this feature is replaced by the alarm management and database synchronization available in iFIX 5.1. Alarm_sync.exe is obsolete and should no longer be used.
- With Enhanced Failover enabled, alarms are generated only on the active SCADA node.
- Since the active node is the only one generating the alarms, only its SAC process is generating alarms.
- During the failover process, from active to standby, both the standby and active SCADA will temporarily generate alarms until the failover is complete.
- If the iClient cannot access the active node through iFIX networking, but can access the standby SCADA through iFIX networking, the iClient uses the data on the standby node. This allows the Alarm Summary to update the current value and acknowledgement status, but it does not retrieve any new alarms until it can access the active node.

Choosing a Communications Protocol for SCADA Synchronization

As of iFIX 2023, there is an option to select which protocol to use for SCADA Synchronization communications for Enhanced Failover – TCP or UDP. (In previous versions, only UDP was available.) New iFIX installations will default to TCP, while upgrades or use of an existing, pre-iFIX 2023 SCU file will continue to use UDP by default.

Protocol selection is made in the SCU's SCADA Configuration dialog:



It is important to understand the properties and requirements of each protocol in order to choose the correct one for your Enhanced Failover scenario.

- **UDP** – UDP is a lightweight, fast, efficient, connectionless protocol. Since it does not open or maintain a network connection, it is faster, but less reliable, than TCP. It broadcasts messages on the network with no guarantee that the message will reach the destination. There is no message acknowledgement built into the protocol. It is best used over short distances. Because of this behavior, SCADA Synchronization using UDP requires a more stringent setup/environment to try to maximize the chance of synchronization messages being successfully received at the destination. A dedicated network and network card (NIC) are required, as is enabling Jumbo Frames and using a cross-over cable. **Use UDP if you need the SCADAs in the Failover pair to be as synchronized as possible, and you can provide a dedicated, stable network for SCADA Synchronization.**
- **TCP** – TCP is a reliable, connection-oriented protocol. It establishes a connection to the destination and provides error-checking, acknowledgements and re-transmission of network messages as needed, all of which makes it comparatively slower than UDP. However, these features make TCP a better choice for longer distances or less-reliable networks. **Use TCP if you cannot provide a**

dedicated network, or experience issues getting UDP communications to work and do not require ‘fast as possible’ data synchronization between your SCADA Failover pair.

NOTE: It is highly recommended that SCADA Synchronization traffic be isolated to its own network card (NIC) since sharing a NIC between iFIX networking and SCADA can result in poor performance of client nodes (e.g., running Workspace). Sharing a NIC can also cause longer delays in synchronizing the data between the SCADA Failover pair, resulting in older data in the case of a failover.

NOTE: It is recommended to disable all **Offload** settings for your Enhanced Failover and iFIX networking NIC properties. If using a virtual server, you may have to also do this on the virtual NICs and/or switches.

Understanding Enhanced Failover

When you configure Enhanced Failover, you need to choose one node to be the primary node and the other to be the secondary. When iFIX starts, each SCADA node will start in standby mode, and then after SCADA-to-SCADA communication is established, choose its correct state. If both the primary and secondary nodes can communicate with each other, and they are both in the same state (either active or standby), then the primary will become active and the secondary will become standby.

During startup, if communication cannot be made to the partner node, then the node being started becomes the active node. If you can communicate with the partner node and it's active, nothing happens. However, if the partner node is also in standby mode, the primary node becomes active.

If the secondary node starts more quickly than the primary, it will become the active SCADA node. When the primary starts in this case, it remains on standby until a failure causes it to switch.

When iFIX starts on the iClient, it attempts to establish iFIX networking communication with its primary and secondary SCADA Servers. If both nodes are available, the iClient establishes an iFIX networking connection with both of them but retrieves its data and alarms only from the active SCADA. If only one SCADA Server is available, the iClient establishes a connection with it. If neither SCADA Server is available, the iClient polls both nodes until it establishes a connection with at least one SCADA Server.

If an iClient loses its network connection to the active SCADA, the iClient fails over to the standby SCADA, if available. The client remains connected to the standby SCADA until the active SCADA becomes available to the client again. In this condition, the client displays an iFIX Notification message indicating that the client cannot receive alarms, cannot do writes, and may display data that is out of date. This message box closes within a minute after the iFIX networking connection to the active SCADA is restored. The message box will remain on the screen until the connection to the active node is restored, or until the SCADA nodes switch roles.

Security Checks Used with Enhanced Failover

There are two security features associated with Enhanced Failover:

- Manual Failover application feature
- Enhanced Failover security area

When iFIX security is enabled, the following security checks are performed. Unauthorized users are blocked and violations are logged to the Security Log.

- When enabling or disabling Maintenance Mode using the SCADA Sync Monitor application, the Manual Failover application feature is checked. This feature should be assigned to users or groups who are allowed to manually enable or disable Maintenance Mode using the SCADA Sync Monitor.
- When enabling or disabling Maintenance Mode using the SCADASync tag, the Enhanced Failover security area is checked. This security area should be assigned to users or groups who are allowed to enable or disable Maintenance Mode using the SCADASync tag.
- When switching SCADA roles using the NSD tag, both the Manual Failover application feature and the Enhanced Failover security area are checked. The Manual Failover application feature is checked against the user who is currently logged on the SCADA node that the NSD tag resides on. The Enhanced Failover security area is checked against the user who is currently logged on to the client node that the switch is invoked from. Both security features should be assigned to users or groups who are allowed to manually switch SCADA roles using the NSD tag.

Security Area for Enhanced Failover

If iFIX security is enabled, you are encouraged to use a security area to restrict manual SCADA node role switching to specific users. One security area is supported for Enhanced Failover. This security area can be assigned to authorize users of your Enhanced Failover configurations through the System Configuration Utility (SCU). The Enhanced Failover security area can be set on either or both the primary and secondary nodes; however, it is recommended to use the same security area on **both nodes** in your Enhanced Failover configuration. With the security area configured, you can prevent unauthorized manual SCADA node role changes that are performed locally or remotely. For example, you can prevent specific users from enabling Maintenance Mode.

The Enhanced Failover security area is checked when enabling and disabling Maintenance Mode from the SCADASync tag and when manually switching SCADA roles from the NSD tag.

► To assign a security area for Enhanced Failover:

1. In the SCU of the primary or secondary node, on the Configure drop-down menu, click SCADA. The SCADA Configuration dialog box appears.
2. In the Enhanced Failover Security Area field, enter the security area name.
3. Click OK.

For more information on how to set up security in iFIX, refer to the Configuring Security Features e-book

For more information on the SCADA Configuration dialog box and configuring a node with the SCU, refer to the Setting up the Environment e-book.

What Happens when a Failover Occurs?

When a failure is detected, the active node goes into a standby state, and the standby node goes into an active state. A list of what happens during each change of state is described below.

When the active node goes into a standby state:

- SAC goes into a standby state, blocks stop being processed.
- If enabled, Alarm ODBC pauses from processing messages.
- The SCADA Synchronization process (SCADASync.exe) stops pushing data to the standby SCADA node.
- The active node switches its role (via SCADARoleMgr.exe) to become the standby SCADA node.

When the standby node goes into an active state:

- SAC goes into an active state, block processing begins.
- The standby node switches its role (via SCADARoleMgr.exe) to become the active SCADA node.
- Alarm ODBC begins processing messages.
- The SCADA Synchronization process (SCADASync.exe) begins to synchronize with the standby SCADA.

Alarm Handling for SCADA Servers

When you configure the networking and SCADA options in the SCU for both partner SCADA Servers, the Alarm Startup Queue Service is automatically enabled. This service ensures that alarms are not lost during session loss and reconnection, or during failover.

When an alarm occurs on a SCADA Server, the alarm is sent to all iClients. The iClient accepts alarms from the active node only, regardless of whether it is the primary or secondary SCADA. Alarms are not generated by the standby SCADA.

At the iClient, alarms and messages display the logical node name in brackets. In the following example, the logical node name is LNN.

```
04/29/98 22:49:45.1 [LNN] AI-1 HI 72.00
```

However, if the message is generated by the Database Manager or because of networking problems, node names within the alarm text display the physical node name.

When a node is configured as part of a SCADA Server pair, the Alarm Summary Queue on each SCADA node needs to be twice as big as it would be if the node were not part of a SCADA pair. For example, if you are generating 500 alarms, the Alarm Summary Queue must be set to 1000. If the Alarm Summary Queue overflows, you may see alarms appear and disappear in the alarm summary. Refer to the [Implementing Alarms and Messages](#) manual for more information on queue sizes.

Logical Node Names

When configuring Enhanced Failover, you define a logical node name to represent the physical names of the primary and secondary SCADA nodes. The applications on the iClient should be configured to

communicate with the logical node name. iFIX substitutes the active node name at run time based on which SCADA Server is available. The combination of the logical node name and the physical, primary and secondary SCADA Server names is referred to as the primary and secondary grouping. You configure the primary and secondary grouping in the SCU of the iClient and of each SCADA Server.

The Local Node and Local Logical Names are configured in the Local Startup Definition dialog box of the System Configuration Utility (SCU). The primary and secondary nodes are configured in the Failover area of the SCADA Configuration dialog box in the SCU. For iClients, the primary and secondary groupings are configured in the Remote Nodes area of the Network Configuration dialog box of the SCU.

I/O Drivers and Enhanced Failover

I/O drivers must be configured separately on each SCADA node, when setting up Enhanced Failover.

With Enhanced Failover, only the real time values for the Simulation (SIM) and Simulation 2 (SM2) drivers are synchronized between the active and standby nodes. When the database synchronization occurs, registers update in the SM2 and SIM drivers on the standby node.

NOTE: The SM2 driver increments the retry count if its global section is in use when it tries to poll. Because the SCADA synchronization process updates this section frequently, the SM2 polling task on the standby node often finds the section locked.

I/O driver poll tables (other than SM2 and SIM) are not synchronized. For instance, if you have the MBE driver running on both SCADA nodes, each driver will maintain its own set of values in its I/O poll table for the contents of the PLC values. It is likely that each poll table will have different values for the same registers, depending on the timing of the different polls.

Scan, Alarm, and Control (SAC) does not process blocks on the standby SCADA, so there is a possibility that the I/O driver could stop polling, after the access time expires. This will cause the data in the I/O poll table to be out of date until SAC starts processing the blocks again. You should balance your need for the most recent data after a failure with the extra polling traffic on your PLC network.

NOTE: GE 7x drivers support the use of a Primary Rate and Secondary (poll) Rate. When the Access Time time-out occurs, if configured, polling will occur at the Secondary Rate. This reduces network traffic, yet allows the poll table of the driver to possess fairly recent data from the PLC in the event that the SCADA becomes the active SCADA.

Be aware that you may need to reconfigure your driver polling time and access time in the Power Tool, depending on your needs and the configuration of the driver.

IMPORTANT: Driver configuration changes made on the Primary SCADA will be synchronized to the Secondary only if the configuration file is stored in the PDB folder. If necessary, manually copy the configuration file to the Secondary SCADA. In either case, you must restart the I/O driver on the Secondary SCADA to load the updated configuration. Otherwise, newly added tags will go off-scan if the Secondary SCADA becomes the Active node.

Considerations for Using IGS vs. Other Drivers with Enhanced Failover

When using iFIX with enhanced failover, the data and/or file synchronization does not influence or control the I/O driver operations, which are independent on each node. As a result, the possibility exists that a driver on the active node will be in a different state than a driver on the standby because independent com-

munications are not synchronized as part of iFIX's enhanced failover. The 7x driver architecture is very different than the IGS - so consider the MBE for comparison purposes.

- **Consideration 1:** Alarm acknowledgments are not retained after failover

Using the MBE on both nodes, where all datablocks are set with a primary poll time, no secondary poll time, and access time disabled in the configuration on both nodes. This setup means that the MBE will always poll each datablock at the defined primary rate from each scada node, regardless of active/standby scada node state. We have not seen a system that will show an alarm ack being lost on failover when the MBE is configured to always poll for data on both nodes.

If you configure an access time and no secondary poll rate for the datablocks, this means the MBE would stop actively polling on the standby node with SAC in the warm standby state. In this configuration, you will notice alarm ack's lost on an active to standby failover. This is due to the alarm transitioning from whatever state it was in (i.e., high) to some other state (i.e., no data or comm) when the MBE on the standby node started actively polling based on the SAC warm restart and "waking up" the datablocks (resetting access times) and initiating new polling requests for data.

We have not seen a system that will show an alarm ack being lost on failover when the IGS is configured with the same iFix project startup ini file in place on both nodes AND configuring the IGS to always poll for data. See below for additional information about how to ensure the IGS is configured to constantly poll for data on both scada nodes.

- **Consideration 2:** The MBE can poll devices from both nodes without iFIX running, but the IGS does not

When using the IGS, it doesn't poll for data on startup the same way as the MBE since the IGS doesn't have the same configurable options (primary poll rate/access time/secondary poll rate). The MBE will poll all enabled datablocks when started, regardless of what data is being requested from iFix (SAC). The IGS does not poll for all data on startup, it waits for a client to connect and request certain data (from SAC) at the defined poll rate.

There are two main configuration options to consider when configuring IGS to poll for data with iFix in an Enhanced Failover setup.

1. Configure the IGS project options to never deactivate any iFix PDB tags.

This "deactivate" setting is found in the IGS Server GUI, under File, project properties, iFix PDB settings...the checkbox at the bottom for "iFix PDB Read Inactivity". If this checkbox is NOT selected, the IGS will poll for all items in the PDB (on startup, based on the use of the project startup ini file) on both nodes, regardless of the active/standby state of SAC.

2. Using the iFix project startup ini file on both nodes.

The IGS server maintains a special iFIX configuration file for the default server project that contains all items that will be accessed by the iFIX client (database tags). This configuration file is used to automatically start scanning items before iFIX requests item data. Therefore, data updates that are only requested once (such as AO/DO) will have an initial value when requested iFIX. For information on using this feature for existing iFIX projects, refer to the instructions below.

NOTE: If you have an existing `default_fix.ini` and you are not sure if it contains current tag information, it would be best to delete it with iFIX shut down, and then re-create it to ensure it captures the current (complete) iFIX pdb information as it applies to IGS tags. Also make sure the file contents are identical on both SCADA nodes.

To create a new ini file:

1. Export the PDB database from `databasemanager`.
2. Reload the empty database.
3. Import the exported `.csv` file so that each item in the database will be re-validated with the server.
4. Save the database as type `.pdb`.

This process will generate a new configuration file in the same folder as the default server project file (`default.opf`), containing the name "`default_FIX.ini`".

Depending on how long it takes to read an initial value for all the items in the project, it may be necessary to delay the start of SAC processing. Doing so will allow the server enough time to retrieve all initial updates before the iFIX client requests data from the server.

There is always a chance that the value that caused the original alarm on the primary node could be different when the standby node becomes active, and if very close to an alarm threshold (or change of state for a digital), the alarm could transition to a different state during the time it takes the standby node to become the active node. For example, if the driver on the secondary node had a communication failure, depending on timing/recovery, a tag with a value on the active node could be in a comm alarm state when the standby node transitions to active.

Alarm ODBC Service and Enhanced Failover

The iFIX Alarm ODBC Service writes iFIX alarms and messages to an ODBC-compliant relational database. When using the Alarm ODBC Service, the Enhanced Failover feature provides for synchronization of the alarm logging to the ODBC database (relational database). Only the Alarm ODBC running on the active SCADA will write to SQL. The Alarm ODBC on standby does not write to SQL.

Be aware that when using the Alarm ODBC Service with Enhanced Failover:

- The Alarm ODBC Service does not inform Mission Control if it is running on the active or standby node. If the counter for the logged alarms is incrementing, then the Alarm ODBC Service assumes it is the active node. Use the NSD fields to check if the node is active or standby.
- In the ODBC relational database, knowing whether the active or standby node logged an alarm message is not easily determined if only the logical node name is logged. If you choose to log the physical node name column, however, you can determine which SCADA of the SCADA pair logged them.
- During the process of a failover, there is a small window during which you may get duplicate alarms, if you have a large burst of alarms when the failover is occurring (while both nodes think they are still active). You can look for the most recent failover alarm message to see when the failover occurred.
- When a SCADA node is in standby mode, the Alarm ODBC service does not send alarms to the SQL database. To always send alarms to the SQL database, even in standby mode, you can include a command line parameter in the `fix.ini` file to do so. Add a `/all` to the "`RUN-N=%ALMODBC.EXE`" command in your `FIX.ini` file, like this:

```
[ALARM ODBC]
RUN=%ALMODBC.EXE /all
```

The following figure illustrates some examples of failover alarm messages (shown in a portion of the Alarm History window):

8/8/2008	10:18:03.4	[ALBANY]	SCADASYNC SCADA Sync Communication Lost with
8/8/2008	10:20:15.6	[ALBANY]	SCADASYNC SCADA Sync Communication Lost with
8/8/2008	10:18:08.4	[ALBANY]	SCADASYNC SCADA Sync Communication Lost with
8/8/2008	10:18:08.6	[FOXBORO]	set the SCADA to ACTIVE status
8/8/2008	10:18:08.6		Connection Failover: failover attempted
8/8/2008	10:18:08.6		Connection Failover: connection to RELIC has been switch
8/8/2008	10:18:08.6	[FOXBORO]	SAC is in Active mode
8/8/2008	10:18:08.7	[FOXBORO]	SAC - Warm Restart
8/8/2008	10:18:08.7	[FOXBORO]	SAC - Initialization Complete

Considerations When Working with Configuration Hub

If using Enhanced Failover, you must be in Maintenance Mode to make changes to your Database or Model in Configuration Hub. Maintenance Mode allows you to temporarily suspend synchronization between the two SCADA nodes in an Enhanced Failover pair. This allows you to add or modify groups and tags in your iFIX database while the Scan, Alarm, and Control (SAC) program is running. When you enter Maintenance Mode, SCADA synchronization temporarily stops; synchronization between the SCADA pair is suspended. After Maintenance Mode is enabled, you can make changes to the database on the primary node.

Additionally, all changes to a Failover pair's Database or Model must be made on the Primary node. Changes made to a Failover pair's Database or Model on the Secondary node cannot be published.

Every time you make a change in the configuration and publish, the data is reloaded in the configuration and the driver is restarted. This is important to know if you are making changes on a live system. You will NOT need to restart iFIX after you make any changes in the Configuration Hub. However, after you exit Maintenance Mode, you will need to stop and restart the driver from Mission Control on the secondary in order to pick up the configuration changes.

Using Configuration Hub with iFIX Enhanced Failover

In an Enhanced Failover setup, both the Primary and Secondary Nodes can register and login to Configuration Hub. See iFIX Plugin Registration.

- Once registered, you can login and work with Configuration Hub on the Primary and Secondary Nodes.
- When making changes to the Database or Model you must be in Maintenance Mode, and those changes must be made on the Primary node.
- Changes made while in Maintenance Mode need to be published in Configuration Hub to the iFIX Node.
- Once all changes to the Database or Model have published, disable Maintenance Mode in the Primary Node. This will allow the Primary Node to synchronize changes with the Secondary Node.

Deleting Servers or Groups

Be aware that when the iFIX SCADA Enhanced Failover pair has the OPC UA Driver configured, any server or group delete operation in the Configuration Hub UI on the Primary will not be deleted on Secondary after the maintenance mode synchronization happens. The Secondary SCADA continues to retrieve data since

the server and/or group still exist on the Secondary. As a workaround, manually delete the server and group files from the secondary SCADA, since you cannot run Configuration Hub on the secondary SCADA.

Server and Group configuration files are found in the PDB\iFixUaClient folder, in Servers and Groups folders, respectively. Each server and group has its own file. In each of these folders, compare the contents on the Primary node to those on the Secondary. If a file exists on the Secondary but not on the Primary then open the file in a text editor and verify that it is a server or group that was deleted from the Primary. If so, delete that file from the Secondary.

For all other operations, the synchronization works as expected such as: Server Create, Driver tag deletions or updates, Group updates, and so on.

Notes on Certificate Management

When the iFIX SCADA is part of an Enhanced Failover pair and we have enabled the OPC UA Driver on the SCADA, each physical SCADA needs to establish trust with the configured OPC UA Server separately. After both SCADAs can communicate to a remote OPC UA Server individually using their certificates, you can then bring the iFIX SCADAs up as failover pair. Be sure to confirm that you can communicate individually first.

Special I/O Addresses

There are special I/O addresses in iFIX that are very helpful in a Redundancy Configuration for the OPC UA Client. Using the ConnectionStatus and EndpointUrl addresses, you can see the overall connected status of a (logical) server, and the endpoint it is currently using for data.

Proficy Historian and Enhanced Failover

If you use Proficy Historian in conjunction with Enhanced Failover, your Proficy Historian Archiver should not be installed on either of the SCADA pair; it should be on a remote machine. Historian Collectors should be running on your iFIX SCADA nodes – both the primary and secondary. Your collectors can be configured as redundant collectors, but they do not have to be. To configure redundant collectors, you use the Proficy Historian Administrator. For more details, refer to the "Using the Historian Administrator" electronic book in the Proficy Historian online help.

Be aware of the following when working with Proficy Historian and Enhanced Failover:

- If you want to collect data and alarms from SCADAs in an Enhanced Failover pair, you can do that in the same way as in previous versions of iFIX. To collect data, use an iFIX native collector or use the Historian OPC collector to the iFIX OPC data server. Put one data collector on each SCADA in the pair. Be sure to collect data by logical node name. To collect alarms, put an alarm collector on each SCADA node.
- Proficy Historian collectors currently do not support Windows Vista. So, if you want to use Enhanced Failover and Proficy Historian, do not install iFIX on Windows Vista.
- Tags are added to the default collector selected on the SCADA node from Configure Historian Server(s) dialog box. To access this dialog box, in the iFIX Workspace, in Ribbon view, on the Administration tab, in the Proficy Historian Group, in the Configure Historian list, click Configure Historian Server.

- Only a primary collector can be set as the default collector. Secondary collectors are not available for selection.
- Historical data links are not affected by a SCADA Server failover since they continue to request data from the same Proficy Historian Archiver.
- The Integrated Historian feature for iFIX allows you to add tags only from an active SCADA node.
- With the Integrated Historian feature, iFIX always adds tags as LogicalNodeName.TagName.F_CV except for a text block. For a text block, it is added as LogicalNodeName.TagName.A_CV.

Customizing the Synchronization Process with SCADASync.ini

The SCADASync.ini file controls many aspects of the synchronization process. Some of the items you can customize include how log files are created and the frequency of synchronization. By default, the SCADASync.ini is located in the iFIX LOCAL directory. An example of the SCADASync.ini file appears below:

```
[SyncManager]
; EnableSIMFailureButtons=0
EnablePDBSyncButtons=1
TimeSyncRateMilliseconds=15000
Port=53014
;IMPORTANT: On the Primary SCADA, this value must match the 'Port' setting on the Secondary SCADA
PartnerPort=53014
;WARNING: Changing this setting to disable PDB compression during synchronization can cause
;significant delays and undesirable behavior, especially with larger databases (PDBs).
UsePDBCompression=1
;Retry and Timeout settings for file synchronization messages
FileSendRetries=5
FileSendTimeOut=20000

;MMSync parameters govern synchronization from secondary to primary when Maintenance Mode is exited.
;By default, alarm acknowledgement sync and simulation register sync are enabled and the sync timeout is set to 60 seconds.
;See Electronic Books for more information about these parameters.
;MMSyncAlarmAcks=1
;MMSyncSimRegs=1
;MMSyncTimeout=60

[ScadaRoleMgr]
; default: 0 - to prevent this SCADA from checking client connections.
; Client pulling after failover should now be done by CONMGR. Old default was 60 seconds
ClientConnectionsCheckInterval=0
DelayAutomaticAfterManualSwitch=5

[FileSync0]
FIXDIR=PDBPATH
Inclusion="*.*"
Exclusion="*.TMP;*.EVS;~*.*;*.foo"
IdleTime=5000
Recursive=1

;Settings affecting the ScadaSync.log file
[LogFile]
DeleteOnStartup=1
;Set DebugLevel to 0 to minimize messages logged to file, 255 to write all debug messages in the log file
DebugLevel=0
;Set DailyLog to 1 to generate a log file with a new name each day
DailyLog=0
;Uncommenting this next line will force communication failure messages to be logged to the ScadaSync.log file,
```

;regardless of the DebugLevel setting. It will also override the DeleteOnStartup value to 1/Enabled
;Type=Comm

Key Descriptions of SCADASync.ini

The following table describes the keys available in the SCADASync.ini for customizing the SCADA synchronization process:

Section	Key	Description
[SyncManager]	EnableSIMFailureButtons	<p>Specifies whether you allow a user to simulate a communication failure for the corresponding transport.</p> <p>If the value is 1, buttons are enabled on the SCADA Sync Monitor Transport page and users are allowed to simulate a communication failure for the corresponding transport. A value of 1 is recommended only in a test environment.</p> <p>If the value is 0 (the default), this simulation cannot occur.</p> <p>Valid Entries: 0 or 1. The default value is 0.</p>
	EnablePDBSyncButtons	<p>Specifies whether the Maintenance Mode button is available on the PDB Synchronization Information page of the SCADA Sync Monitor.</p> <p>If the value is 1, the Enable/Disable Maintenance Mode button is available on the primary node.</p> <p>If the value is 0, the Enable/Disable Maintenance Mode button is unavailable.</p> <p>Valid Entries: 0 or 1. The default value is 1.</p>
	FileSendRetries	<p>Specifies how many times a failed file transfer from the Primary to the Secondary will be retried.</p> <p>Valid entries: 0 to 20. The default value is 5.</p>
	FileSendTimeOut	<p>Specifies the amount of time, in milliseconds, that the Primary waits for the Secondary to acknowledge receipt of a file being transferred.</p> <p>Valid entries: 5000 to 60000. The default value is 20000.</p>

MMSyncAlarmAcks

Enables or disables Maintenance Mode alarm acknowledgment synchronization.

Valid Entries:

- 0 = Disable
- 1 = Enable (default)

NOTES:

- Absence of the parameter or setting the parameter to a non-zero value, enables the feature.
- This key is ignored on the secondary node.

MMSyncSimRegs

Enables or disables Maintenance Mode simulation register synchronization.

Valid Entries:

- 0 = Disable
- 1 = Enable (default)

NOTES:

- Absence of the parameter or setting the parameter to a non-zero value, enables the feature.
- This key is ignored on the secondary node.

MMSyncTimeout

Enables, disables, or sets the timeout period for the simulation register synchronization. This key governs how long to wait for the simulation register synchronization to complete.

When disabled, the primary SCADA node waits indefinitely and will not exit Maintenance Mode until simulation register synchronization is completed.

Valid Entries:

- 0 = Disable
- n = 1 to 300 seconds (default=60 seconds)

NOTES:

- Absence of the parameter results in the default value.
- This key is ignored on the sec-

PartnerPort	<p>Secondary node.</p> <p>Specifies the port to connect to on the partner SCADA node for ScadaSync communications (for both UDP and TCP). If a port is not specified in the INI file, the default value of 53014 will be used.</p>
Port	<p>Specifies the port to use on this SCADA node for ScadaSync communications (for both UDP and TCP). If a port is not specified in the INI file, the default value of 53014 will be used.</p> <p>NOTE: If the Port setting on the Secondary SCADA does not match the PartnerPort setting on the Primary SCADA, ScadaSync will not be able to establish communications and synchronization will not occur.</p>
TimeSyncRateMilliseconds	<p>Represents the delay, in milliseconds, between each database synchronization. This setting has a default value of 15000. If your application requires faster updates, modify this setting (removing it will cause synchronization to occur as fast as possible).</p> <p>IMPORTANT: Use extreme caution when modifying this setting. For example, with a RAMP block, if a data change occurs during this delay, your data may not be accurate when the synchronization occurs. Change this setting only if you have knowledge of the types of data your pictures reference.</p>
UsePDBCompression	<p>Specifies if the in-memory PDB image will be zipped before being sent to the Standby partner node.</p> <p>Valid Entries:</p> <p>0 = Disable</p> <p>1 = Enable (default)</p> <p>NOTE: When this setting is enabled, ScadaSync.exe may consume slightly more CPU when it is preparing to send a PDB snapshot to the Standby SCADA.</p> <p>IMPORTANT: It is recommended this</p>

[ScadaRoleMgr] ClientConnectionsCheckInterval	<p>setting be enabled, especially for large PDBs. Disabling this setting can lead to longer PDB synchronization times and delays in role switching.</p> <p>The interval, in seconds, for the active SCADA node to verify that the iClients are pointing to the correct node.</p> <p>The lower you set the time for the interval, the more you increase the network traffic.</p> <p>This parameter should be set to 0 (disabled) on most SCADA nodes. It is only used on SCADA nodes that communicate with older iClients, which require dynamic connections to "pull" clients to the active SCADA node.</p> <p>Valid Entries: 10 – 600. The default value is 0 (disabled).</p>	
DelayAutomaticAfterManualSwitch	<p>The number of seconds that the SCADA Role Manager waits before it makes any active or standby decisions, after a manual switch.</p> <p>Valid Entries: 2 – 60. The default value is 5.</p>	
[FileSync0]	FIXDIR	<p>The iFIX directory that you want synchronized. iFIX 5.1 only supports the PDBPATH directory.</p> <p>Valid Entries: PDBPATH</p>
Inclusion	<p>The list of files or a specified filter (each item in this list is separated by a semicolon (;) mark) to send to the standby node when the file(s) change.</p> <p>Default Value: "*" *</p>	
Exclusion	<p>The list of files or a specified filter (each item in this list is separated by a semicolon (;) mark) to be excluded from the file synchronization. iFIX 5.1 only supports: "*.TMP;*.EVS;~*.*.*.foo"</p> <p>Valid Entries: "*.TMP;*.EVS;~*.*.*.foo"</p>	
IdleTime	<p>The number of milliseconds that a PDB file remains unchanged before it is sent from the active to the standby node after a failover occurs. The default value is 5000 milliseconds (5 seconds).</p>	

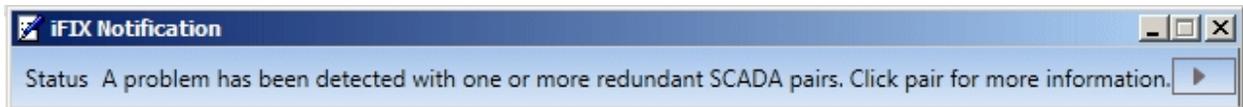
[LogFile]	Recursive	<p>Default Value: 5000</p> <p>Specifies if the synchronization process should monitor sub-directories.</p> <p>If the value is 0, sub-directories not monitored.</p> <p>Valid Entries: 0 or 1. The default value is 1, and should not be changed.</p> <p>NOTE: The sub-directory must exist on both the Primary and Secondary SCADAs for the Recursive setting to function properly.</p>
	DebugLevel	<p>Specifies whether debugging messages, shown in the Debug Log of the SCADA Sync Monitor, are sent to the SCADASync.log file.</p> <ul style="list-style-type: none"> • When the value is 0, no debugging messages are sent to the log file. • When the value is 255, all debugging messages are sent to the log file. <p>Valid Entries: 0 or 255. The default value is 0.</p> <p>NOTE: Use this option carefully as there are many debugging messages. The log file can become very large and fill up the SCADA's hard drive.</p>
	DeleteOnStartup	<p>Specifies whether the log file is deleted on startup or if messages are added to the existing log when iFIX starts.</p> <ul style="list-style-type: none"> • If the value is 1, the existing SCADASync.log is deleted when iFIX starts. • If the value is 0, new messages are appended to the existing SCADASync.log when iFIX starts. <p>Valid Entries: 0 or 1. The default value is 1.</p> <p>NOTE: Use this option carefully as this file can become very large and may fill up the SCADA's hard drive.</p>
	DailyLog	<p>Specifies whether a new log file will be created each day, using the date in the file name.</p>

Type	<p>Valid Entries:</p> <ul style="list-style-type: none"> • 0 = Do not create a new log file each day (default). • 1 = Create a new log file each day. <p>Specifies whether communication failure debug messages should be logged to file, regardless of the DebugLevel setting. It also overrides the DeleteOnStartup setting to '1'/Enabled.</p> <p>Valid Entries:</p> <ul style="list-style-type: none"> • Communication or Comm = Enables described behavior. • No value = Disables described behavior (default).
------	--

iFIX Notification and Enhanced Failover

iFIX Notification (iFIXNotificationFG.exe and iFIXNotificationBG.exe) is a program installed with iFIX that notifies a user through a message window when a failover occurs. iFIX Notification runs in the system tray, for easy and fast access. You can either open the iFIX Notification window from the system tray, or wait for a change in state to occur for it to display automatically.

When a change in failover status occurs, the iFIX Notification window displays a message with information on screen about the status of the change, such as the following example.



If you want more information, click the arrow beside the message. A table appears with a status of all the logical nodes included in your Enhanced Failover configuration. In the following example, there is only one logical node.

Logical Node	Current Connection	Primary Node	Primary Status	Secondary Node	Secondary Status	Status
FOX2	STANDBY	VANILLA	STANDBY	DYNAMITE	STANDBY	BAD

In this example, the user on an iFIX client node is only able to communicate with a standby SCADA node. You cannot write to a standby SCADA node, and a standby SCADA node does not generate any alarms. Since this limits what the operator can do, the iFIX Notification window that appears is modal, remaining on screen – informing the user about the condition until an active SCADA node becomes avail-

able again. For more examples of this window, refer to the [Network Failure Detection on the iClient](#) section.

Be aware that the iFIX Notification applications (iFIXNotificationFG.exe and iFIXNotificationBG.exe) are added to the list of iFIX startup commands in FIX.INI when you install iFIX. If you do not use Enhanced Failover, you can safely delete these iFIX Notification programs from the FIX.INI file.

Description of the Fields in the Notification Table

The following table describes the fields that appear in the iFIX Notification details window.

Column	Description
Logical Node	The logical node name represents the pair of SCADA nodes configured to use Enhanced Failover. A client using a logical node obtains data from the active SCADA node in the pair.
Current Connection	The status of the SCADA node the client is currently connected to: Active or Standby.
Primary Node	The physical node name of the primary SCADA node.
Primary Status	The status of the primary SCADA node: Active or Standby.
Secondary Node	The physical node name of the SCADA secondary node.
Secondary Status	The status of the secondary SCADA node: Active or Standby.
Status	The status of the network: Good, Bad, or Unknown (disabled).

When iFIX Notification Displays the Message

When a client loses its iFIX networking connection to the active SCADA, iFIX fails over to the standby SCADA, if available. The client remains connected to the standby SCADA until the active SCADA becomes available to the client again. While in this condition, the client displays an iFIX Notification window indicating that the client cannot receive alarms, cannot do writes, and may display data that is out of date. This window closes within a minute after the iFIX networking connection to the active SCADA is restored. For more examples of this window, refer to the [Network Failure Detection on the iClient](#) section. If it is not possible to restore the connection for some period of time, you can manually fail the active server so that the standby becomes active. The iFIX Notification feature then clears the message.

How Notification Works, in More Detail

iFIX Notification runs as two programs: iFIXNotificationFG.exe (for the foreground) and iFIXNotificationBG.exe (for the background). The iFIXNotificationBG.exe program runs in the background gathering information about the SCADA nodes. iFIXNotificationBG.exe notifies the foreground program, iFIXNotificationFG.exe, when changes occur in the failover status. The foreground program displays the iFIX Notification window when the change occurs so that a user can see the issue and take immediate action, if required. If any Workspace popups display that require immediate action, such as those for

acknowledging alarms or for information on communication losses, the iFIX Notification window will be pushed behind them. The foreground client does this by readjusting the Z ordering of the iFIX Notification window, allowing the iFIX Notification window not to block any Workspace pop-ups.

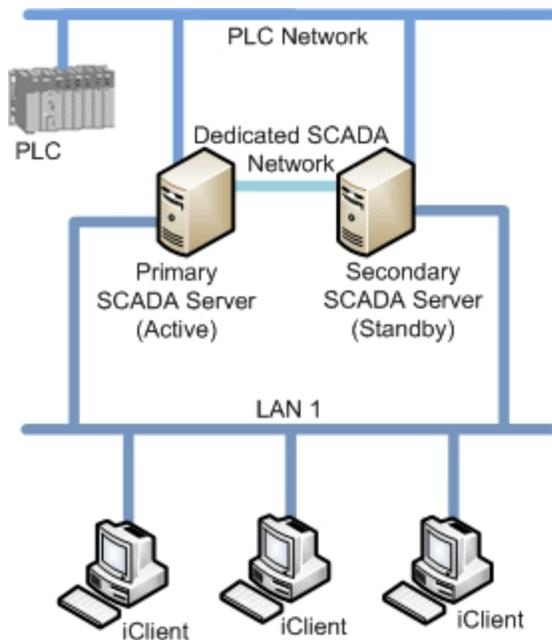
iFIX Notification (iFIXNotificationFG.exe and iFIXNotificationBG.exe) will run when iFIX runs as a service. Be aware, however, of the following cases where you may need to manually start it:

- If you use a Remote Desktop Connection to start iFIX as a service from a remote machine.
- If you select the "Start at Boot Time" option in the SCU's Local Startup Definition (Configure > Local Startup) and restart the computer remotely.

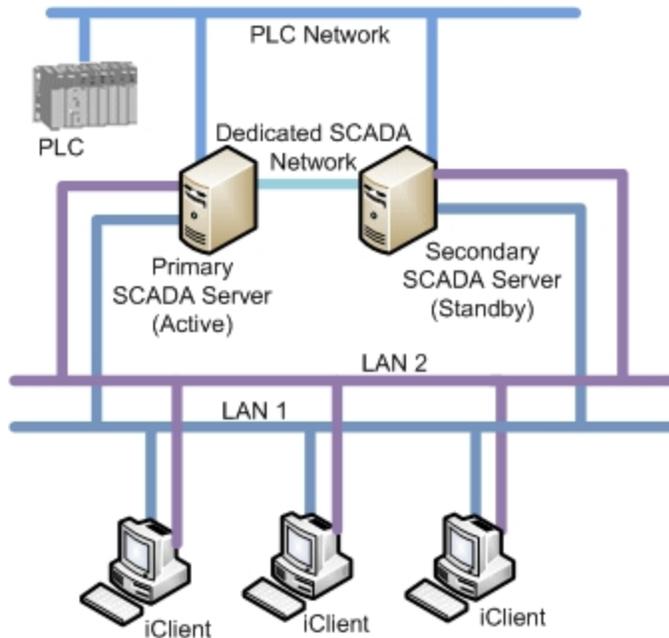
In both cases, the iFIX Notification Foreground program, iFIXNotificationFG.exe, does not start automatically, and subsequently the iFIX Notification window does not launch. To manually start it in this instance, double-click the iFIXNotificationFG.exe in the iFIX folder.

Configuration Examples: Enhanced Failover

The following figure illustrates an Enhanced Failover configuration. It includes two SCADA Server partners – a primary and secondary node. There is a dedicated network for SCADA-to-SCADA communication, another network for SCADA-to-iClient communication, and another network for PLC communication only. In this example there are three iClients accessing the currently active node, and one PLC on the network.



The following figure illustrates the same configuration, with an additional LAN (illustrated in purple) for redundant LAN support.



NOTE: Although a dedicated network is not necessary when using the TCP protocol, it is the recommended configuration. The lack of a dedicated SCADA network can negatively impact picture performance on client machines and database synchronization.

Recovery Examples: Enhanced Failover Behavior

The following scenarios, illustrated in more detail below, describe failure situations that can occur:

- Primary SCADA Unavailable
- Secondary SCADA Unavailable
- Both Primary and Secondary SCADA Unavailable
- iFIX Network to Primary SCADA from the Client Unavailable
- iFIX Network to Secondary SCADA from the Client Unavailable
- Dedicated Network Between Primary and Secondary Unavailable
- Complete Network Failure

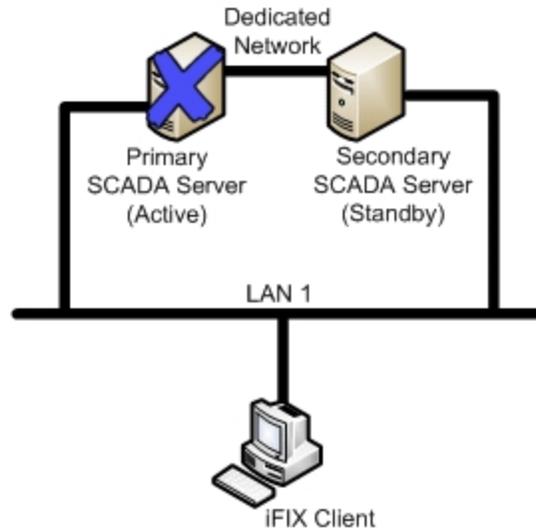
The following example shows one Local Area Network (LAN) for iFIX networking and one dedicated LAN between the SCADA failover pair as the Primary network for data and alarm synchronization. Also in use is the iFIX network, as the Secondary network, for data and alarm synchronization.

The sections that follow describe the recovery state of the primary SCADA, secondary SCADA, and iClient should one of these scenarios occur.

NOTE: Although TCP does not require the dedicated network indicated in the diagrams below, the behavior illustrated in the examples would be expected if one were used.

Scenario 1: Primary SCADA Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and a single failure point.

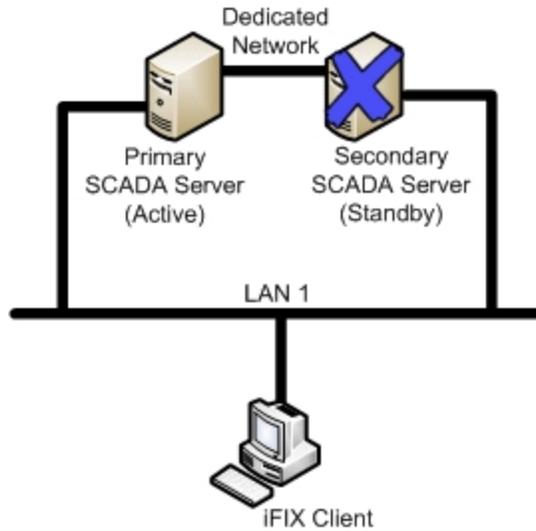


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Unavailable.
Secondary SCADA Server	Switches to Active. No Synchronization.
iFIX Client	The iFIX Client detects loss of communication to primary node and switches to newly active node. The iFIX Client generates a system message that communication was lost to the primary SCADA node. The Client obtains data and alarms from secondary SCADA.

Scenario 2: Secondary SCADA Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and another single failure point.

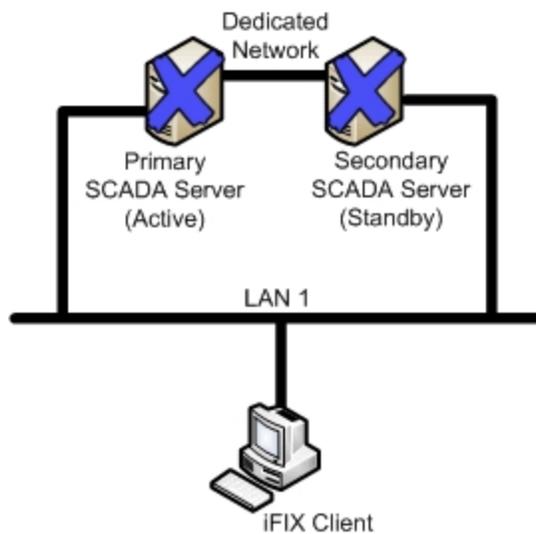


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Active. No Synchronization.
Secondary SCADA Server	Unavailable.
iFIX Client	The iFIX Client detects loss of communication to secondary node. The iFIX Client generates a system message that communication was lost to the secondary SCADA node. The Client continues to obtain data and alarms from Primary SCADA.

Scenario 3: Both Primary and Secondary SCADA Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and two failure points.

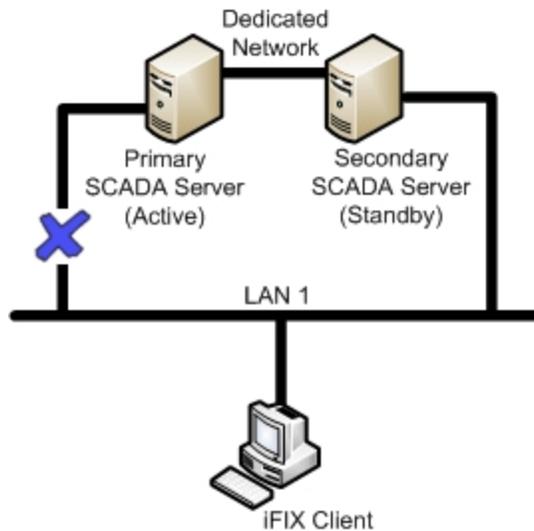


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Unavailable.
Secondary SCADA Server	Unavailable.
iFIX Client	The iFIX Client generates a system message that communication was lost to both the primary and secondary SCADA nodes. The iFIX Client fails to obtain data and alarms.

Scenario 4: iFIX Network to Primary SCADA from the Client Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and a single failure point.

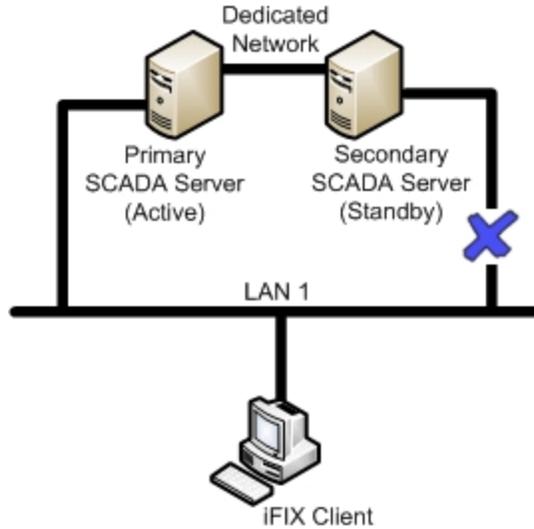


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Active. Synchronization occurs over dedicated network.
Secondary SCADA Server	Standby. Since active and standby nodes are communicating over the dedicated network, they never switch.
iFIX Client	The iFIX Client generates a system message that communication was lost to the primary SCADA node. The iFIX Client switches to the standby SCADA and fails to obtain up-to-date data directly from the active SCADA. The iClient reads data from the standby SCADA but will not get new alarms. The iFIX Notification application displays a message in this situation. Writes from the iClient node are not allowed.

Scenario 5: iFIX Network to Secondary SCADA from the Client Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and a single failure point.

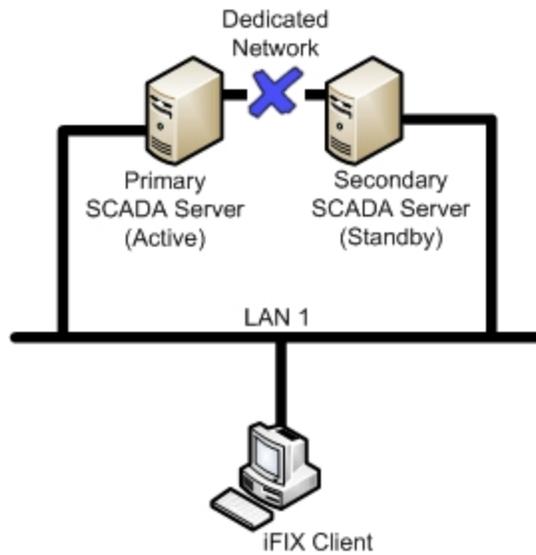


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Active. Synchronization occurs over dedicated network, if configured.
Secondary SCADA Server	Standby.
iFIX Client	The iFIX Client generates a system message that communication was lost to the secondary SCADA node. The Client continues to obtain data and alarms from the primary SCADA.

Scenario 6: Dedicated Network Between Primary and Secondary Unavailable

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and a single failure point.

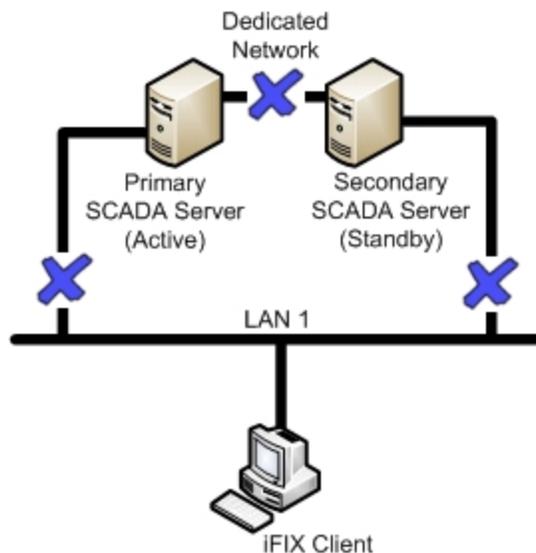


The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Active. Synchronization occurs over LAN1.
Secondary SCADA Server	Standby.
iFIX Client	The iFIX Client obtains data and alarms from the primary SCADA.

Scenario 7: Complete Network Failure

The following example illustrates a single local area network (LAN), with a dedicated network for SCADA synchronization, and multiple failure points.



The following table describes the items in the previous figure.

Item	State
Primary SCADA Server	Active. No Synchronization.
Secondary SCADA Server	Active. No Synchronization.
iFIX Client	The iFIX Client generates a system message that communication was lost to both the primary and secondary SCADA nodes. The iFIX Client fails to obtain data and alarms.

Configuring a SCADA Server Pair for Enhanced Failover

This section provides detailed information on configuring Enhanced Failover. It includes the following sections:

- [Checklist for Enhanced Failover Configuration](#)
- [Configure Computers for Enhanced Failover](#)
- [Assigning Physical and Logical Node Names](#)
- [Enabling Enhanced Failover](#)
- [Configuring Data Transport for Options for Enhanced Failover](#)
- [Configuring iClients](#)
- [Disabling the 1914 Error Message](#)
- [Testing Your Enhanced Failover Configuration](#)
- [Tips for Enhanced Failover Configurations](#)

NOTE: After you perform all the required steps for configuration in the System Configuration Utility (SCU), you will need to save the changes. Restart iFIX on each computer to apply the changed settings.

Configuring Computers for Enhanced Failover

Confirm that your primary and secondary computers meet the minimum hardware requirements for the Enhanced Failover feature. For a list of supported hardware, refer to the section of the iFIX Getting Started guide, or the IPI.

For Enhanced Failover, Gigabit-Ethernet cards (or better) are required for Data Sync Transport communication. When using UDP, a dedicated card is required for Data Sync Transport communication. When using TCP, one card can be used for both iFIX and Data Sync Transport communication, although two are strongly recommended to avoid slower updates of data and alarms on clients.

Use the following checklist to confirm that your primary and secondary computers are configured properly before continuing with the rest of the Enhanced Failover configuration. Validate that the SCADAs, I/O drivers, and iClients function independently before continuing with the Enhanced Failover configuration.

The next set of configuration steps describe how to enable Enhanced Failover and defines partner nodes, so that the SCU configuration on both the primary and secondary nodes is also the same.

Preparation Checklist for Enhanced Failover

When you configure the primary and secondary computers for Enhanced Failover, both SCADA computers should be configured the same way. Each computer should have:

- A License key with the Enhanced Failover option enabled.
 - If you are using UDP, one additional Gigabit-Ethernet card (or better) dedicated for SCADA-to-SCADA traffic (for a total of two network cards). The dedicated SCADA-to-SCADA network card should be excluded from the iFIX-to-iFIX network (i.e., not enabled for LAN redundancy) and used exclusively for Enhanced Failover synchronization. Both network cards must be of the same speed, and appear on the compatibility list for each card. It is strongly recommended that the cards be of the same make and model number, and use the same drivers.
 - As noted above, the use of two NICs is strongly recommended, although not required, for TCP.
 - If using an ESXi Server, or any other virtual machine, each SCADA should have the same type of virtual NIC and virtual NIC driver.
 - Both network cards should be installed and configured properly on both SCADAs. The wake-up upon receiving a socket or/and request feature must be disabled on the dedicated SCADA-to-SCADA network card. SpeedStep® technology is not supported and must not be enabled. Due to limited bandwidth and latency, it is strongly advised that you do not use wireless networking technology in your networking solution. It is also recommended to disable all Offload settings for your Enhanced Failover and iFIX networking NIC properties. If using a virtual server, you may also have to do this on the virtual NIC's and/or switches.
 - Each network card (NIC) should have a name. For instance, you can use iFIX, SCADA Sync, a company network name, and so on. Did you record the IP address? The NIC slot/order or IP address could be affected. It is desirable that both machines have the same NIC cards and NIC order (slot). The power save settings on your computers and dedicated network card (NIC) must be disabled. Do not use any power setting features that affect CPU clock speed.
 - All network cables and connections should be correct. If you are using UDP, you must use a direct connection via a Cat6 crossover cable, without going through any switches, hubs, or routers.
 - If you are using UDP, Jumbo Frames technology must be used on the dedicated network for Enhanced Failover. Jumbo Frames technology allows for an Ethernet frame of 9000 MTU for the payload, compared to a frame of 1500 bytes without the Jumbo Frames.
 - Additional hardware requirements should be met. Please refer to the Systems Requirements tab in the IPI.
 - The same version of the Windows operating system running.
 - The same major and minor version of iFIX with the same SIMs installed, if any, on both the primary and secondary nodes.
- IMPORTANT:** If Proficy Historian is integrated with iFIX, be sure to additionally review the [Historian and Enhanced Failover](#) section.
- The same iFIX security configuration in the Enhanced Failover pair, plus all View/iClient nodes connecting to the SCADA Server. In order to automatically fail over, you need to have either

security enabled on all nodes, or security disabled on all nodes. Discrepancies in security configuration levels may result in an inability to automatically fail over.

- The same I/O drivers with the same configuration, including polling times. Confirm the I/O drivers are listed in the same order in both SCUs, on both SCADAs.
- The same Database (.PDB) files on both the primary and secondary nodes. Both Primary and Secondary SCADAs should be shut down when you copy the iFIX PDB and Driver files from the Primary SCADA to the Secondary SCADA.
- The same Database Dynamos (loadable blocks) installed. Be sure that the slot numbers for Database Dynamos are also identical. For more information on slot numbers, refer to the steps in the [Understanding Slot Numbers](#) section in the Building a SCADA System e-book.

NOTE: Database Dynamo mismatches cause the synchronization process to fail, and may prevent your standby computer from becoming active.

- Connections to the same PLC(s).
- The same system time.
- Identical iFIX system configuration for any of the following items, if used:
 - User and application features, if security is enabled in iFIX
 - PIC directory (optional)
 - .INI files, including the Scadasync.ini, network.ini, and filtererrors.ini (optional)
 - Background Scheduler
 - System Extension Toolkit (STK) modules
 - Integration Toolkit or Productivity Pack
 - Alarm Services
 - Alarm printer, file, history queues, and areas
 - Auto Alarm Manager (AAM)
 - Proficy Historian Collectors
 - iFIX security settings

NOTE: The Alarm Areas (AAD) need to be defined on the local node and then synchronized with the partner node. Even though the LogicalName may point to the local node, in the AAD it could be pointing to the partner node. With the desired .PDB loaded on the active SCADA, copy the AlarmAreas.AAD file from the PDB folder on the active SCADA to the PDB folder on the standby SCADA. File Synchronization will, by default, copy the .AAD file. You should now be able to view Alarm Areas correctly on either SCADA node.

Checklist for Enhanced Failover Configuration

To ensure that you configured the Enhanced Failover feature properly, use the following checklist. This checklist lists each task in the configuration process, and whether it applies to the primary node, secondary node, and/or iClient.

Task	Primary SCADA	Secondary SCADA	iClient(s)	For more information see...
Confirm that each computer's hardware is setup cor-	✓	✓	✓	Hardware Requirements section of

rectly and meets the minimum requirements.				the iFIX Getting Started guide
Validate that all iFIX systems run properly, making sure that the SCADA Servers, I/O drivers, and Clients function independently before even starting to configure Enhanced Failover.	✓	✓	✓	Configure Computers for Enhanced Failover
Define the local and logical names in the SCU.	✓	✓		Assigning Physical and Logical Node Names
Enable Enhanced Failover and configure your primary and secondary pair in the SCU.	✓	✓		Enabling Enhanced Failover
Enable at least one LAN adapter for data synchronization and configure IP addresses in the Data Transport Options dialog box in the SCU.	✓	✓		Configuring Data Transport for Options for Enhanced Failover
Add the logical node name of the SCADA pair in the remote node list on the iClient.			✓	Configuring iClients
In the remote node list of iClient, enable the logical node name and define the Primary Node and Secondary Node.			✓	Configuring iClients
Disable the 1914 error message.	✓	✓	✓	Disabling the 1914 Error Message
Validate your Enhanced Failover configuration.	✓	✓	✓	Testing Your Enhanced Failover Configuration

Configuring Computers for Enhanced Failover

Confirm that your primary and secondary computers meet the minimum hardware requirements for the Enhanced Failover feature. For a list of supported hardware, refer to the section of the iFIX Getting Started guide, or the IPI.

For Enhanced Failover, Gigabit-Ethernet cards (or better) are required for Data Sync Transport communication. When using UDP, a dedicated card is required for Data Sync Transport communication. When using TCP, one card can be used for both iFIX and Data Sync Transport communication, although two are strongly recommended to avoid slower updates of data and alarms on clients.

Use the following checklist to confirm that your primary and secondary computers are configured properly before continuing with the rest of the Enhanced Failover configuration. Validate that the SCADAs, I/O drivers, and iClients function independently before continuing with the Enhanced Failover configuration.

The next set of configuration steps describe how to enable Enhanced Failover and defines partner nodes, so that the SCU configuration on both the primary and secondary nodes is also the same.

Preparation Checklist for Enhanced Failover

When you configure the primary and secondary computers for Enhanced Failover, both SCADA computers should be configured the same way. Each computer should have:

- A License key with the Enhanced Failover option enabled.
- If you are using UDP, one additional Gigabit-Ethernet card (or better) dedicated for SCADA-to-SCADA traffic (for a total of two network cards). The dedicated SCADA-to-SCADA network card should be excluded from the iFIX-to-iFIX network (i.e., not enabled for LAN redundancy) and used exclusively for Enhanced Failover synchronization. Both network cards must be of the same speed, and appear on the compatibility list for each card. It is strongly recommended that the cards be of the same make and model number, and use the same drivers.
- As noted above, the use of two NICs is strongly recommended, although not required, for TCP.
- If using an ESXi Server, or any other virtual machine, each SCADA should have the same type of virtual NIC and virtual NIC driver.
- Both network cards should be installed and configured properly on both SCADAs. The wake-up upon receiving a socket or/and request feature must be disabled on the dedicated SCADA-to-SCADA network card. SpeedStep® technology is not supported and must not be enabled. Due to limited bandwidth and latency, it is strongly advised that you do not use wireless networking technology in your networking solution. It is also recommended to disable all Offload settings for your Enhanced Failover and iFIX networking NIC properties. If using a virtual server, you may also have to do this on the virtual NIC's and/or switches.
- Each network card (NIC) should have a name. For instance, you can use iFIX, SCADA Sync, a company network name, and so on. Did you record the IP address? The NIC slot/order or IP address could be affected. It is desirable that both machines have the same NIC cards and NIC order (slot). The power save settings on your computers and dedicated network card (NIC) must be disabled. Do not use any power setting features that affect CPU clock speed.
- All network cables and connections should be correct. If you are using UDP, you must use a direct connection via a Cat6 crossover cable, without going through any switches, hubs, or routers.
- If you are using UDP, Jumbo Frames technology must be used on the dedicated network for Enhanced Failover. Jumbo Frames technology allows for an Ethernet frame of 9000 MTU for the payload, compared to a frame of 1500 bytes without the Jumbo Frames.
- Additional hardware requirements should be met. Please refer to the Systems Requirements tab in the IPI.
- The same version of the Windows operating system running.
- The same major and minor version of iFIX with the same SIMs installed, if any, on both the primary and secondary nodes.

IMPORTANT: If Proficy Historian is integrated with iFIX, be sure to additionally review the [Historian and Enhanced Failover](#) section.

- The same iFIX security configuration in the Enhanced Failover pair, plus all View/iClient nodes connecting to the SCADA Server. In order to automatically fail over, you need to have either security enabled on all nodes, or security disabled on all nodes. Discrepancies in security configuration levels may result in an inability to automatically fail over.
- The same I/O drivers with the same configuration, including polling times. Confirm the I/O drivers are listed in the same order in both SCUs, on both SCADAs.
- The same Database (.PDB) files on both the primary and secondary nodes. Both Primary and Secondary SCADAs should be shut down when you copy the iFIX PDB and Driver files from the Primary SCADA to the Secondary SCADA.
- The same Database Dynamos (loadable blocks) installed. Be sure that the slot numbers for Database Dynamos are also identical. For more information on slot numbers, refer to the steps in the [Understanding Slot Numbers](#) section in the Building a SCADA System e-book.

NOTE: Database Dynamo mismatches cause the synchronization process to fail, and may prevent your standby computer from becoming active.

- Connections to the same PLC(s).
- The same system time.
- Identical iFIX system configuration for any of the following items, if used:
 - User and application features, if security is enabled in iFIX
 - PIC directory (optional)
 - .INI files, including the Scadasync.ini, network.ini, and filtererrors.ini (optional)
 - Background Scheduler
 - System Extension Toolkit (STK) modules
 - Integration Toolkit or Productivity Pack
 - Alarm Services
 - Alarm printer, file, history queues, and areas
 - Auto Alarm Manager (AAM)
 - Proficy Historian Collectors
 - iFIX security settings

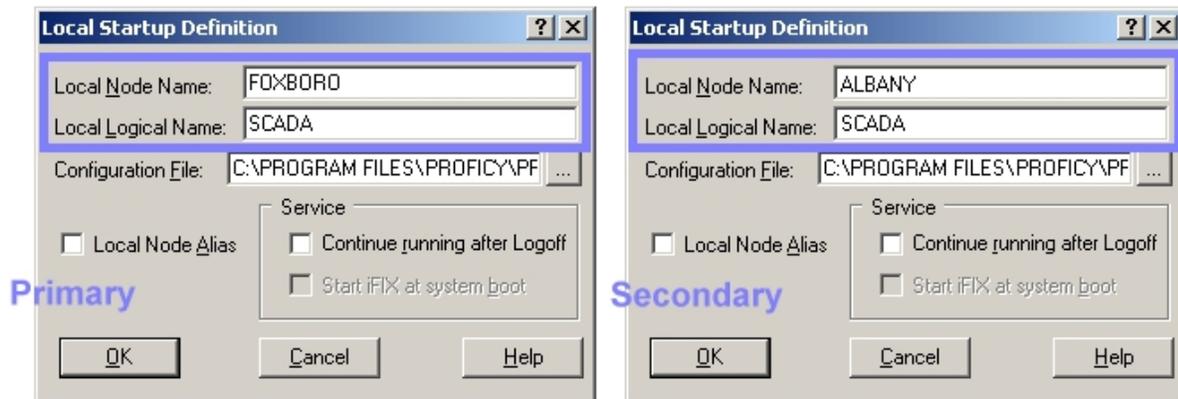
NOTE: The Alarm Areas (AAD) need to be defined on the local node and then synchronized with the partner node. Even though the LogicalName may point to the local node, in the AAD it could be pointing to the partner node. With the desired .PDB loaded on the active SCADA, copy the AlarmAreas.AAD file from the PDB folder on the active SCADA to the PDB folder on the standby SCADA. File Synchronization will, by default, copy the .AAD file. You should now be able to view Alarm Areas correctly on either SCADA node.

Assigning Physical and Logical Node Names

The *physical nodename* is the local iFIX node name, and should be unique within your iFIX network. The *logical node name* is a name that represents the Enhanced Failover SCADA pair (that is, the name will

be the same on both SCADAs). Both the physical and logical node names must be defined on the primary and standby SCADA nodes.

Use the Local Startup Definition dialog box in the System Configuration Utility (SCU) to define the physical (local) and logical node names. In the SCU, you define the local node name and logical node name in the Local Startup Definition dialog box. The following figure shows an example of the Local Startup Definition dialog box for a primary node named FOXBORO, and a secondary node named ALBANY. Both areas are highlighted in the following figure. The logical node name for both is SCADA.



Primary and Secondary Node, Local Startup Definition Dialog Box

► **To define your local and logical node names on the primary SCADA:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.
3. In the Local Node Name field, enter the unique primary node name.
4. In the Local Logical Name field, enter the common logical node name.
5. Click OK.

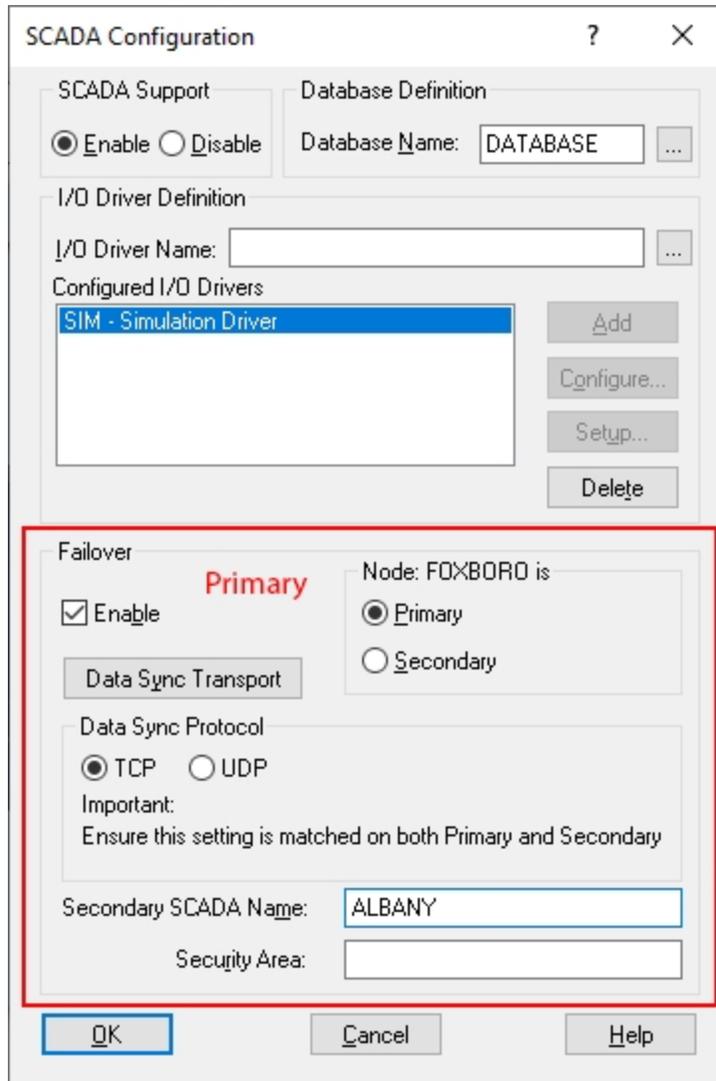
► **To define your local and logical node names on the secondary SCADA:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click Local Startup. The Local Startup Definition dialog box appears.
3. In the Local Node Name field, enter the unique primary node name.
4. In the Local Logical Name field, enter the common logical node name.
5. Click OK.

Enabling Enhanced Failover

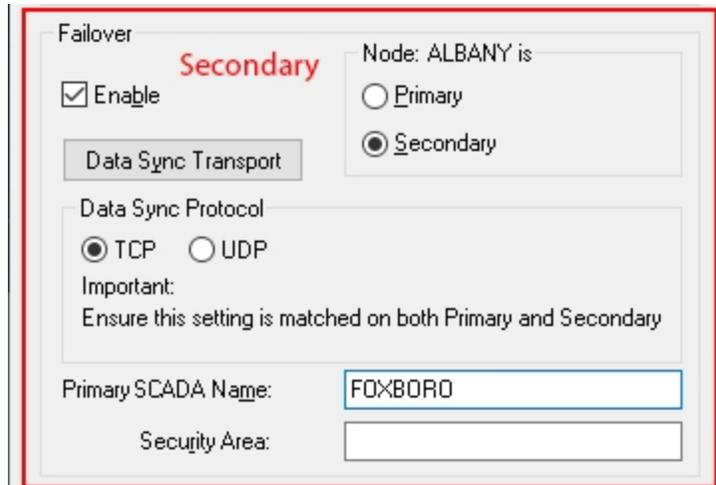
To use the Enhanced Failover feature, you must enable it and define the SCADA pair. Use the SCADA Configuration dialog box in the System Configuration Utility (SCU) to enable redundancy and define the partner nodes (primary and secondary pairing). These steps must be performed on both the primary and secondary nodes.

Use the SCADA Configuration dialog box to configure these items. The following figure shows an example of the SCADA Configuration dialog box for a primary node named FOXBORO, where a secondary node named ALBANY is defined. The Failover area of the dialog box is highlighted in the following figure.



Primary Node, SCADA Configuration Dialog Box

The next figure shows the portion of the SCADA Configuration dialog box that you edit for a secondary node named ALBANY. The primary SCADA node name FOXBORO is defined.



Secondary Node, Portion of SCADA Configuration Dialog Box Requiring Edits

► **To enable Redundancy and configure pairs on the primary SCADA:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click SCADA. The SCADA Configuration dialog box appears.
3. In the Failover area, select the Enable check box.
4. In the Node area, select the Primary option.
5. In the Secondary SCADA Name field, enter the name of your secondary SCADA node.
6. In the Data Sync Protocol area, select TCP or UDP.
7. Click OK.

► **To enable Redundancy and configure pairs on the secondary SCADA:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click SCADA. The SCADA Configuration dialog box appears.
3. In the Failover area, select the Enable check box.
4. In the Node area, select the Secondary option.
5. In the Primary SCADA Name field, enter the name of your primary SCADA node.
6. In the Data Sync Protocol area, select the same protocol you chose for the primary SCADA node.
7. Click OK.

Configuring Data Sync Transports for Enhanced Failover

For Enhanced Failover, you need to select the network LAN adapter(s) to use for SCADA synchronization on both the primary and secondary SCADA nodes. The data sync transports should be

configured when you first configure your primary and secondary SCADA nodes. You must already have your hardware installed and configured (obtain an IP Address) before you can enter your iFIX configuration.

To configure your data sync transports and the IP address for the partner SCADA:

1. Open the System Configuration Utility (SCU).
2. In the SCADA Configuration dialog box, click the Data Sync Transport button. The Data Sync Transport Options dialog box appears.

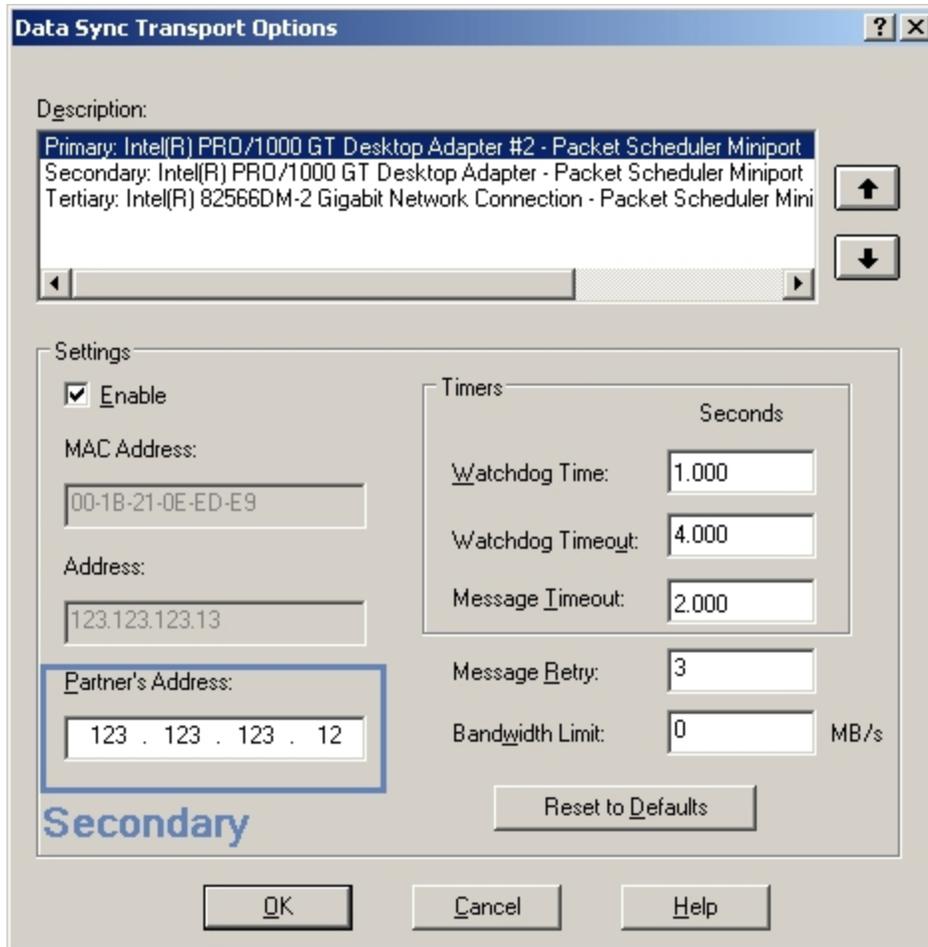
Select the LAN adapter(s) to use for SCADA synchronization and select their order. When using UDP, the two network cards (for these two IP addresses) need to be on the same physical network, and should be static or fixed IP addresses. All available adapters are enabled by default, including those used for iFIX networking. You should disable any adapter that is not used for SCADA synchronization.

Up to three data sync transports can be configured in the Data Sync Transport Options dialog box.

If you are using only one network adapter (i.e., Primary), it must be at the top of the list. If you are using multiple adapters, they must be in the same order on each SCADA (e.g., Primary should be first, Secondary should be second, Tertiary should be third).

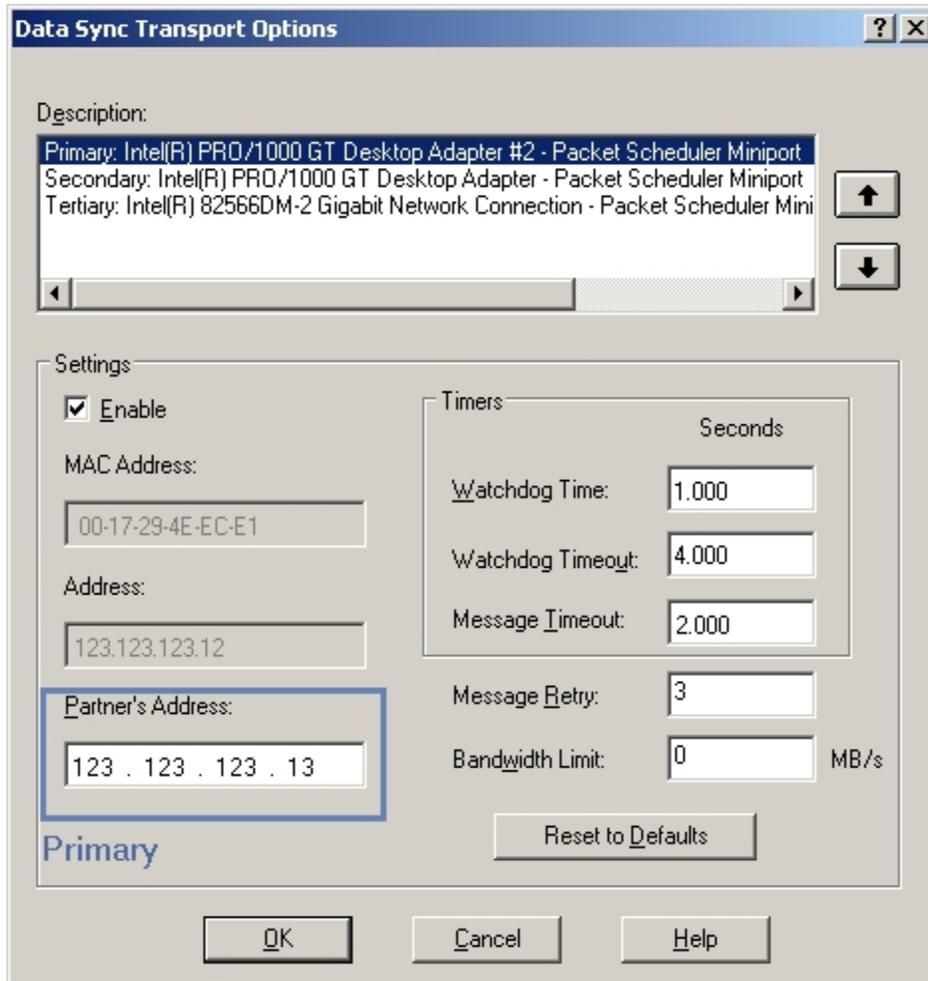
If you add or remove LAN adapters at a later date, you will need to re-configure the data sync transports, as well as the network configuration settings in the SCU. The primary, secondary, and tertiary LAN connections and partner IP address must be entered for each LAN.

The following example shows the Data Sync Transport Options dialog box for a primary node with the Partner's Address field highlighted. In this figure, the secondary node partner, ALBANY, has an IP address of 123.123.123.12.



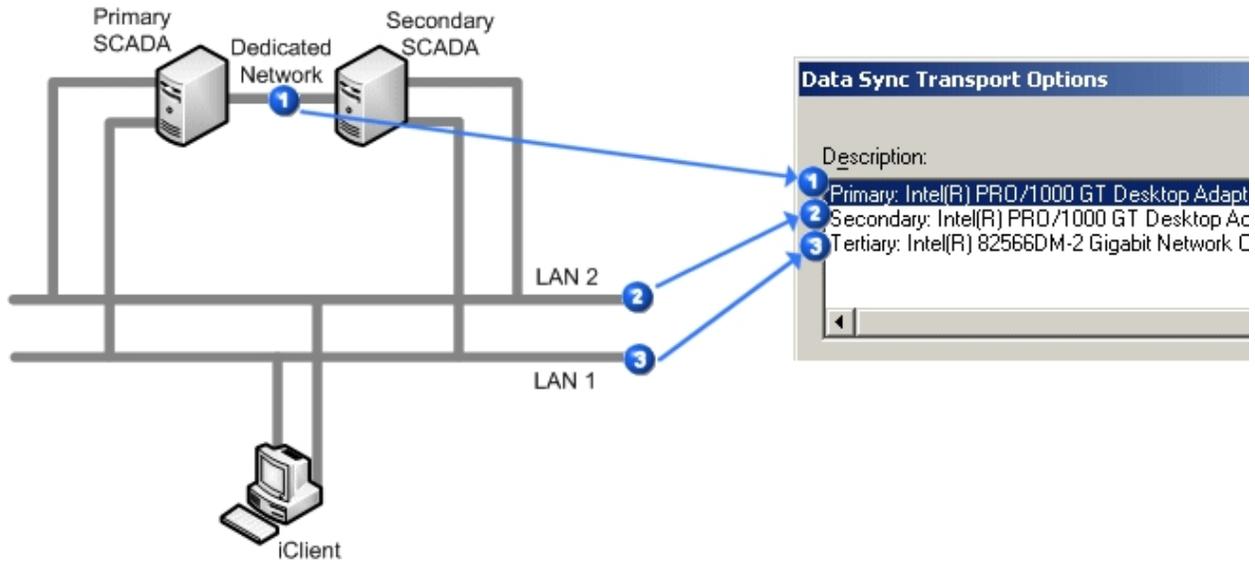
Primary Node, Data Sync Transport Dialog Box

The next figure shows the Data Sync Transport Options dialog box that you edit for the secondary node, ALBANY. The primary node, FOXBORO, has an IP address of 123.123.123.13. Notice how the Address and Partner's Address fields are reversed.



Secondary Node, Data Sync Transport Dialog Box

It is not required for all three network choices to be Gigabit-Ethernet cards; however, it is strongly recommended that you use at least one Gigabit-Ethernet card for dedicated SCADA-to-SCADA traffic, as the Primary data sync transport. In this example, the dedicated SCADA-to-SCADA network is selected as the Primary data sync transport. LAN1 and LAN2 are primarily used for iFIX networking. LAN1 is the iFIX primary network; LAN2 is the backup iFIX network (as configured in the Advanced Network Configuration). LAN2 is selected as the secondary SCADA synchronization transport as it will carry less traffic than LAN1. LAN2 is selected as the tertiary SCADA sync transports as it will carry more traffic than LAN2. The following figure illustrates how these three transport options map to the available network adapters.



NOTE: Although this example shows Enhanced Failover configured with iFIX LAN Redundancy Enhanced Failover and iFIX LAN Redundancy do not have to be configured together. One can be used separately without the other. Primary, Secondary, and Tertiary data sync transports can be configured with or without iFIX LAN Redundancy.

NOTE: The Dedicated Network in the above example is required only if you are using UDP.

Data Sync Transport Options Dialog Box

The following table describes the fields in the Data Sync Transport Options dialog box.

Item	Description
Description area	Lists all available network adapters for use as primary, secondary, and tertiary data sync transports in the order of priority. Up to three LAN adapters can display in this field. Use the Up and Down arrows to move a network adapter up or down in the list, to change the priority levels. The descriptions that appear here match what appears in the network configuration for the operating system.
Enable	Select this check box to use the selected network adapter for SCADA synchronization.
MAC Address	This field is for viewing purposes only. The Media Access Control (MAC) address represents a unique identifier for the selected network adapter on the local computer.
Address	This field is for viewing purposes only. The Address is the IP address for the selected network adapter on the local computer.
Partner's Address	Enter the IP address in this field into the Partner Address field on the other SCADA node in the pair. Enter the IP address of the partner SCADA node. If you are configuring the primary SCADA, this IP address is the

	<p>IP address of the corresponding network adapter on the secondary SCADA node.</p> <p>If you are configuring the secondary SCADA, this IP address is the IP address of the corresponding network adapter on the primary SCADA.</p> <p>The IP address that you enter should be a static or fixed IP address. Do not use DNS-assigned IP addresses for Enhanced Failover.</p>
Watchdog Time	<p>Enter a value, in seconds, indicating how long ScadaSync.exe waits if it has not heard from the partner SCADA. A ping message (data packet) is sent to the partner SCADA if there has been no communication with the partner node in this time period.</p>
Watchdog Timeout	<p>By default, this value is 1.000 second.</p> <p>Enter a value, in seconds, indicating how long you want ScadaSync.exe to wait before determining that this transport is not connected.</p>
Message Timeout	<p>By default, this value is 4.000 seconds.</p> <p>Enter a value, in seconds, indicating how long ScadaSync.exe waits for an acknowledgement from the partner SCADA (indicating that a data packet is received successfully). If an acknowledgement is not received by this time-out period, the retry logic initiates according to the value of the Message Retry field.</p> <p>When a message times out, the SCADA Sync Monitor (a diagnostic program) displays a message on the debug output screen. On this screen, the timer will show up as milliseconds. For more information on this screen in the SCADA Sync Monitor, refer to the Debug Log for Troubleshooting section.</p>
Message Retry	<p>By default, the Message Timeout value is 2.000 seconds.</p> <p>Enter the number of times to retry sending a data packet, if an error or time-out occurred.</p>
Bandwidth Limit	<p>By default, this value is 3.</p> <p>Enter the number of megabytes that you want to throttle network traffic by. By default, this value is 0 (no throttling).</p> <p>If a non-dedicated network between the SCADA pair is being used for data synchronization, this setting should be utilized so as to not consume an inordinate amount of network bandwidth.</p>
Reset to Defaults	<p>As an example, on a dedicated Gigabit-Ethernet, values between 20 and 30 MB/s are typical.</p> <p>Click this button to replace the current settings in the Data Sync Transport Options dialog box with the default factory settings.</p>

Steps to Configure the Data Sync Transports

► To define the data sync transports on the primary SCADA:

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click SCADA. The SCADA Configuration dialog box appears.
3. In the Failover area, confirm that the Enable check box is selected. If it is not, select Enable now.
4. In the Failover area, click the Data Sync Transport button. The Data Sync Transport Options dialog box appears.
5. In the Description list, highlight the network adapter to use for data synchronization between the SCADA pair.
6. Select the Enable check box.
7. If you want the enabled adapter to appear on another line (slot), you can move the adapter up or down in the list using the up and down arrow buttons.
8. In the Partner's Address field, enter the IP address of the secondary SCADA node.
9. Leave the default settings for the rest of the fields.
10. Click OK.

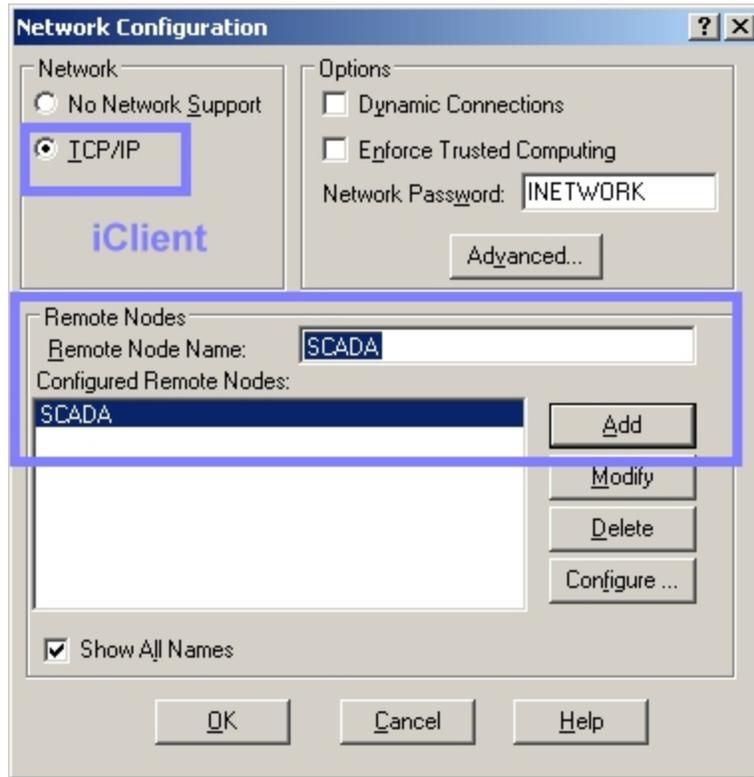
► To define the data sync transports on the secondary SCADA:

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click SCADA. The SCADA Configuration dialog box appears.
3. In the Failover area, confirm that the Enable check box is selected. If it is not, select Enable now.
4. In the Failover area, click the Data Sync Transport button. The Data Sync Transport Options dialog box appears.
5. In the Description list, highlight the network adapter to use for data synchronization between the SCADA pair.
6. Select the Enable check box.
7. If you want the enabled adapter to appear on another line (slot), you can move the adapter up or down in the list using the up and down arrow buttons.
8. In the Partner's Address field, enter the IP address of the primary SCADA node.
9. Leave the default settings for the rest of the fields.
10. Click OK.

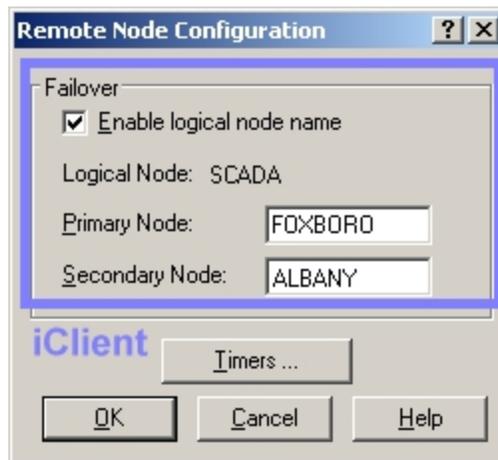
Configuring iClients

To configure an iClient for Enhanced Failover, in the SCU for the iClient, you must add the logical name of the SCADA pair to the remote node list in the Network Configuration dialog box. You must do this for all iClients, as well as the primary and secondary pairing for this SCADA node. The following figure

shows an example of the Network Configuration dialog box for an iClient node with the fields requiring edits highlighted.



After you make these changes in the Network Configuration dialog box, you need to configure the logical node name in the Remote Network Configuration dialog box. These steps must be performed on all iClient or View nodes that obtain data from the SCADA pair. The following example shows the Remote Network Configuration dialog box for an iClient node with the fields requiring edits highlighted. The primary node name is FOXBORO, while the secondary node name is ALBANY, and logical node name is SCADA.



iClient, Remote Node Configuration Dialog Box

How the iClient Works in Run Mode

When iFIX starts, the iClient attempts to establish iFIX networking communication with its primary and secondary SCADA Servers.

If both nodes are available, the iClient establishes an iFIX networking connection with both of them but will get its data and alarms only from the active SCADA. If only one SCADA Server is available, the iClient establishes a connection with it. If neither SCADA Server is available, the iClient polls both nodes until it establishes a connection with at least one SCADA server.

If iFIX is stopped on the active SCADA, the computer is shut down, all networking to the SCADA fails, or a manual failover is initiated, the standby SCADA will become the active SCADA. All iClient nodes will switch to the newly active node and will now get their data and alarms from the newly active SCADA.

If LAN Redundancy is not enabled (only one network path is enabled for iFIX Networking):

If the iClient loses its iFIX networking connection to the active SCADA, it fails over to the standby SCADA, if available. The iClient remains connected to the standby SCADA until the active SCADA becomes available to the iClient again. In this condition, the iClient displays an iFix Notification message indicating that you will not receive alarms, cannot do writes, and displayed data may be out of date. This message box closes within a minute after iFIX networking connection to the active SCADA is restored. If a write is attempted in this condition, the following prompt displays: "Cannot write value. The SCADA node is in Standby mode." You will also receive a prompt if you attempt to modify the database from the Database Manager on the iClient node.

If LAN Redundancy is is enabled (two network paths are enabled for iFIX Networking):

If the iClient loses its iFIX networking connection to the active SCADA, the LAN redundancy feature will switch to use the other iFIX network to continue to get data and alarms from the active SCADA. If the second iFIX network also fails, the iClient fails over to the standby SCADA, if available. The iClient remains connected to the standby SCADA until the active SCADA becomes available to the iClient again. In this condition, the iClient will display an iFIX Notification message indicating that you will not receive alarms, cannot do writes, and displayed data may be out of date. This message box closes within a minute after iFIX networking connection to the active SCADA is restored. If a write is attempted in this condition, the following prompt displays: "Cannot write value. The SCADA node is in Standby mode." You will also receive a prompt if you attempt to modify the database from the Database Manager on the iClient node.

Steps to Configure

1. [Add the remote node on the iClient.](#)
2. [Configure the logical node name \(remote node\) on the iClient.](#)

IMPORTANT: If you use Enhanced Failover with LAN Redundancy, you must also update the HOSTS file on the primary computer, the secondary computer, and all iClient computers that connect to the active SCADA Server pair. Make sure that the HOSTS files contain static or fixed IP addresses for the primary and secondary SCADA nodes.

► **To add the remote node on the iClient:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click Network. The Network Configuration dialog box appears.
3. In the Network area, select the TCP/IP option.
4. In the Remote Node Name field, enter the name of the logical node name of the SCADA pair.
5. Click Add. The name now appears in the Configured Remote Nodes list.
6. Click OK.

► **To configure the logical node name (remote node) on the iClient:**

1. On the Start menu, point to Programs, iFIX, and then System Configuration. The System Configuration Utility (SCU) appears.
2. On the Configure menu, click Network. The Network Configuration dialog box appears.
3. In the Configured Remote Nodes list, select the logical node name that you added.
4. Click Configure. The Remote Node Configuration dialog box appears.
5. Select the Enable Logical Node Name check box.
6. In the Primary Node field, enter the primary node's local node name.
7. In the Secondary Node field, enter the secondary node's local node name.
8. Click OK to close the Remote Node Configuration dialog box.
9. Click OK.

Disabling the 1914 Error Message

When an iClient establishes a connection to an active SCADA Server node, it starts to read data from that node. When the active SCADA Server node becomes unavailable or manual switching of the active SCADA occurs, the iClient momentarily loses its session with that node, causing a message box to appear with following message:

```
1914: Node.Tag.Field Connection Not Established With Node
```

To suppress this message from appearing on screen, edit the FilteredErrors.ini file, which is located in the C:\Program Files (x86)\Proficy\iFIX\Local directory. Add the 1914 error code to the FilteredErrors.ini file, as shown in the following example:

```
;To add an error code to be filtered increment the count and set  
;the Error equal to the return code
```

```
[ErrorCodes]  
Count = 4  
Error1 = 1620  
Error2 = 1914  
Error3 = 1915  
Error4 = 8517
```

In this example, all typical network session errors are suppressed. After you edit the FILTEREDERRORS.INI file, restart the iFIX WorkSpace to ensure your changes take effect.

► **To suppress the 1914 message from appearing on screen:**

1. Open the FilteredErrors.ini file in a text editor, such as Notepad. The FilteredErrors.ini file is typically located in the C:\Program Files (x86)\Proficy\iFIX\Local directory.
2. Add a line for your entry, as in the following example:

```
;To add an error code to be filtered increment the count and set  
;the Error equal to the return code
```

```
[ErrorCodes]  
Count = 4  
Error1 = 1620  
Error2 = 1914  
Error3 = 1915  
Error4 = 8517
```

3. Save the file.

Testing Your Enhanced Failover Configuration

After you complete your Enhanced Failover configuration, be sure to save your changes in the System Configuration Utility (SCU) on both the primary and secondary nodes. You can now begin to test your changes. Validate each node independently, then validate the pair.

► **To test your nodes:**

1. Start the Primary node and verify that it's working properly.
2. After you confirm the Primary node is working properly, shutdown the Primary node.
3. Start the Secondary node and verify that it's working properly.
4. After you confirm the Secondary node is working properly, shutdown the Secondary node.
5. Restart the Primary node.
6. Restart the Secondary node. This allows the SCADAs to start in the preferred SCADA roles: the Primary as Active, and the Secondary as Standby.
7. Allow a minute or two for the nodes to connect, ensuring all data & alarms settle out before the Failover status changes.
8. Confirm that the Primary SCADA starts as the Active node and all driver and PLC communications are good. The iClients should connect to the Primary and have the ability to change and read data. The Secondary SCADA should start up as the Standby node.

Use the following tools to help you monitor the initial status of the Enhanced Failover pair and the network:

- Windows Task Manager, Networking tab – to see if your networking cards are doing what they are configured to do, and that each adapter is performing appropriately.

- Windows Task Manager, Processes tab – to verify that ScadaSync.exe and ScadaRoleMgr.exe are listed as running on both SCADAs.
- [SCADA Sync Monitor](#) – to display runtime information about the primary and secondary SCADA Servers.
- [Runtime Information Fields](#) – to display additional runtime information available about your primary and secondary SCADA Servers, that does not already display in the SCADA Sync Monitor. These fields can be added to pictures or EDA applications. For example, these fields allow you to access more information about your data sync transports than you can in the SCADA Sync Monitor.
- [Mission Control](#) – to view the status of the Scan, Alarm, and Control (SAC) program and whether blocks are being processed.
- [NetDiag](#) – to check network communication, particularly if you are using Enhanced Failover with LAN Redundancy.

Tips for Enhanced Failover Configurations

Recommendations for working with Enhanced Failover in iFIX include:

- For scripts in pictures that you develop, always use the logical node name, unless you specifically need to use the physical node name.
- EDA programs should use the logical node name as well.
- Ensure the same loadable blocks” (also called Database Dynamos) are installed on both SCADAs in the same slots.
- When configured and running, use the SCADA Sync Monitor to check the status of the SCADA nodes. For more information on this and other uses of the SCADA Sync Monitor, refer to the [Enhanced Failover Diagnostics with the SCADA Sync Monitor](#) section.
- Use the FILTEREDERRORS.INI file to filter out commonly displayed error messages such as the 1914 error message displayed when a failover occurs. For steps, refer to the [Disabling the 1914 Error Message](#) section.
- Use the [Checklist for Enhanced Failover Configuration](#) to ensure that you configured the Enhanced Failover feature properly. This checklist lists each task in the configuration process, and whether it applies to the primary node, secondary node, and/or iClient.
- Be sure to enable the Keep Alive Network Timer in the SCU for network configuration on all nodes. Decreasing the Keep Alive Timer increases the frequency of the delivery of failover status from the SCADA nodes to the clients. For more information, refer to the [Timer Dialog Box](#) section of the [Setting Up the Environment](#) e-book.
- On redundant SCADA nodes, do not reduce the SAC delay interval below the default value (8 seconds). This allows the SCADA Role Manager (ScadaRoleMgr.exe) to set the node status of ACTIVE or STANDBY before the SAC initializes. For more information, refer to the [Controlling SAC Startup](#) section of the [Setting Up the Environment](#) e-book.

IMPORTANT: The SAC delay period **must be the same** on both the primary and secondary nodes. When the SAC delay on the primary node is less than the SAC delay on the secondary node, the secondary node may incorrectly try to become ACTIVE.

- Synchronize the clocks on the SCADA nodes. For more information, refer to the following section [Synchronizing the Clocks on the SCADA Servers](#).
- Identify factors that are affecting performance and improve them, if possible.

Synchronize the Clocks on the SCADA Servers

To ensure that all iClients see the same data and alarms, synchronize the clocks on both the primary and secondary SCADA nodes. If the clocks are not synchronized and a failover occurs, alarms received from the primary and secondary nodes could have significantly different timestamps, even if both alarms were generated at the same instant. You can synchronize the SCADA clocks using the NET TIME command. Refer to the Windows operating system online Help for more information.

Identify Factors Affecting Performance

Factors that can affect database (PDB) synchronization timing include:

- Database size
- Network speed and/or traffic
- Network adapter used

Enhanced Failover and VMWare ESX or ESXi Server

When using Enhanced Failover with iFIX include and VMWare, be aware that:

- For data synchronization between both the Primary and the Secondary SCADAs, use a CAT6 cable (without going through any switches, hubs, or routers), or the VMXNET 3 network adapter (for UDP only).
- Use a 1 Gigabit-Ethernet NIC card (or better) or the VMXNET 3 network adapter NIC for dedicated SCADA-to-SCADA traffic (for a total of two network cards). The NIC cards need to match exactly. It is recommended to disable all Offload settings for your Enhanced Failover and iFIX networking NIC properties. If using a virtual server, you may also have to do this on the virtual NIC's and/or switches.
- By default, port 53014 should be open on your firewall. If you change this port in the scadasync.ini file, ensure the newly configured port is open.
- The IP address associated with the network card (NIC) definition in the FIX SCU Data Sync Transport Options should match the IP address associated with the NIC properties in the Windows network configuration.
- The cable or switch between the SCADAs is functioning correctly. Be sure that you can ping both the Primary and Secondary by iFIX node name, from each of the SCADA nodes.
- The FIX.ini file contains the right settings in the [PartnerSCADA] section. Make sure both ScadaSync.exe and ScadaRoleMgr.exe are listed. You can also check in Windows Task Manager on both SCADAs to make sure both tasks are currently running.
- The power savings settings are disabled on the NIC cards.
- The Windows HOSTS file contains the correct IP address and iFIX nodename for both the Primary and the Secondary SCADAs. Make sure this file is the same on both SCADAs.

- The Windows HOSTS file should contain the correct IP address for iFIX networking. Make sure this file is the same on both SCADAs. The IP addresses for the SCADA Synch NIC cards should not be in the HOSTS file.
- The driver versions match between both the Primary and the Secondary SCADAs, and they are in the same order in the SCU.
- The driver configuration files, AAD file, and the PDB file should have been copied from the Primary to the Secondary so they are identical.
- If you are running iFIX as a Service on one SCADA, confirm that you are running it as a Service on the other SCADA. (If you are running iFIX as a Service on one SCADA, you must run it as a Service on the other SCADA.)
- Run BTKCFG.exe on both SCADAs. Make sure they both have the same loadable blocks configured and they are all using the same slot number.
- Jumbo Frames are enabled for the Data Sync NICs and they both have the same MTU value. See the next section for more details.

For detailed information on all system requirements, see the section of the iFIX Getting Started guide. For a complete checklist of all items to check in your enhanced failover configuration, see [Configuring Computers for Enhanced Failover](#).

Configuring Jumbo Frames when Using VMWare

NOTE: This section applies to UDP only.

By default, the VMWare image may have the MTU value for Jumbo Frames set to 1500. On the VMWare ESX/ESuXi Server, set this value to 9000.

The NIC card on the physical machine may not have a valid value for 9000, but may have a value of 9014. You can use this value even though the MTU you set in VMWare ESX/ESXi Server will have a value of 9000.

To enable Jumbo Frames for software and dependent hardware iSCSI adapters in the vSphere Web Client, change the default value of the MTU parameter:

1. Browse to the host in the vSphere Web Client navigator.
2. Click the Manage tab, and then click Networking.
3. Click Virtual Switches and select the vSphere switch that you want to modify from the list.
4. Click Edit Settings.
5. On the Properties page, change the MTU parameter. (This step sets the MTU for all physical NICS on that standard switch. The MTU value should be set to the largest MTU size among all NICS connected to the standard switch. ESXi supports the MTU size up to 9000 Bytes.)
6. After you make these changes, reset the systems and start them in the proper sequence.

For more information on Jumbo Frames configuration for VMWare, see article ID 1007654 on the VMWare support web site: <http://kb.vmware.com/selfservice>.

Monitoring Network Status

The Network Status Display (NSD) fields are available for writing application programs and create displays that monitor and control iFIX networking. This section explains how to use the Network Status Display tag on the iClient to:

- Monitor network status.
- Monitor Enhanced Failover status and manually initiate failover to the standby SCADA.
- Trigger an event on failover to the standby SCADA or LAN.

Monitoring Network Status

You can monitor the status of the network using the NSD diagnostic fields. This feature allows you to monitor sessions on your network, determine which nodes are active, and display the name of the local node. In the event that a SCADA Server becomes unavailable, you can also display an error code and text describing the current state of the connection with each SCADA Server.

iFIX provides the Network Status Display (NSD) tag that you can use when designing displays for monitoring and controlling Enhanced Failover and LAN Redundancy. This tag is not a database block. It is a special tag residing on each networked node that displays diagnostic, failover, and network information. Refer to the table of available Network Status Display fields in the [Network Status Display Fields](#) section.

To access the fields, use the server.node.NSD.field syntax. In the following example, PACKER1 is the local physical name. NSD is always the tag.

```
FIX32.PACKER1.NSD.A_PRIMARYSCADA_0
```

NOTE: TCP/IP networking must be enabled in the SCU to use NSD fields in iFIX.

Monitoring Enhanced Failover Status and Initiating Manual Failover to the Standby SCADA

Three NSD fields have been added for Enhanced Failover: SCADAREDUN, SCADASTATUS, and SWITCHSCADAROLE.

F_SCADAREDUN is a read-only field that returns an indication as to whether enhanced failover is enabled on the SCADA node. If Enhanced Failover is enabled, a 1 displays, and if it is disabled, a 0 displays.

F_SCADASTATUS and A_SCADASTATUS are read-only fields that return an indication as to whether the SCADA node is in an active state or the standby state. If the SCADA is in an active state, a 1 (or ACTIVE) displays, and if it is in the standby state, a 2 (or STANDBY) displays.

In addition to monitoring the SCADA status or having automatic SCADA failover, you can also manually force a SCADA failover to occur at any time. For example, you can manually switch to the standby SCADA node when the active SCADA node needs to be shut down for maintenance. When iFIX security is enabled, the Manual Failover application feature is checked prior to performing the manual SCADA failover. The Manual Failover application feature should be assigned to users or groups who are allowed to manually initiate SCADA failover.

F_SWITCHSCADAROLE and A_SWITCHSCADAROLE are read/write fields that return an indication as to whether the SCADA node is in an active state or the standby state. If the SCADA is in an active state, a 1 (or ACTIVE) displays, and if it is in the standby state, a 2 (or STANDBY) displays. To perform a manual SCADA failover, a write of 1 (or ACTIVE) causes the SCADA to become the active SCADA. A write of 2 (or STANDBY) causes the SCADA to become the standby SCADA.

Enabling/Disabling Drivers on SCADA Pairs

For the active SCADA node, you must enable its drivers so that it can poll for data. Similarly, for a standby SCADA you should disable its drivers in order to reduce the load on the PLCs.

For further information, refer to:

- Disable the IGS Driver on an iFIX Enhanced Failover Standby Scada
- Enable or Disable Datablocks, Devices or Channels in a 7.x Driver Programmatically

Triggering an Event on Failover

You may want to trigger an event when a SCADA failover occurs. For example, you may want to display a message informing the operator of the failover, and when the operator acknowledges the message, close a valve or sound an alarm. Use the Scheduler to create schedules to do this. Refer to the [Creating and Editing Schedules and Entries](#) section for more information.

To trigger an event on SCADA failover, write to the A_FAILOVER or F_FAILOVER Network Status Display field. This field is set to 1 on automatic or manual failover. You must reset it to 0 to receive notification of subsequent failovers.

To see if any connection has had a SCADA failover, read the F_SCADAANYFAILOVER field. It is set to non-zero if any F_FAILOVER field is set to non-zero.

To trigger an event on LAN failover, write to the F_LANFAILOVER or A_LANFAILOVER field. This field is set to 1 on LAN failover. You must reset it to 0.

To see if any connection has had a LAN failover, read to the F_LANANYFAILOVER field. It is set to non-zero if any F_LANFAILOVER field is set to non-zero.

For more information on the Network Status Display fields, refer to the [Network Status Display Fields](#) section.

Network Status Display Fields

What is the NSD Tag?

The Network Status Display (NSD) tag is a system tag that allows you to monitor network information. This tag is not a database block. It is a special tag residing on each networked node that contains diagnostic, failover, and network information.

The Network Status Display (NSD) fields contain networking information. For instance, these fields include node specific information such as the current active node name, the logical SCADA name, the backup path, the failover status, and so on. Networking must be enabled in SCU, or you will not be able to view the fields for NSD tags.

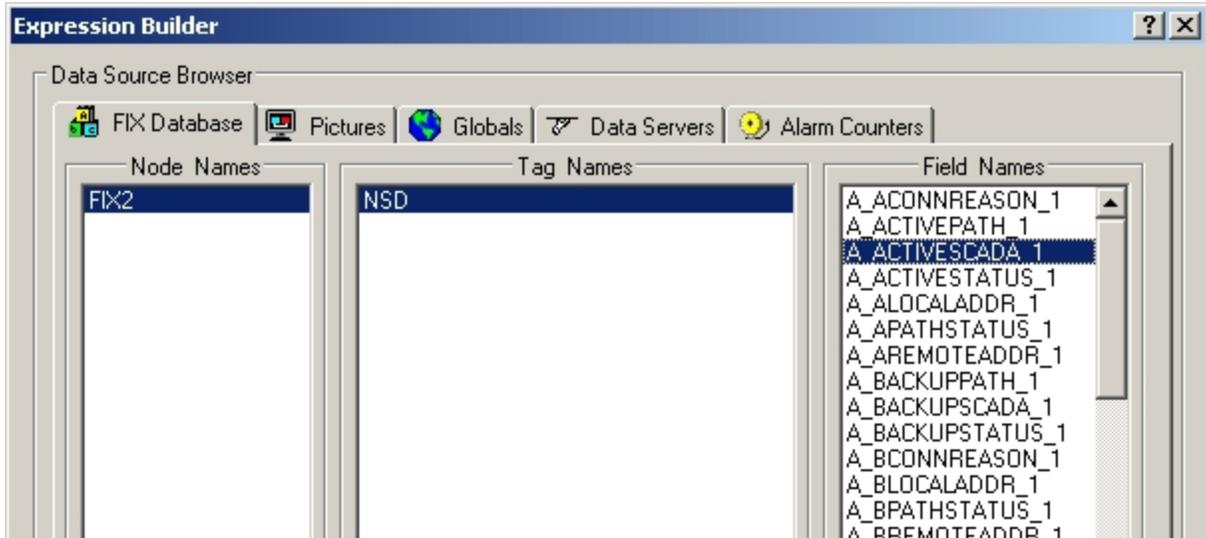
NSD fields can be used in a datalink in an iFIX picture. For instance, to display networking information for troubleshooting or diagnostics.

If you do not have an iFIX key on your computer, you will not be able to access the NSD tag. This is because in Demo mode, iFIX does not have networking enabled. You must have a key on your computer that supports networking in order to display the NSD information in iFIX. The NSD tag is not supported in iFIX Demo mode.

How to View NSD Fields in iFIX

To view NSD fields in iFIX, you must first enable TCP/IP networking enabled in the SCU (in the Network Configuration dialog box).

You can view NSD field names from the iFIX WorkSpace, using the iFIX Expression Builder. On the iFIX Database tab, select the Node name, and then the NSD tag should appear in the list of tags. When you click the NSD tag, the fields should appear in the field names column, as shown in the following figure.



Zero-based NSD Fields

In the following table, the _0 through _200 appended to field names indicates that information is available on a per-connection basis. When _0 is appended to a field name, the information pertains to the local node. Since there can be up to 200 node names in the SCU, _1 through _200 typically correspond to the order of the names in the SCU. However, any primary and secondary grouping in the SCU that contains the local node name is always located at index _0.

One-based NSD Fields

In the following table, if the field is 1-based, when _1 is appended to a field name, the information pertains to the local node. _2 through _200 typically correspond to the order of the names in the SCU. Any primary and secondary grouping in the SCU that contains the local node name is located at index _1.

Field Descriptions

The following table lists the fields that are available for the Network Status Display (NSD) tag.

Network Status Display (NSD) Fields

Field Name	Description
A_ACONNREASON_0 through A_ACONNREASON_200	The current state of the connection to the active node. This is either "Established" or text describing the current state.
F_ACTIVECLIENTS	The total number of connected view nodes.
A_ACTIVEPATH_0 through A_ACTIVEPATH_200	Indicates if the active path is the primary or secondary path.
F_ACTIVEPATH_0 through F_ACTIVEPATH_200	A 0 in this field indicates that the primary path is the active path; a 1 indicates that the backup path is the active path.
A_ACTIVESCADA_0 through A_ACTIVESCADA_200	Active SCADA Server name, which can be either the primary or secondary node name.

A_ACTIVESTATUS_0 through A_ACTIVESTATUS_200 F_ACTIVESTATUS_0 through F_ACTIVESTATUS_200	Status of the connection to the active SCADA (OK or an error code). It will be one of the primary, logical, or secondary statuses.
A_ALOCALADDR_0 through A_ALOCALADDR_200	This is for the active network connection. For TCP/IP, displays the local IP address used to reach the remote node.
F_ALLOWREMOTEWRITES_0 through F_ALLOWREMOTEWRITES_200	This field is 1 if remote nodes are allowed to write to the NSD fields on the active node, or 0 if writes are not allowed.
A_APATHSTATUS_0 through A_APATHSTATUS_200 F_APATHSTATUS_0 through F_APATHSTATUS_200	Status of the connection over the active path. This is either the primary or secondary status.
A_AREMOTEADDR_0 through A_AREMOTEADDR_200	This is for the active network connection. For TCP/IP, displays the IP address of the remote node.
A_BACKUPPATH_0 through A_BACKUPPATH_200	Backup network path. When using LAN Redundancy, it shows the paths per connection. For TCP/IP, it is the IP address.
A_BACKUPSCADA_0 through A_BACKUPSCADA_200	Standby SCADA Server name for this connection.
A_BACKUPSTATUS_0 through A_BACKUPSTATUS_200 F_BACKUPSTATUS_0 through F_BACKUPSTATUS_200	Status of the connection to the standby SCADA (OK or an error code).
A_BCONNREASON_0 through A_BCONNREASON_200	The current state of the connection to the standby node. This is either "Established" or text describing the current state.
A_BLOCALADDR_0 through A_BLOCALADDR_200	This is for the backup network connection. For TCP/IP, displays the local IP address used to reach the remote node.
A_BPATHSTATUS_0 through A_BPATHSTATUS_200 F_BPATHSTATUS_0 through F_BPATHSTATUS_200	Status of the connection to the backup network path.
A_BREMOTEADDR_0 through A_BREMOTEADDR_200	This is for the backup network connection. For TCP/IP, displays the IP address of the remote node.
A_CONNDIRECTION_0 through A_CONNDIRECTION_200	Indicates whether the connection is incoming or outgoing. -> if outgoing. <- if incoming. <-> if both outgoing and incoming.
A_CURACTIVENODE_0 through A_CURACTIVENODE_200 F_CURACTIVENODE_0 through F_CURACTIVENODE_200	Indicates if the active node is the primary or secondary SCADA. A 0 in this field indicates that the primary SCADA is the active node; a 1 indicates that the secondary SCADA is the active node.

200	
A_FAILDISABLE_0 through A_FAILDISABLE_200	Automatic SCADA failover state.
F_FAILDISABLE_0 through F_FAILDISABLE_200	A 0 in this field indicates that automatic SCADA failover is enabled if it is configured; a 1 disables automatic SCADA failover. Manual failover is still possible.
A_FAILOVER_0 through A_FAILOVER_200	This field is set to 1 on automatic or manual SCADA failover. You must reset it to 0 to receive notification of subsequent failovers.
F_FAILOVER_0 through F_FAILOVER_200	You can read to this field to trigger an event on SCADA failover.
F_FAILOVERMANL_0 through F_FAILOVERMANL_200	Total number of manual failovers to this node since iFIX startup.
F_FAILOVERTOTAL_0 through F_FAILOVERTOTAL_200	Total number of failovers (automatic and manual) to this node name since iFIX startup.
F_LANANYFAILOVER	Use this field to see if any connection has had a LAN failover. It is set to a non-zero number, if any.
A_LANFAILDSABL_0 through A_LANFAILDSABL_200	Enabled in this field indicates that LAN Redundancy is enabled if it is configured; Disabled indicates LAN Redundancy is disabled.
F_LANFAILDSABL_0 through F_LANFAILDSABL_200	Use this field to disable LAN Redundancy on a per connection basis.
A_LANFAILOVER_0 through A_LANFAILOVER_200	This field is set to 1 on LAN failover. You must reset it to 0.
F_LANFAILOVER_0 through F_LANFAILOVER_200	
F_LANFAILOVERTOTAL_0 through F_LANFAILOVERTOTAL_200	Total number of automatic failovers to this path since iFIX startup. Session losses that are re-established over the same network path are not included.
A_LOCALNAME	Displays the local physical node name.
A_LOGICALNAME_0 through A_LOGICALNAME_200	Logical SCADA Server name for this connection. (Same as A_LOGICALSCADA and retained for backwards compatibility.)
A_LOGICALSCADA_0 through A_LOGICALSCADA_200	Logical SCADA Server name for this connection.
A_LOGICALSTATUS_0 through A_LOGICALSTATUS_200	Status of the connection to the logical SCADA (OK or an error code).
F_LOGICALSTATUS_0 through F_LOGICALSTATUS_200	
A_NETNAME_0 through A_NETNAME_200	Name used to connect to the remote node. For TCP/IP, it is the remote node name.
A_PCONNREASON_0 through A_PCONNREASON_200	The current state of the connection to the primary node. This is either "Established" or text describing the current state.
A_PLOCALADDR_0 through A_PLOCALADDR_200	This is for the active network connection. Displays the local TCP/IP address used to reach the remote node.
A_PPATHSTATUS_0 through A_PPATHSTATUS_200	Status of the connection over the primary network path.

F_PPATHTHSTATUS_0 through F_PPATHTHSTATUS_200	
A_PREMOTEADDR_0 through A_PREMOTEADDR_200	This is for the active network connection. For TCP/IP, displays the IP address of the remote node.
A_PRIMARYPATH_0 through A_PRIMARYPATH_200	Primary network path. When using LAN Redundancy, it shows the paths per connection. For TCP/IP, it is the IP address.
A_PRIMARYSCADA_0 through A_PRIMARYSCADA_200	Primary SCADA Server name for this connection.
A_PRIMARYSTATUS_0 through A_PRIMARYSTATUS_200	Status of the connection to the primary SCADA (OK or an error code).
F_PRIMARYSTATUS_0 through F_PRIMARYSTATUS_200	
A_PROTOCOL	Displays the current protocol (TCP/IP) that iFIX is using for networking.
A_SCADASTATUS	The status of the SCADA node: ACTIVE (1) or STANDBY (2).
F_SCADASTATUS	
A_SWITCHSCADAROLE	A request for change in state: ACTIVE (1) or STANDBY (2).
F_SWITCHSCADAROLE	NOTE: The user who is currently logged on must have rights to the Enhanced Failover security area in order to perform a manual SCADA node role switch.
F_ALLOWREMOTEWRITES	This field is 1 if remote nodes are allowed to write to the NSD fields on this node, or 0 if writes are not allowed.
A_CURACTIVENODE_0 through A_CURACTIVENODE_200	Indicates if the active node is the primary or secondary SCADA. A 0 in this field indicates that the primary SCADA is the active node; a 1 indicates that the secondary SCADA is the active node.
F_CURACTIVENODE_0 through F_CURACTIVENODE_200	You can write to this field to perform a manual failover.
F_FAILDISABLE_0 through F_FAILDISABLE_200	SCADA Server failover state. A 0 in this field indicates that SCADA Server failover is enabled if it is configured; a 1 disables SCADA Server failover. Manual failover is still possible.
A_FAILDISABLE_0 through A_FAILDISABLE_200	You can write to this field to disable automatic failover to the standby SCADA on a per-connection basis.
A_FAILOVER_0 through A_FAILOVER_200	This field is set to 1 on automatic or manual SCADA failover. You must reset it to 0 to receive notification of subsequent failovers.
F_FAILOVER_0 through F_FAILOVER_200	You can read to this field to trigger an event on SCADA failover.
F_FAILOVERMANL_0 through	Total number of manual failovers to this node since iFIX startup.

F_FAILOVERMANL_200	
F_FAILOVERTOTAL_0 through F_FAILOVERTOTAL_200	Total number of failovers (automatic and manual) to this node name since iFIX startup.
F_LANANYFAILOVER	Use this field to see if any connection has had a LAN failover. It is set to non-zero if any F_LANFAILOVER_# field is set to non-zero.
F_LANFAILDSABL_0 through F_LANFAILDSABL_200	A 0 in this field indicates that LAN Redundancy is enabled if it is configured; A 1 indicates LAN Redundancy is disabled. Use this field to disable LAN Redundancy on a per connection basis.
A_LANFAILOVER_0 through A_LANFAILOVER_200	This field is set to 1 on LAN failover. You must reset it to 0.
F_LANFAILOVER_0 through F_LANFAILOVER_200	
F_LANFLOVRTOTAL_0 through F_LANFLOVRTOTAL_200	Total number of automatic failovers to this path since iFIX startup. Session losses that are re-established over the same network path are not included.
F_SCADAANYFAILOVER	Use this field to see if any connection has had a SCADA failover. It is set to non-zero if any F_FAILOVER_# field is set to non-zero.
F_SCADAREDUN	This field is set to 1 if Enhanced Failover is enabled; it is set to 0 if it is disabled.
F_TRANSACTTIME_0 through F_TRANSACTTIME_200	Indicates the amount of time, in milliseconds, that it took this iClient to get data from the SCADA Server the last time data transfer occurred.

Example Uses of Network Status Display Fields

To view NSD field names in the iFIX Expression Builder, you must have TCP/IP networking enabled in the SCU (in the Network Configuration dialog box). The NSD tag is not supported in iFIX Demo mode. Refer to the [Network Status Display Tag](#) section for more information.

NSD fields can be used in datalinks, for instance, to provide information on the current status of the SCADA network. In addition to the fields that already existed in previous releases, you can use the following new NSD fields in datalinks to monitor and switch the SCADA status:

- Fix32.physicalnodename.NSD.F_SCADAREDUN to display if Enhanced Failover is enabled on a SCADA node.
- Fix32.physicalnodename.NSD.F_SCADASTATUS (or A_SCADASTATUS) to display the current failover status of SCADA node.
- Fix32.physicalnodename.NSD.F_SWITCHSCADAROLE (or A_SWITCHSCADAROLE) to force the failover status of the active SCADA node to standby or of the standby SCADA node to active.

Other examples are provided in the following sections.

SCADA Failover

You can identify when a SCADA Server failover has occurred using a Network Status Display field (for example, A_FAILOVER_0 through A_FAILOVER_200, F_FAILOVER_0 through F_FAILOVER_200), or through the alarm messages.

iFIX sends an alarm message whenever SCADA Server failover occurs.

For example, if you are communicating from an iClient named LN1_VIEW to a primary SCADA node named FOXBORO, and the active SCADA fails over to the secondary SCADA node named ALBANY, the message on the iClient is:

```
06/07/2013 16:35:21.5 [FOXBORO] SAC is in Standby mode
06/07/2013 16:35:22.5 Connection Failover: failover attempted
06/07/2013 16:35:22.5 Connection Failover: connection to FOXBORO has been switched to ALBANY
06/07/2013 16:35:21.5 [ALBANY] SAC is in Active mode
```

LAN Failover

You can use a Network Status Display field (A_LANFAILOVER_0 through A_LANFAILOVER_200, F_LANFAILOVER_0 through F_LANFAILOVER_200) or the messages to identify when a LAN failover has occurred.

iFIX sends a message whenever LAN failover occurs.

For example, if you are communicating from an iClient named LN1_VIEW over TCP/IP address 1.1.1.2 to a SCADA node named FOXBORO, and the session is lost and re-established over TCP/IP address 198.212.170.4, the message on the iClient is:

```
19:24:00.0 [LN1_VIEW] Connection to [FOXBORO]
switched to 1.1.1.2 - 1.1.1.5 to 198.212.170.4 - 198.421.103.6
```

Custom Pictures with Logical and Physical Node Names

You can use either the logical or physical node name in displays to access data. You will only be able to write on the active SCADA. This section explains the impact of using one or the other and uses the iFIX WorkSpace as an example. This also applies to VBA scripts and any application that uses EDA (Easy Data Access) to access process data. For more information, refer to the [Writing Scripts](#) manual.

Pictures with links to tag names using the logical node name always display data from the active SCADA, regardless of whether it is the primary or secondary SCADA. This is done without requiring the picture to be opened, closed, or replaced after failover.

If you want to access data from a specific SCADA Server using the physical node name (and have a session established to it), you can read data from both the primary and secondary SCADA, regardless of which one is active, but you can only write to the SCADA that is active. You cannot write to the SCADA that is in standby mode. This is because you used the physical node name in the datalink. The picture displays data from the physical SCADA Server specified. If communication with that SCADA Server is lost, data for datalinks using the physical node name is not available at the iClient until the connection is re-established with that node.

For example, if the datalink on the iClient node is using the logical node name of the SCADA pair (for example LNN.DI_VALVE_OPEN.F_CV) and it is currently getting data from the primary SCADA (which is the active SCADA) and a failover to the standby SCADA occurs, then the datalink still displays data that is from the now active secondary SCADA.

However, if the datalink the iClient node is using the physical node name of the primary SCADA pair (for example FOXBORO.DI_VALVE_OPEN.F_CV) and is currently getting data from the primary SCADA (which is the active SCADA) and a failover to standby SCADA occurs, then the datalink displays @@@@ and a 1914 "Connection not established" prompt displays.

EDA and Network Status Display (NSD) Fields

With EDA applications in iFIX releases prior to 5.0, processing was done on one node, and then processing was done on the other, on a field-by-field basis. With Enhanced Failover, updates are made only when items change, saving valuable processing time and allowing the failover to occur faster.

If you are upgrading from a prior iFIX release, you will need to re-evaluate the NSD fields you use to get the status. Older EDA applications created for failover scenarios may not be correct when all the new information available in iFIX 5.1 is considered. There are new NSD fields that you may want to evaluate for use in your applications.

If you are creating new EDA applications, or modifying existing ones, you can use the following new NSD fields in datalinks to monitor and switch the SCADA status:

- **Fix32.physicalnodename.NSD.F_SCADAREDUN** to display if Enhanced Failover is enabled.
- **Fix32.physicalnodename.NSD.F_SCADASTATUS (or A_SCADASTATUS)** to display the current status of SCADA node.
- **Fix32.physicalnodename.NSD.F_SWITCHSCADAROLE (or A_SWITCHSCADAROLE)** to force the switching of the active SCADA node to the standby.

With these new fields, you can control EDA applications based on the SCADA role and mode.

Troubleshooting Enhanced Failover

Some common troubleshooting issues are provided in the following table. If you are new to Enhanced Failover, refer to the [Troubleshooting Checklist for Enhanced Failover Configuration](#) section if you do not know where to start troubleshooting your configuration.

IMPORTANT: When troubleshooting, be aware starting and stopping SAC in an Enhanced Failover environment is not recommended. Doing so, could place your system in an unexpected state. While the capability of starting and stopping the SAC is provided via Mission Control and with the iFIX Integration toolkit, such action on an Enhanced Failover pair may lead to an unexpected failover and role change. A restart of the SAC process will be interpreted as a failure and subsequently lead the standby SCADA node to be promoted to an active role. You may want to consider this prior to stopping and restarting SAC on any node in a failover pair.

Issue	Resolution
SCADA Failover feature is not enabled in the license for	This error found in ScadaRoleMgr.log indicates that your key does not support the Enhanced Failover feature. Check your

<p>this node.</p>	<p>key in the License Viewer, and contact GE to purchase an upgrade or replace a defective key.</p> <p>You will also get an error message at iFIX startup indicating the SCADA failover feature is not enabled in the license for your node.</p> <p>You must purchase the additional Enhanced Failover option (SCADA Failover) for all SCADA nodes if you plan to use SCADA Failover in iFIX.</p>
<p>The following errors appear:</p>	<p>These errors indicate that your loadable block configurations on one or both nodes are not configured properly. Loadable block configurations must be the same on both primary and secondary nodes. Use the BTKCFG utility on both SCADA nodes to exactly match your loadable block configurations. Loadable blocks are also referred to as Database Dynamos.</p>
<p>PDB Sync Loadable Block <blockname> Not defined locally.</p>	<p></p>
<p>PDB Sync Loadable Block <blockname> Not defined on remote node.</p>	<p></p>
<p>PDB Sync Loadable Block Mismatch locally <blockname> version <ver> remote <blockname> version <ver>.</p>	<p></p>
<p>Both SCADAs are active (as displayed in ScadaSyncMonitor, or as indicated by messages in alarm services destinations).</p>	<p>Verify your Ethernet connection being utilized for SCADA Synchronization (preferably this is a dedicated LAN connection).</p> <p>On both SCADAs, in the Task Manager, verify that ScadaSync.exe and ScadaRoleMgr.exe are listed.</p> <p>On both SCADAs, in the SCU, check your Failover configuration, start the ScadaSyncMonitor (ScadaSyncMonitor.exe is found in the iFIX install folder) and check that the transport is configured for the appropriate LAN adapter and the partner's address is correctly defined.</p> <p>Ensure that at least one client is connected to the SCADAs. A SCADA will not switch to Standby if there are no active client connections to its partner, since it cannot tell if the partner's network is OK.</p>
<p>iClient with logical node names cannot connect to a partner SCADA.</p>	<p>Make sure that the iClient is configured properly. Refer to the Configuring iClients section.</p> <p>Make sure the iClient machine can ping the SCADA node(s) using the iFIX node name.</p> <p>Verify the Hosts files are configured correctly on all node links. For more information, refer to the Before You Begin with TCP/IP section in the Setting Up the Environment e-book.</p>
<p>The I/O driver configuration is causing issues. For instance, blocks are going off scan, or question marks appear for data links (the default indic-</p>	<p>Your driver configuration or node configuration (where the driver is installed) could be invalid. Try running each node independently before configuring Enhanced Failover to determine if the drivers are configured differently on each node. They should be configured identically.</p>

<p>ation that there is no data, and is defined in the User Preferences).</p>	
<p>When the active switches to the standby node, the blocks go off scan and you see @@@@ signs or question marks instead of real data. The node fails back to the other node. All blocks are still off scan, after it fails back.</p>	<p>Your standby node is most likely not configured properly. Your driver configuration could be invalid. Try running each node independently before configuring Enhanced Failover to determine if the drivers are configured differently on each node. Make sure that your drivers are configured the same on each node. Validate that both systems run properly alone before reconfiguring Enhanced Failover.</p>
<p>iClient nodes display error message number 1914, every time the active SCADA switches.</p>	<p>This is an expected message if the 1914 error has not been configured to be filtered. When an iClient establishes a connection to an active SCADA Server node in run mode, the iClient starts to read data from that node. When the active SCADA Server node switches to the partner SCADA, the iClient momentarily loses its session with that node, causing this error to appear.</p> <p>You can suppress this error from appearing on screen. For more information on how to suppress this message and others, refer to the Reading Data from iFIX Pictures in iClients section.</p>
<p>Connection Not Established With Node.</p>	<p>When any iClient loses its iFIX networking session with a remote node, this error to appears in alarm service destinations. Check your Ethernet connections.</p>
<p>iFIXNotification dialog displays for an extended length of time.</p>	<p>iFIXNotification dialog displays when iClient is only able to communicate with a standby SCADA node. Check your Ethernet connections being used for iFIX networking.</p>
<p>Standby SCADA displays "Connection Failover: failover attempted" message every minute in alarm services destinations.</p>	<p>This is not a synchronization message. This message indicates that the iFIX networking connection to the Active SCADA has failed. Check the Ethernet connection being used for iFIX networking.</p>
<p>Failover takes a long time.</p>	<p>Adjust the session timers. Refer to the Working with Configurable Session Timers section in the Setting Up the Environment manual for more information.</p>
<p>On iClients, alarms are being lost during failover periods.</p>	<p>Make sure that the Alarm Startup Queue is enabled and that the queue size is large enough to handle the alarms. Refer to the Implementing Alarms and Messages manual for more information on this service.</p>
<p>On iClients, alarms are missing from the summary link or alarms appear and disappear in the alarm summary link.</p>	<p>Make sure that the Alarm Summary Queue on the node is twice as big as it would normally be if the node were not part of a SCADA server failover pair. For example, if you are generating 500 alarms, the Alarm Summary Queue must be set to 1000. Refer to the Implementing Alarms and Messages manual for more information on queue sizes.</p>
<p>You are not seeing any alarms.</p>	<p>Use the Alarm Status Utility (almstat.exe) to check if alarms are coming into the alarm queues and being taken out. To start this utility while iFIX is running, type the following at the command line:</p>

almstat

If this utility verifies there are no alarms coming in or out, then you need to troubleshoot your alarm configuration or cabling. For more information, refer to the [Implementing Alarms and Messages](#) manual.

A View node or iClient connects to a secondary SCADA. The secondary SCADA remains in standby mode, instead of connecting to the primary node. Alarms do not display, and datalinks are not updating on secondary, View, or iClient.

Check the network connections used with iFIX networking. A network cable could be unplugged

After invoking the Database Manager on an iClient (View node), the list of available nodes does not contain the names of the expected SCADA nodes.

Wait until the iFIX network session is established to a redundant SCADA for all the node names to display in the list.

Client applications (such as Workspace) running local on the standby SCADA node do not connect to the active SCADA node.

Client applications running locally on the failover SCADA nodes are dependent on an operational iFIX networking path between the SCADA nodes.

Ensure that after a disruption of the synchronization path followed by a disruption of the iFIX network path that both network paths are once again operational.

When only the synchronization path is restored and the iFIX network path between the SCADAs remains bad, the client applications on the local SCADA can only connect to the local SCADA. In this situation, the client applications on the standby SCADA are not able to “write” to the SCADA node.”

To check the iFIX networking path between the SCADA nodes, run NetHis.EXE on each SCADA node. The partner SCADA node should be listed as an established connection.

Data not visible after a failover ("Database Dynamo configuration mismatch" error).

Run BTKCFG.exe on both SCADAs and compare all installed loadable blocks and the slot for each block. Click on a block in the Configured Database Dynamos column and change the slot number in the box on the bottom right. If another block is assigned to the slot you are trying to move a block to, you will have to go to that block and give it a temporary slot number so you can move the desired block to its correct slot. Once the Database Dynamos are configured identically on both SCADAs, save the configuration and exit BTKCFG. Restart iFIX on both SCADAs. You should now see data no matter which SCADA node is Active.

Troubleshooting Checklist for Enhanced Failover Configuration

If you experience issues with Enhanced Failover and you do not know where to begin, start by asking yourself:

1. Do you understand the architecture of your Enhanced Failover system? If not, review the [What is Enhanced Failover?](#), [What is my SCADA Role?](#), and [Components of Enhanced Failover](#) sections, for starters. Other information is also provided earlier in this e-book.
2. Once you understand the architecture, verify that each SCADA node works independently without Enhanced Failover enabled. For tips, refer to the [Testing Your Enhanced Failover Configuration](#) section.
3. Confirm that you configured the primary and secondary nodes appropriately. Both SCADA computers in the pair should be configured the same way. For a helpful checklist on what to check, refer to the [Preparation Checklist for Enhanced Failover](#) section. Be sure to investigate each and every item in the list. If one SCADA has a different configuration, say the drivers and polling times are different, or the Database Dynamos (loadable blocks) are not loaded in the same slots, or network (NIC) cards are configured slightly differently, it will impact your system.
4. Ensure that the iFIX Enhanced Failover option is enabled on both the primary and secondary SCADAs, that both SCADAs are using the same protocol (TCP or UDP), and that your client nodes are configured properly. For more information, refer to the [Checklist for Enhanced Failover Configuration](#) section.
5. Check the [Limitations of Enhanced Failover](#) section. Is your configuration in compliance?
6. If after all those steps, you believe everything is configured properly, the next step is to investigate what is occurring between the network cards. For instance, are your network cards doing what they are configured to do? In the Windows Task Manager, use the Networking tab to investigate if each adapter is performing appropriately. From the Networking tab, look for:
 - 1-Gigabit-Ethernet cards (or better) dedicated for SCADA-to-SCADA traffic (for a total of two network cards, minimum). For UDP, the dedicated SCADA-to-SCADA network cards should be excluded from the iFIX-to-iFIX network (not enabled for LAN redundancy). If either card is less than 1 Gigabyte-Ethernet, it's not a supported configuration. Also, both network cards must be of the same speed.
 - Does each network card have an Adapter name? Are both cards of the same make and model number, and use the same drivers?
 - What is the network utilization of each card and what is the state of each card? Is it operational? For UDP only, is Jumbo Frames technology used on the dedicated network for Enhanced Failover? (Jumbo Frames technology allows for an Ethernet frame of 9000 MTU for the payload, compared to a frame of 1500 bytes without the Jumbo Frames.) Jumbo Frames technology must be used on the dedicated network for Enhanced Failover.
 - Be aware that network card configuration is one of the top configuration issues. For additional details, refer to the [More Information on Network Card Usage](#) section below.
7. If after all of the network configuration checks, you believe everything is configured properly, the next step is to investigate the networking hardware.
 - Are all network cables and connections properly connected? Are you using a direct connection via a Cat6 crossover cable, without going through any switches, hubs, or routers (for UDP only)?

- Do both Gigabit-Ethernet (or better) cards dedicated for SCADA-to-SCADA traffic have the same make and model number imprinted on the actual card or recorded in the user manual (for UDP only)?
8. Finally, another place to investigate is in the Windows Task Manager, on the Performance tab. What is the physical memory available and system cache? Is your computer performing at the necessary level for Enhanced Failover configurations? Be aware that:
- The wake-up upon receiving a socket or/and request feature must be disabled on the SCADA-to-SCADA network card.
 - SpeedStep® technology is not supported and must not be enabled.
 - Due to limited bandwidth and latency, it is strongly advised that you do not use wireless networking technology in your networking solution.
 - The power save settings on your computers and dedicated network card (NIC) must be disabled. Do not use any power setting features that affect CPU clock speed.

More Information on Network Card Usage

Network cards (NICs) may be used for a multitude of tasks within iFIX. The following tasks may each use a separate NIC:

- Driver I/O to PLC connectivity
- SCADA synchronization
- iFIX Client connectivity
- Non-iFIX activity such as company network access

It is important to understand the use of all the network cards on the PC. It is possible to use a particular NIC card for multiple uses by design. It is also possible to inadvertently apply the NIC card to the incorrect uses causing undesirable results.

Tips for working with NICs

- Whenever a new NIC is installed, re-check all configuration items that use the NIC card. The NIC slot/order or IP address could require changes.
- It is desirable that both machines have the same NIC cards and NIC order (slot).
- Some drivers use a NIC IP Address or slot/order number. Communication may cease after installing another NIC card since slot/order may change. The slots should be in the same order on both nodes.
- When copying a Driver Configuration file from one node to another, the slot/order or IP Address may need to be changed on the PC receiving the file.
- It is required to perform SCADA synchronization on a dedicated NIC (for UDP only). It is recommended to have an identical NIC on both the Primary and Secondary SCADA.
- SCADA synchronization should be tested with the “default” NIC settings. Any advanced setting changes should be mirrored on the partner SCADA.
- SCADA synchronization can optionally include a second NIC (as a backup to the first). Often this can be the same NIC as the iFIX Client connection.

- Typically, iFIX Client connectivity uses a different NIC than SCADA synchronization. Only ONE NIC should be enabled in the iFIX Networking configuration (unless LAN Redundancy is used).

Tools for Troubleshooting

The following tools can be used to assist you in troubleshooting Enhanced Failover features in iFIX:

- Windows Task Manager, Networking tab – to see if your networking cards are doing what they are configured to do, and that each adapter is performing appropriately.
- Windows Task Manager, Processes tab – to verify that ScadaSync.exe and ScadaRoleMgr.exe are listed as running on both SCADAs.
- [Log Files](#) – to investigate what error messages may be occurring.
- [Error Messages](#) – to get more information about errors that you find in the logs.
- [Mission Control](#) – to view the status of the Scan, Alarm, and Control (SAC) program and whether blocks are being processed.
- [SCADA Sync Monitor](#) – to display runtime information about the primary and secondary SCADA Servers.
- [Runtime Information Fields](#) – to display additional runtime information available about your primary and secondary SCADA Servers, that does not already display in the SCADA Sync Monitor. These fields can be added to pictures or EDA applications. For example, these fields allow you to access more information about your data sync transports than you can in the SCADA Sync Monitor.
- [NetDiag](#) – to check network communication, particularly if you are using Enhanced Failover with LAN Redundancy.

Log Files for Enhanced Failover

For Enhanced Failover, there are two log files available for troubleshooting:

- **SCADASync.log** – for reviewing log messages that occur during the SCADA synchronization process.
- **ScadaRoleMgr.log** – for debugging the active to standby role switch.

Both of these files can be found in your iFIX LOCAL directory. If you installed iFIX to the default location, this directory location is: C:\Program Files (x86)\Proficy\iFIX\LOCAL.

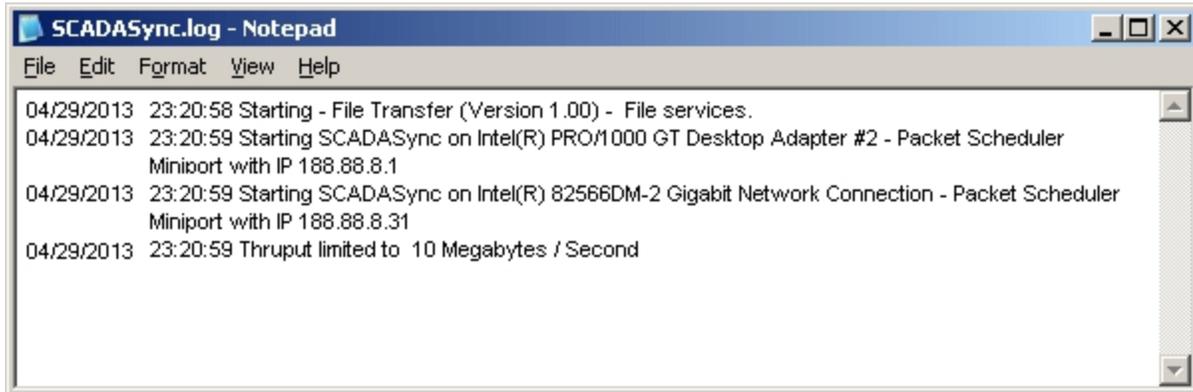
TIPS:

- The SCADA Sync Monitor (SCADASyncMonitor.exe) found in your iFIX install folder can be used to view the information that appears in these logs.
- You can configure whether the SCADASync.log file is refreshed on iFIX startup (so that it does not get overwritten) by using the SCADASync.ini file's DeleteOnStartup key. For more information, refer to the [Customizing the Synchronization Process with SCADASync.ini](#) section.
- By default, debugging messages seen in the Debug Log page of SCADA Sync Monitor are not sent to the SCADASync.log file. For details on how to change the default behavior, refer to the [Customizing the Synchronization Process with SCADASync.ini](#) section.

- Other logs that are not specific to Enhanced Failover, but may also be helpful for reviewing system activity include the iFIX event (.EVT) file, usually found in C:\Program Files (x86)\Proficy\iFIX\ALM folder, and iFIX alarm destinations, such as the Alarm History window, which you can access from the iFIX WorkSpace.

SCADASync.log

The following figure shows an example of the SCADASync.log file with some messages displaying.



Adding the following lines to the SCADASync.ini file causes the SCADASync.log file to be preserved on startup:

```
[LogFile]
DeleteOnStartup=0
```

Adding the following lines to the SCADASync.ini file causes the SCADASync.log file to be deleted on startup:

```
[LogFile]
DeleteOnStartup=1
```

By default, the SCADASync.log file is deleted when iFIX is started.

ScadaRoleMgr.log

To enable logging to the ScadaRoleMgr.log file, add the Logging parameter (/L) to the ScadaRoleMgr.exe command line in the FIX.INI file. The log file will append new entries, even after restarting iFIX, until it reaches its maximum size and then creates a new log file. Older log files will be renamed, with the oldest one being deleted if the maximum number of files to retain has been reached.

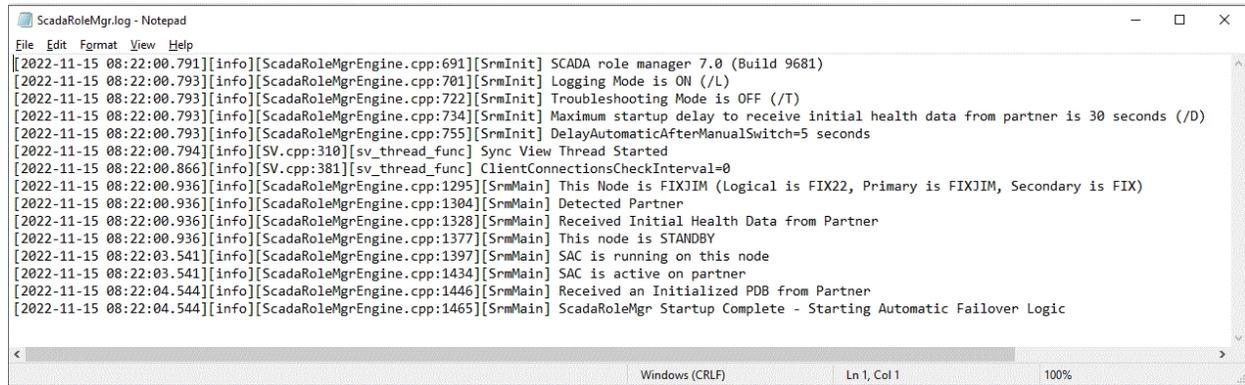
```
[PARTNER SCADA]
...
RUN=%SCADAROLEMGR.EXE /L
...
```

Command Line Parameters

- **/L** - Enables logging to the ScadaRoleMgr.log file.
- **/Sxxx** - Specifies the maximum size of the log file, in MB. Valid entries are from 1 to 100 (default is 5 MB).
- **/Nxx** - Specifies the maximum number of log files to keep. Valid entries are from 1 to 10 (default is 5).

NOTE: In iFIX 2023, the /A (append to log file) command line parameter has been deprecated. The log file always appends now, so that no information is lost when iFIX restarts.

The following figure shows an example of the ScadaRoleMgr.log file with some messages displaying.



System Messages for Enhanced Failover Activity

Examples of system messages generated for Enhanced Failover (that can appear in the SCADARoleMgr.log file) include:

- When the SCADA node is transitioning into the Active state. The message contains the reason for the state transition
- When the SCADA node is transitioning into the Standby state. The message contains the reason for the state transition
- When the partner SCADA goes offline.
- When the partner SCADA comes back online.

Error Messages for Enhanced Failover in iFIX

If a network problem exists that prevents network sessions from establishing or causes network sessions to be terminated due to the SCADA synchronization process, one of the error codes listed in the following table may appear in the SCADA Sync Monitor, the SCADASync.log, or in the iFIX Alarm History program.

Error Codes

Error Message	Description
Node.Tag.Field Connection Not Established With Node	<p>When an iClient establishes a connection to an active SCADA Server node, it starts to read data from that node. When the active SCADA Server node becomes unavailable, the iClient loses its session with that node, causing this error to appear.</p> <p>This error appears in the iFIX event log. For more information on how to suppress this message and others, refer to the Reading Data from iFIX Pictures in iClients section.</p>

Sending File <name> to Partner Node	This message is informational. It indicates that file synchronization has occurred – a file is sent (copied) from one SCADA node to the other. The active node is sending the file; the standby node is receiving the file.
Unable to rename <name1> to <name2>	When iFIX performs file synchronization, it creates a temporary file name on the destination node. After the file is created on the destination node, iFIX removes the temporary file. If iFIX cannot remove the temporary file, this error message occurs. For example, if someone had the file open or if the file was locked this message could display.
File <name> cannot be removed	When iFIX performs file synchronization, it creates a temporary file name on the destination node. After the file is created on the destination node, iFIX removes the temporary file. If iFIX cannot remove the temporary file, this error message occurs. For example, if someone had the file open or if the file was locked this message could display.
File <name> Access Denied	This error occurs if SCADASync needed to copy a file and could not during synchronization.
Finished Sending File %s to Partner Node	This message is informational. If iFIX sends a file, this message indicates when it is received on the partner node.
File Synchronization Transfer Error	This error indicates that part of a file came across from the active node and the standby was not able to validate it.
File Change Notification Error	This error indicates a problem with the file synchronization. In this instance, part of a file came over the network, and something went wrong. For example, the disk was full, or the file was write-protected. Look at the SCADA Sync Monitor for clues. For more information, refer to the Enhanced Failover Diagnostics with the SCADA Sync Monitor section.
Global Section Sync - Bad message	This error indicates that part of the process database came across the network connection improperly. If iFIX cannot validate the message, it is not used. This message is not a typical error, and rarely displays. iFIX will automatically recover from this message.
UDP Socket error <number>	This error occurs if a network card does not initialize (for example, if the network cable is not plugged in).
Thruput limited to <number> Megabytes / Second	This message is informational. It is a network-throttling message.
UDP Buffer allocation FAILED <text message>	This error indicates that iFIX could not allocate memory for a buffer. Call GE Support if this message recurs. This message

	is not a typical error, and rarely displays.
TCP Buffer allocation FAILED <text message>	This error indicates that iFIX could not allocate memory for a buffer. Call GE Support if this message recurs. This message is not a typical error, and rarely displays.
File <name> Received from Partner Node	This message is informational. It indicates that the active node's saved file was copied and added to the standby node.
PDB Sync Loadable Block <blockname> Not defined locally	This error indicates the loadable block configuration on one or both SCADA nodes does not match. Loadable block configuration must be the same on both primary and secondary nodes.
PDB Sync Loadable Block <blockname> Not defined on remote node	This error indicates that there are two different versions of a loadable block installed. Loadable block configuration must be the same on both primary and secondary nodes. Ensure that loadable block DLLs (BTK*.*) are the same on both nodes.
PDB Sync Loadable Block Mismatch locally <blockname> version <ver> remote <blockname> version <ver>	This error indicates the loadable block configuration on one or both SCADA nodes is not configured properly. Loadable block configuration must be the same on both primary and secondary nodes.
PDB Sync Database Block versions don't match for block type <blockname>	This error occurs if iFIX detected a difference in the database versions on the primary and secondary nodes. Process databases must be the same version of iFIX. For example, you cannot have one database be 5.5 and the other is at 5.8. Both SCADA nodes must have the same version of iFIX installed.
Starting SCADASync on <node> with IP <IP>	This message is informational. It indicates that the SCADA synchronization process started on a specified IP address.
SCADA Sync Communication Lost with <IP>	This message is informational. It indicates the SCADA-to-SCADA communication for synchronization has been lost.
SCADA Sync Communication Established with <IP>	This message is informational. It indicates the SCADA-to-SCADA communication for synchronization has been established.
SCADA Failover feature is not enabled in the license for this node	This error indicates that your key does not support the Enhanced Failover feature. Check your key in the License Viewer, and contact GE to purchase an upgrade or replace a defective key. You must purchase the additional Enhanced Failover option (SCADA Failover) for all SCADA nodes if you plan to use SCADA Failover in iFIX.
ScadaSync.exe is not running. Local fields show last known values.	This error indicates that ScadaSync.exe is not running on the SCADA node.
Protocol Mismatch!!! Partner node is configured to use a different protocol for synchronization. No synchronization will occur! Please ensure that the Data Sync Protocol setting	This error indicates that the SCADA nodes are configured to use different protocols (UDP or TCP) and will not be able to synchronize the database. The protocol for each SCADA must match in the SCU files.

matches on partner node.	
Error [-1073479673] adding unsolicited tag [LogicalNodeName.TagName.F_CV] on secondary iFix SCADA server.	<p>This error occurs because the OPC Collector does not fully support logical node names for enhanced failover SCADA servers. When a secondary SCADA server starts up without its primary SCADA server running iFix, it takes time for the secondary iFix SCADA server to declare itself as the active SCADA. At this moment, the OPC collector starts and tries to add tags into the OPC Server with the logical node name in the tag name. Since the secondary SCADA's logical node name is unrecognized, the OPC Collector rejects the request.</p> <p>To avoid this error, it is recommended to collect data from iFix failover SCADA servers using the iFix collector (not the OPC Collector).</p>
ERROR: 'Number: -2147352567 (80020009) Connection Failover Has Not Been Enabled on this Node'.	<p>This error will occur if the wrong node name is used when trying to manually failover a node using the NSD tag. Check the System Configuration Utility (SCU) to ensure node names, and logical node names, are setup correctly. It is recommended that logical node names be unique from any other SCADA's physical node name.</p>
Cannot write to Standby node.	<p>This error, generated from the redundant SCADA, indicates that you are trying to write to the Standby SCADA when WSACTASK is paused and not running on the non-active node.</p> <p>For the graphic that is generating the error, ensure the database tag is using the LogicalNodename that is shared between the redundant SCADA pair. Also, the error will not occur if you do not write directly to the Standby SCADA.</p>
Error 1762 – “Process Database Has Been Modified”.	<p>This problem typically occurs when the application's ScadaRoleManager and AlarmODBC fail to map to SYNCLDBA. This mapping fails because at the time of launch, SYNCLDBA was not yet fully loaded into global memory.</p> <p>Move the loading order of SYNCLDBA.dll within the FIX.INI file on both failover nodes and restart iFix on both nodes. This ensures that SYNCLDBA is loaded into global memory before apps such as ScadaRoleManager and AlarmODBC are launched.</p> <p>SYNCLDBA should be added (moved) to the [SCADA] node section after LDBA.dll. Please note that the ordering is important.</p> <p>SYNCLDBA should be removed from the [PARTNER_SCADA] node - using this example:</p> <pre>[SCADA] DLL=BTK_ETR.DLL</pre>

	<pre> RUN=BTKINIT.EXE BTK_ETR 40 RUN=DBCVT.EXE DLL=LDBA.DLL DLL=ALMDATA.DLL DLL=SYNCLDBA.dll RUN=AREAASTG.EXE RUN=%FIXTOHIST.EXE [PARTNER SCADA] RUN=%SCADASYNC.EXE RUN=%SCADAROLEMGR.EXE /L ;DLL=SYNCLDBA.dll </pre>
File service Retrying Message <file name>	Indicates there was an error or timeout while sending a file to the Standby SCADA, and that the operation is being retried.
File service failed file transfer - <file name>	Indicates that the specified file failed to be sent to the Standby SCADA.
Unable to retrieve partner's protocol, perhaps not running yet. Error = <number>	When iFIX starts on a SCADA with Enhanced Failover enabled, ScadaSync.exe tries to determine the protocol (TCP or UDP) its partner is configured to use. This message indicates that the partner node cannot be reached yet. This commonly occurs because iFIX is not yet fully started on the partner SCADA. The error number indicates the iFIX error that was encountered. An error of 1914 means "Connection NOT established with node".
Partner's protocol has been determined and matches this SCADA's protocol	This message is informational. It indicates that the partner SCADA has been confirmed to be configured to use the same protocol (TCP or UDP) as this SCADA.

Monitoring SAC in Mission Control

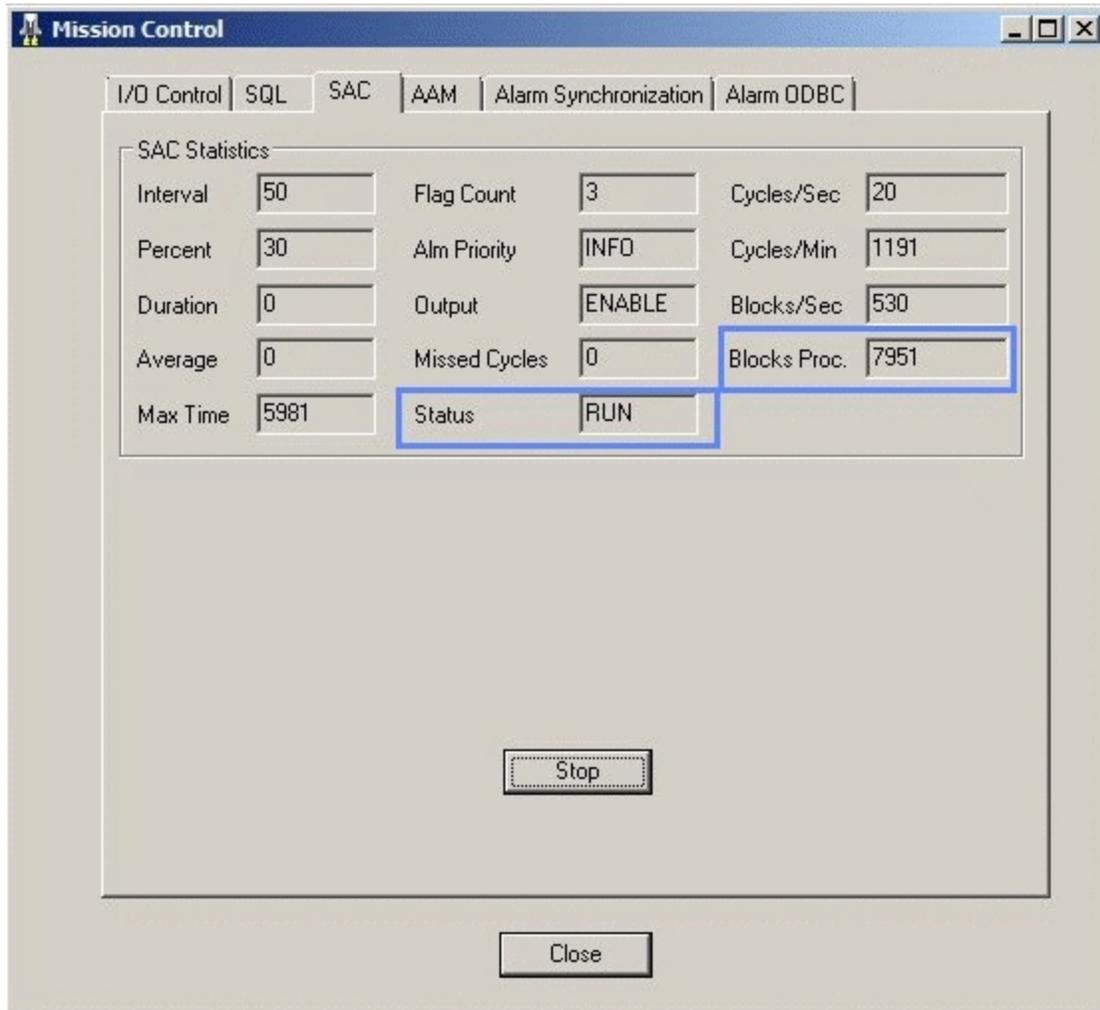
When using the Enhanced Failover feature, you can use the SAC tab in the Mission Control application to view the status of the Scan, Alarm, and Control (SAC) program. The SAC program retrieves process information from an I/O driver or OPC server. Using the data it receives, SAC updates blocks in the database and processes alarms. SAC also writes set point values from the database to a control device. SAC runs independently of the I/O driver or OPC server.

When reviewing the SAC tab in Mission Control, the Status field indicates whether SAC is in one of the following modes:

- Run
- Standby
- Stopped

The following figure shows an example of SAC in Run mode on a primary SCADA Server. The Status field is set to Run, and is highlighted in the following figure. Another field that you may want to monitor is the Blocks Proc. field, which is also highlighted in the following figure. In an Active (running) SCADA, the Blocks Proc. field is continually increasing. If this number stops updating or the Status is stopped, there may be a problem with SAC.

IMPORTANT: Starting and stopping SAC in an Enhanced Failover environment is not recommended. Doing so may lead to an unexpected failover and role change.



Mission Control, with SAC Tab Selected

TIP: You can view more information about SAC in the Health screen of the SCADA Sync Monitor. For more information, refer to the [Diagnostics with the SCADA Sync Monitor](#) section.

NOTE: The fields in the Alarm Synchronization tab in Mission control are unavailable when Enhanced Failover is configured. Use the [SCADA Sync Monitor](#) to view information regarding the synchronization process instead.

More Information on Drivers and SAC

SAC, when running, receives a write request as a result of a user action or internally via another block. SAC processes the request and pushes the request to the driver. It is possible that at any given time you would have a number of pending writes in the driver queue. If the driver is optimized, the goal would be to have the writes get processed very quickly.

NOTE: Configuring the driver to perform tasks as “fast” as possible can be detrimental. Drivers should be optimized based on the actual throughput restrictions and PLC responsiveness.

The speed at which writes in the queue get processed depends primarily on the driver technology (Serial vs. Ethernet) and the driver configuration (whether or not the driver has been properly setup or optimized).

It is important to note that pending writes in the queue do not necessarily indicate issues. It is possible for a driver to have pending writes as long as the count does not continue to permanently grow. It is also possible for a driver to receive thousands of writes, have the queue count increase briefly, and then come back down, ideally close to 0.

The following two examples describe how driver queues and Enhanced Failover are independent of each other.

Example 1: Drivers and SAC

Consider this example: the driver is in the running state on both SCADAs. The driver is very busy and has an average 10 pending writes in the queue. When the “failover” happens, the current active node switches from Active to Standby. SAC will be “paused” at this time.

When the Active node becomes the Standby, the driver is still running. The writes will still be processed as fast as the driver can handle them. The driver remains independent of SAC. So while SAC is paused and no longer processing, the driver will continue to process anything in the write queue. If there are 10 pending writes the driver will write them to the device. If there are no communication errors to be reported, the writes will be successful.

One possible side effect is if you have a very quick driver, the writes will likely be done by the time the second Node is promoted to Active, but if you are using a driver connected over a serial line, then it is possible that the two drivers will attempt writes at the same time against the same IO on the PLC at least for the duration needed for the first driver to empty its write queue.

Example 2: Drivers and SAC

The driver is in the running state only on the Active SCADA (using script). When the “failover” occurs programmatically, one driver is stopped while the other driver is started.

When a driver is stopped either programmatically or manually, the write queue will get flushed. Therefore, if you had 10 pending writes, then stop the driver, you just lost 10 writes and the writes will never take place.

It is important to understand that this is not a driver issue. Understanding a driver’s capability, testing, and optimizing the driver based on actual throughput restrictions and PLC responsiveness is the best way to ensure desired driver performance.

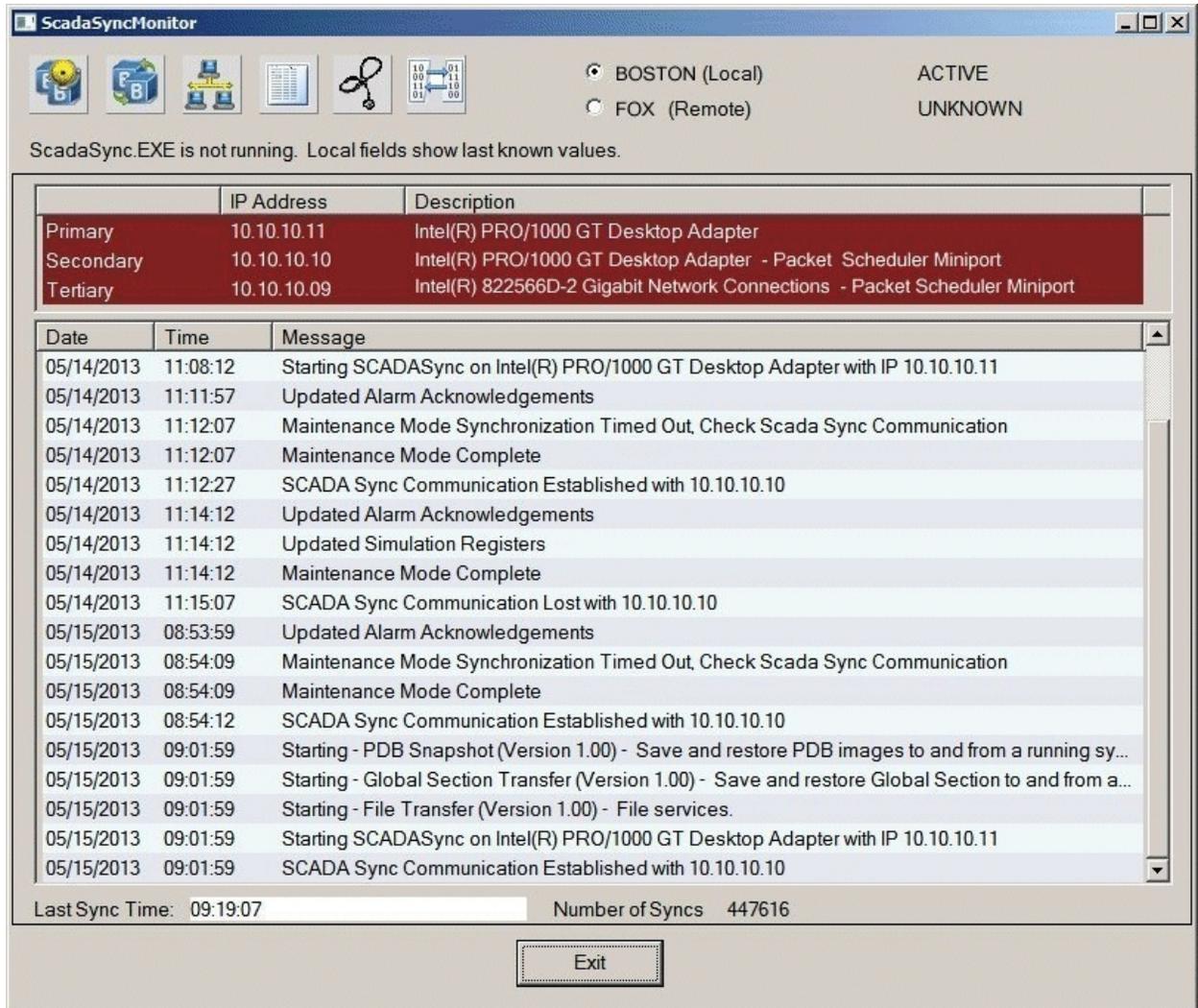
Enhanced Failover Diagnostics with the SCADA Sync Monitor

The SCADA Sync Monitor displays information about the primary and secondary SCADA Servers. You can use it to view diagnostic information about your Enhanced Failover configuration, or for troubleshooting issues with your Enhanced Failover configuration.

The SCADA Sync Monitor displays whether the selected SCADA is in active or standby state, shows how often database synchronizations occur, whether the database synchronization networks are in good communication, debug log messages that occur during synchronization of the databases, SAC information, and the overall system health on both nodes. You can view the status and information from either SCADA by selecting either the local or partner SCADA.

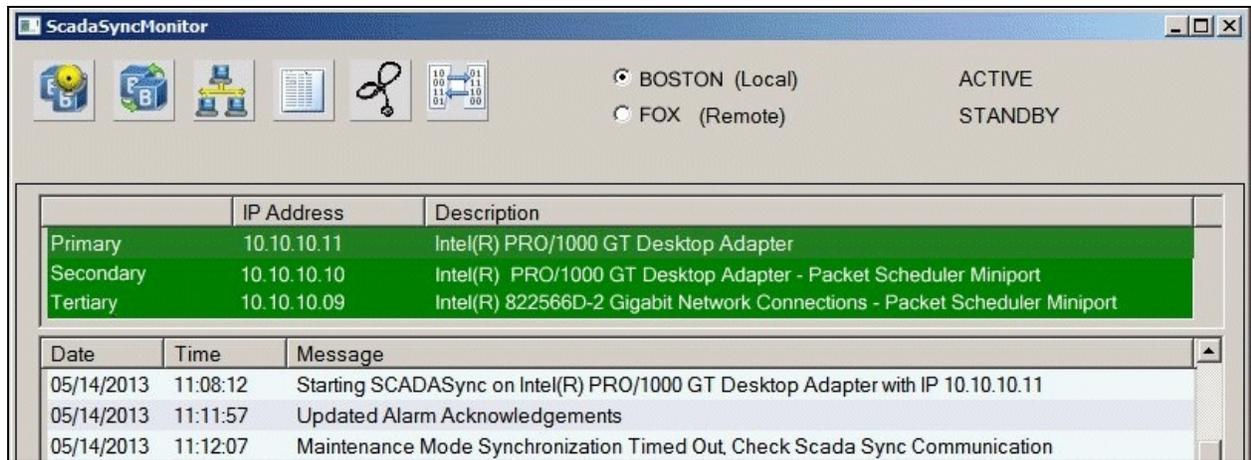
The following figures illustrate the ScadaSyncMonitor dialog box. The top section of this dialog box contains six SCADA Sync Monitor toolbar buttons. To the right of the toolbar buttons, there are two option buttons, which allow you to select either the local or partner SCADA node. The status of both nodes displays to the right of the buttons.

- When ScadaSync.exe is not running, an alert message under the toolbar indicates that "ScadaSync.exe is not running. Local fields show last known values." Below this alert message, the Primary, Secondary, Tertiary IP Address and Descriptions area displays white text in a red area.



ScadaSync.exe Not Running

- When ScadaSync.exe is running, there is no alert message under the toolbar. The Primary, Secondary, Tertiary IP Address and Description area displays in white text in a green area to indicate that the communication networks are all in good health. The partner nodes are communicating successfully with each other, and that all three networks are available.



ScadaSync.exe Running

► **To open the SCADA Sync Monitor:**

1. Open Windows Explorer and locate the iFIX install folder. By default, this folder is: C:\Program Files (x86)\Proficy\iFIX.
2. Double-click the ScadaSyncMonitor.exe file. The SCADA Sync Monitor dialog box displays.
3. Click the button in the toolbar for the information that you want to display. Also, select either the local or partner node using the radio buttons. For information on the toolbar buttons, refer to the table in the following section.

NOTE: • When starting your SCADA pair the connection state flow displayed in SCADA Sync Monitor may be different based on the protocol used. When using the TCP protocol, both SCADAs may spend a short time in the Active state until the TCP connection is established and they negotiate their respective roles. Also, be aware that it takes longer for SCADA Sync to initially get to an Active / Standby state with TCP than UDP.

Toolbar for SCADA Sync Monitor

The following table describes the functions of each of the icons in the toolbar for the SCADA Sync Monitor. You can use the drop-down list to view the active or standby node.

Icon	Function
	Overview of the SCADA Node Synchronization History
	PDB Synchronization Status
	Communication Status
	Debug Log for Troubleshooting
	Overall System Health



Global Memory Synchronization Status (Internal Troubleshooting Tool, for Customer Support and Development)

Overview of the SCADA Node Synchronization History



The Overall Partner Status screen in the SCADA Sync Monitor allows you to view whether the primary and secondary SCADA Server pair are communicating and view event log messages pertaining to Enhanced Failover.

The following table describes the fields that appear in this screen.

Field or Area	Description
Primary, Secondary, Tertiary Area	Provides the IP address and hardware descriptions of Primary, Secondary, Tertiary networks for Enhanced Failover. These networks are defined in the Data Sync Transport Options dialog box in the SCU (accessed from the SCADA Configuration dialog box). When communication is good, the enabled adapter appears green. If communication is bad, the enabled adapter is red. If communication is not configured, no additional color appears. If the network card failed to initialize (for instance, if the network cable is not plugged in), no additional color appears.
Message List	Displays the last 64 messages related to partner SCADA communications including their date and time. If you need to review messages older than the last 64, you can review the <code>sca-dasync.log</code> file, in your iFIX LOCAL directory. If you installed iFIX to the default location, this directory location is: <code>C:\Program Files (x86)\Proficy\iFIX\LOCAL</code> .
Last Sync Time	The last time the PDB was sent to the partner node.
Number of Syncs	The number of synchronizations that occurred since you started iFIX.

Database Synchronization Status



The Database Synchronization screen in the SCADA Sync Monitor displays information on the database synchronization between the active and standby nodes. For instance, by looking at this screen you can determine how fast the database updates are occurring between the active and standby nodes.

The following table describes the fields that appear in this screen.

Field or Area	Description
Last Time Sent	The time the SCADA last sent a successful synchronization.
Last Date Sent	The date the SCADA last sent a successful synchronization.

Seconds Between Synchronizations	<p>The total number of seconds it takes to synchronize the active database with the standby database, from beginning to end.</p> <p>The value of this field is always greater than the "Duration of Last PDB Synchronization" field.</p> <p>The Seconds Between Synchronizations field is perhaps the most valuable field to monitor on this screen.</p>
Duration of Last PDB Synchronization	The total number of seconds it took to send the synchronized data from the active database to the standby database, over the active network connection.
Number of Synchronizations Sent	Total number of synchronizations sent since iFIX started and a successful synchronization communication occurred. The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.
Number of Synchronizations Received	Total number of synchronizations received since iFIX started and a successful synchronization communication occurred. The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.
Number of PDB Blocks PDB Size in Bytes	<p>The number of database blocks included in the synchronization.</p> <p>The size of the entire iFIX process database that is being synchronized, in bytes.</p>
Last Sending Error	The number of the last error message that appeared.
Enable/Disable Maintenance Mode	<p>This button is available only on the primary node. It is not displayed on the secondary node.</p> <p>Maintenance Mode allows you to temporarily suspend synchronization between the two SCADA nodes, so that you can make changes to your database while the SAC is still running.</p> <p>When you finish making your changes, click the Disable Maintenance Mode button to become the active node; your changes will now be synchronized with the standby node. For more information, refer to the Maintenance Mode section.</p> <p>NOTE: Using maintenance mode forces both SCADAs in a pair to active status. This will place increased load on your PLC network, as the I/O drivers on both nodes are polling at the active rate. Both nodes will generate alarms.</p>

Communication Status



The Communication Status screen in the SCADA Sync Monitor displays information about the bytes sent and received on each network transport.

The following table describes the fields that appear in this screen.

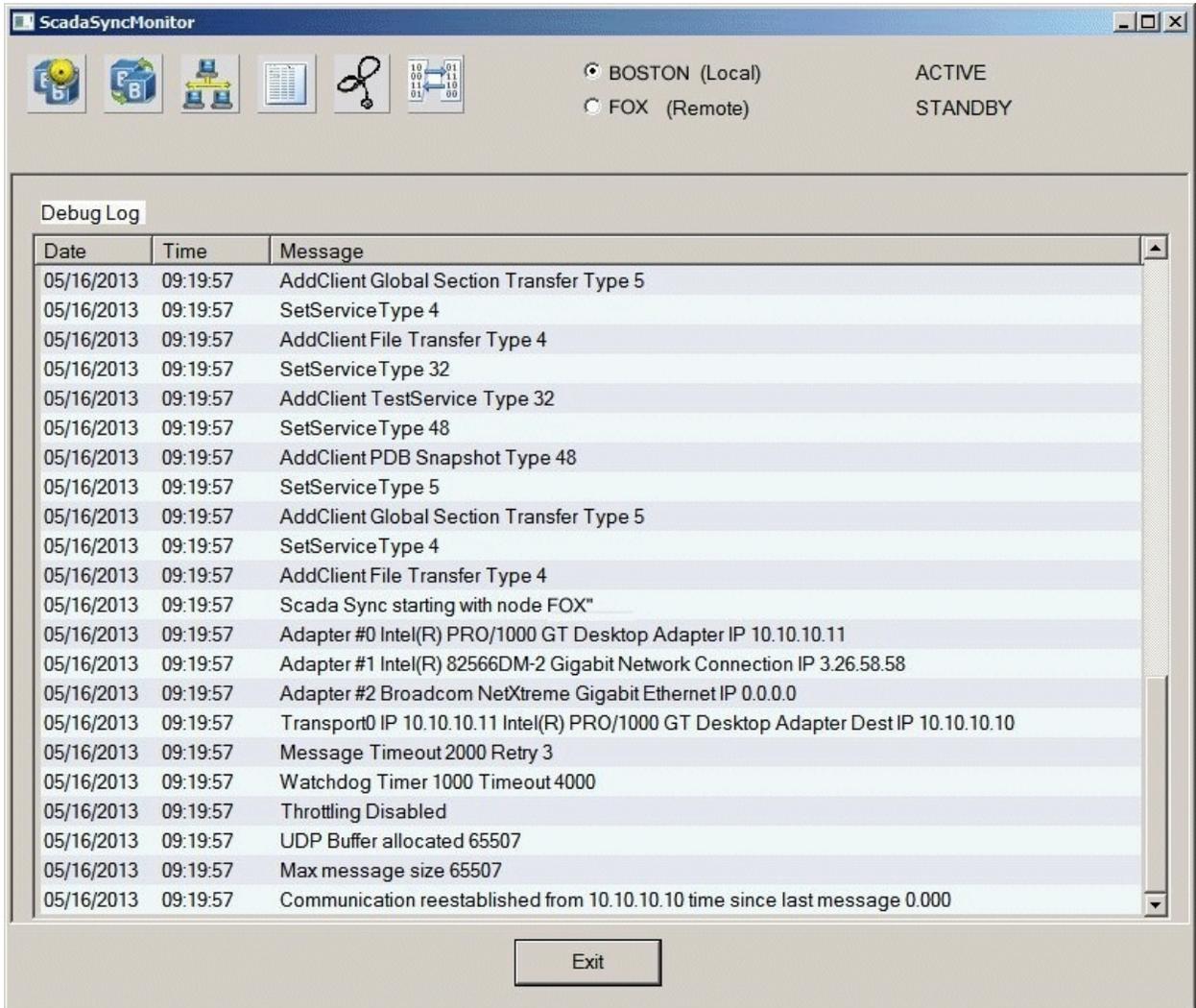
Field or Area	Description
Transport 1, 2, or 3	Displays the name of the network (primary, secondary, or tertiary). This name is configured in the Data Sync Transport dialog box in the SCU. You access this dialog box from the SCADA Configuration dialog box.
Status	Displays the status of the network: Good, Bad, or Unknown (disabled).
Bytes Sent	Displays the total number of bytes sent on the network. The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.
Bytes Received	Displays the total number of bytes received on the network. If the value for the Bytes Received field is incrementing, that indicates good health of the network. The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.
Bytes per Second	Displays the number of bytes processed per second on the network.
Average ACK Time (Seconds)	Displays the average time it takes the partner SCADA to acknowledge the communication status on the network.
Watchdog Count	Displays the number of times that the watchdog timer has checked the network connection between the primary and secondary SCADA nodes. Every time the watchdog updates, it is assumed that the connection is active. If after some period of time the primary network does not receive a watchdog update from the partner SCADA Server, the connection is considered not running and the Watchdog times out. The Watchdog Timeout field is configured in the Timers area of the Data Sync Transport dialog box in the SCU. You access this dialog box from the SCADA Configuration dialog box.

Debug Log for Troubleshooting



The Debug Log screen in the SCADA Sync Monitor displays detailed debug messages that occur during the SCADA synchronization process.

The Debug Log screen displays debugging information. The following figure shows an example of these debug messages in the SCADA Sync Monitor. This screen is intended for use by GE Support and Development only.



Overall System Health



The Overall System Health screen in the SCADA Sync Monitor displays the general health of your local and remote SCADA pair.

The following table describes the fields that appear in this screen.

Field or Area	Description
iFIX Version	The version of iFIX running on your local and remote nodes.
Node Status	The status of iFIX running on the local and remote nodes: ACTIVE, STANDBY, UNKNOWN.

SAC Running	The status indicating whether the Scan, Alarm, and Control (SAC) program is Running or Stopped.
SAC Active	The status indicating whether SAC is communicating between the active and standby nodes. Use this field to determine the Enhanced Failover state of the local and remote nodes: ACTIVE or STANDBY.
SAC Tick	The number of times SAC sent and/or received data.
SAC Alive	The status indicating whether SAC is running (1=Yes, 0=No).
Available Memory	The available memory, in bytes, on your local and remote nodes.
Total Memory	The total memory, in bytes, on your local and remote nodes. Use this field along with the "Available System Disk Space" and "Available Memory" fields to troubleshoot disk space errors.
Available System Disk Space	The available system disk memory, in bytes, on your local and remote nodes. Use this field along with the "Total Memory" and "Available Memory" fields to troubleshoot disk space errors.
Available LocPath Disk Space	If the available disk space is zero, it causes a failover. The available local path memory, in bytes, on your local and remote nodes.
Physical Node	If the available disk space is zero, it causes a failover. The iFIX node name.
Logical Node	The logical node name for the SCADA pair. The logical node name represents a primary and standby SCADA pair. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU.
Primary Node	The primary node name. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU.
Secondary Node	The secondary node name. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU.

Global Memory Synchronization Status



The Global Memory Synchronization Status screen in the SCADA Sync Monitor displays internal troubleshooting information for Customer Support and Development.

This screen is for internal purposes only.

Runtime Information Fields for Enhanced Failover

The runtime information fields for Enhanced Failover reside within the SCADASync tags (also known as Enhanced Failover tags) on SCADA nodes configured for Enhanced Failover. These fields are very helpful for troubleshooting your Enhanced Failover configuration.

If you do not have an iFIX license on your computer, you will not be able to access the SCADASync tags or fields. This is because in Demo mode, iFIX does not allow you to enable Enhanced Failover. You must have a license on your computer that supports Enhanced Failover in order to display the SCADASync information within iFIX. SCADASync tags and fields are not supported in iFIX Demo mode.

What are SCADASync Tags?

SCADASync tags contain diagnostic and network information pertaining to your Enhanced Failover configurations. These tags are designated solely for Enhanced Failover and are *not* database blocks. SCADASync tags are special tags residing on the SCADA nodes associated with your Enhanced Failover configuration. These tags include Enhanced Failover specific information such as the name of the currently active node, whether the Primary node is in Maintenance Mode, the logical SCADA name, the failover status, and so on. SCADASync tags and field names can be inserted into an iFIX picture as a datalink, for instance.

How to Use and View SCADASync Tags in iFIX

You can use SCADASync tags in the iFIX WorkSpace or EDA-based applications. To view SCADASync tags in the iFIX WorkSpace, you must first enable Enhanced Failover in the SCU (in the SCADA Configuration dialog box) on the SCADA nodes. In this same dialog box, to fully configure Enhanced Failover, you need to set your Primary and Secondary nodes, and Data Sync Transports. For more on Enhanced Failover configuration, refer to the [Configuring a SCADA Server Pair for Enhanced Failover](#) section

From within an iFIX picture, you can view the SCADASync tag using a datalink. It is important to use the **physical** node name, not the logical node name of the SCADA node in the datalink. Refer to the [Reading Data in iFix Pictures on iClients](#) section for more information about physical and logical node names.

There are two SCADASync tags:

- SCADASync[0] refers to the node specified in the datalink.
- SCADASync[1] refers to the partner of the node specified in the datalink.

SCADASync[0]

SCADASync[0] refers to the node specified in the datalink. For example, say you wanted to enter a data source that allows you to force the primary node into Maintenance Mode. In the datalink, you could enter a data source like this:

```
Fix32.PrimaryPhysicalNodeName.SCADASync[0].A_MAINTENANCEMODE
```

In this example, you would replace PrimaryPhysicalNodeName with the physical name of the primary SCADA node as configured in the SCU (the Local Node Name in the Local Startup Definition dialog box). Since, it is an A_ tag, a True or False entry appears in your picture in run mode (as opposed to the F_ tag which displays a 1 or a 0).

SCADASync[1]

SCADASync[1] refers to the partner of the node specified in the datalink. For example, say you want to determine what remaining disk space is available on the secondary SCADA node. You could enter a data source like the following in your picture.

```
Fix32.PrimaryPhysicalNodeName.SCADASync[1].E_SYSTEMDISK
```

This data source is equivalent:

```
Fix32.SecondaryPhysicalNodeName.SCADASync[0].E_SYSTEMDISK
```

In these examples, you would replace PrimaryPhysicalNodeName or SecondaryPhysicalNodeName with the physical names of the primary and secondary SCADA nodes as configured in the SCU (in the Local Node Name in the Local Startup Definition dialog box). Since, it's an E_ tag, a value of up to 40 whole number digits and 16 decimal digits can display in run mode to describe the available system disk space left on your Windows system disk drive.

Field Descriptions

The following table lists the SCADASync fields that are available for use with the Enhanced Failover feature.

SCADASync Fields

Field Name	Description
A_AVAILMEM E_AVAILMEM	The available memory, in bytes, on the specified node. Use this field along with the "A/E_SYSTEMDISK" and "A/E_TOTALMEM" fields to troubleshoot disk space errors. A_AVAILMEM represents a whole number, restricted only by the number of characters you select when you add the field to your picture. E_AVAILMEM represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.
A_AVEPDBACK E_AVEPDBACK F_AVEPDBACK	The average time, in seconds, that it took for the last database synchronization. A_AVEPDBACK represents a whole number, restricted only by the number of characters you select when you add the field to your picture. E_AVEPDBACK represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing. F_AVEPDBACK represents a floating point value can be displayed in your picture.
A_IFIXVERSION	The version of iFIX running on the node you specify. For example, if a Primary node referencing this tag was running iFIX

	5.1, Fix32.PrimaryNode.SCADASync[0].A_IFIXVERSION, then 5.1.6846 would display in run mode.
A_LASTACKTIME E_LASTACKTIME	The last time a network handshaking acknowledgement was sent from the partner node. This timestamp is based on the local regional settings from the computer receiving the acknowledgement.
A_LASTMSG[0-63]	<p>Displays any of the last 64 messages related to partner SCADA communications. Each message includes a timestamp. If you do not specify an index number, the A_LASTMSG field represents the most current message in the log. However, if you want to identify a specific message number (for instance, the message before the most recent one in the list – the second to last message), you would use the field: A_LASTMSG[1], since the index starts at 0.</p> <p>0 is the last message in the queue displayed in the SCADA Sync Monitor's message list, while 63 is the first message in the queue. Once 64 messages are reached, the queue resets. For more information, refer to the Overview of the SCADA Node Synchronization History section.</p> <p>If you need to review messages older than the last 64, you can review the SCADASync .log file, in your iFIX LOCAL directory. If you installed iFIX to the default location, this directory location is: C:\Program Files (x86)\Proficy\iFIX\LOCAL.</p>
A_LOCPATHDISK E_LOCPATHDISK	<p>The available disk space where iFIX is installed, in bytes. If the available disk space is zero, it causes a failover.</p> <p>A_LOCPATHDISK represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_LOCPATHDISK represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_LOGICALNODE	The logical node name for the SCADA pair. The logical node name represents both the active and standby SCADA pair. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU of the specified node.
A_MAINTENANCEMODE F_MAINTENANCEMODE	<p>Provides a way for you to disable or enable Maintenance Mode on the Primary node. In Maintenance Mode, database modifications are done on the Primary node. This means that you can only write to the Primary node's A_MAINTENANCEMODE or F_MAINTENANCEMODE field. For more information on Maintenance Mode, refer to the Maintenance Mode section.</p> <p>For A_MAINTENANCEMODE, the value of TRUE is enabled, while FALSE is disabled.</p> <p>For F_MAINTENANCEMODE, the value of 1 is enabled, while 0 is disabled.</p>

A_MSG[0-63]	<p>Displays any of the last 64 messages related to partner SCADA communications. Each message includes a timestamp. If you do not specify an index number, using A_MSG, the very first message in the log displays. However, if you want to identify a specific message, for instance the second message in the list, you would use the field: A_MSG[1], since the index starts at 0.</p> <p>0 is the first message in the queue displayed in the SCADA Sync Monitor's message list, while 63 is the last message in the queue. Once 64 messages are reached, the queue resets. For more information, refer to the Overview of the SCADA Node Synchronization History section.</p> <p>If you need to review messages older than the last 64, you can review the SCADASync .log file, in your iFIX LOCAL directory. If you installed iFIX to the default location, this directory location is: C:\Program Files (x86)\Proficy\iFIX\LOCAL.</p>
A_MSGTIMEOUT E_MSGTIMEOUT	The number of times that a synchronization message had no response from the partner node.
A_NUMOFTPORT F_NUMOFTPORT	The number of data synchronization transports configured. Typically, this number is 3, which represents the Primary, Secondary, and tertiary data transports.
A_PDBCMPLETEMSG E_PDBCMPLETEMSG	The total number of times it took to send the synchronized data to the partner node over the active network connection.
A_PDBLASTERROR	<p>The last error message that appeared during a database synchronization.</p> <p>If you need to review more than just the most recent synchronization error message, you can review the SCADASync.log file in your iFIX LOCAL directory. If you installed iFIX to the default location, this directory location is: C:\Program Files (x86)\Proficy\iFIX\LOCAL.</p>
A_PDBNUMOFBLOCKS E_PDBNUMOFBLOCKS	The number of database blocks included in the last synchronization sent from this node to its partner.
A_PDBNUMOFSYNCS E_PDBNUMOFSYNCS	The number of synchronizations that were sent since you started iFIX.
A_PDBNUMRECVD E_PDBNUMRECVD	The total number of synchronizations received since iFIX started and a successful synchronization communication occurred. The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.
A_PDBRCVDDATE	The last date that the iFIX database was received by the partner node.
A_PDBRCVDTIME	The last time that the iFIX database was received by the partner node. This time is based on the local regional settings of the computer receiving the information.
A_PDBSECBTWNSYNC E_PDBSECBTWNSYNC	<p>The total number of seconds it takes to synchronize the active database with the standby database, from beginning to end. This field is a very valuable field to monitor.</p> <p>The value of this field is always greater than the A/E_</p>

	<p>PDBCMPLETEMSG field.</p> <p>A_PDBSECBTWNSYNC represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_PDBSECBTWNSYNC represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_PDBSENTDATE	The last date that the iFIX database was sent to the partner node.
A_PDBSENTTIME	The last time that the iFIX database was sent to the partner node. This time is based on the local regional settings of the computer requesting the information.
A_PDBSIZEINBYTES E_PDBSIZEINBYTES	<p>The size of the entire iFIX database that is being synchronized, in bytes.</p> <p>A_PDBSIZEINBYTES represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_PDBSIZEINBYTES represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_PDBSYNCDURATION E_PDBSYNCDURATION	<p>The total number of seconds it took to send the synchronized data from the active database to the standby database, over the active network connection.</p> <p>A_PDBSYNCDURATION represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_PDBSYNCDURATION represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_PHYSICALNODE	The physical node name of the specified iFIX node.
A_PRIMARYNODE	The primary physical node name configured on the specified node. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU.
A_PROTOCOL	The protocol used for synchronization by the specified iFix node. The value will be either UDP or TCP.
A_RCVMSGTIMEOUT E_RCVMSGTIMEOUT	The number of times that the SCADA node received an incomplete synchronization message.
A_SACACTIVE E_SACACTIVE	<p>The status indicating whether the Scan, Alarm, and Control (SAC) is processing the database.</p> <p>A value of 0 represents standby (not processing the database), while 1 means it is actively processing the database.</p>
A_SACSTATUS E_SACSTATUS	The status indicating whether the Scan, Alarm, and Control (SAC) program is Running or Stopped. 1=Running, 0=Stopped).

A_SACTICK E_SACTICK	The number of times the Scan, Alarm, and Control (SAC) program sent and/or received data.
A_SACTICKISRUNNING E_SACTICKISRUNNING	The status indicating whether the Scan, Alarm, and Control (SAC) program is healthy or not. (1=Alive, 0=Dead).
A_SECONDARYNODE	The secondary physical node name configured on the specified node. This field can be used to determine if the active and standby pair was configured properly in the Local Startup Definition dialog box in the SCU.
A_STATUS F_STATUS	The status of the specified node: STANDBY (0), ACTIVE (1), or MAINTENANCE (2).
A_SYSTEMDISK E_SYSTEMDISK	<p>The available system disk of the Windows system disk drive, in bytes, left on the specified node. Use this field along with the "A/E_TOTALMEM" and "A/E_AVAILMEM" fields to troubleshoot disk space errors. If the available disk space is zero, a failover occurs.</p> <p>A_SYSTEMDISK represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_SYSTEMDISK represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TOTALGOODCON E_TOTALGOODCON	The number of good iFIX network connections on the specified node.
A_TOTALMEM E_TOTALMEM	<p>The total memory, in bytes, on the specified node. Use this field along with the "A/E_SYSTEMDISK" and "A/E_AVAILMEM" fields to troubleshoot disk space errors.</p> <p>A_TOTALMEM represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_TOTALMEM represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TPORTACKCNT[0-2] E_TPORTACKCNT[0-2]	<p>The number of times the specified SCADA node acknowledged the network communication status for the specified data transport.</p> <p>A [0] following the field name refers to the primary data transport. [1] refers to the Secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORTACKCNT[0] represents the number of acknowledgements on the primary data transport.</p>
A_TPORTAVEACK[0-2] E_TPORTAVEACK[0-2]	<p>The average time it takes the specified SCADA node to acknowledge the communication status on the network for the specified data transport.</p> <p>[0] following the field name refers to the primary data transport. For example, A_TPORTAVEACK[0] represents the average time for acknowledgements from the primary data transport.</p> <p>[1] refers to the secondary data transport.</p>

	<p>[2] refers to the tertiary data transport.</p> <p>A_TPORTAVEACK[] represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_TPORTAVEACK[] represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TPORTBYTESASEC[0-2] E_TPORTBYTESASEC[0-2]	<p>The number of bytes processed, per second, on the network for the specified data transport.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORTBYTESASEC[0] represents the number of bytes processed by the primary data transport.</p> <p>A_TPORTBYTESASEC[] represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_TPORTBYTESASEC[] represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TPORTBYTESREVD[0-2] E_TPORTBYTESREVD[0-2]	<p>Displays the total number of bytes received on the network for the specified data transport. If the value for the bytes received is incrementing, that indicates good health of the network.</p> <p>The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORTBYTESREVD[0] represents the total number of bytes received by the primary data transport.</p> <p>A_TPORTBYTESREVD[] represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_TPORTBYTESREVD[] represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TPORTBYTESENT[0-2] E_TPORTBYTESENT[0-2]	<p>The total number of bytes sent on the network for the specified transport.</p> <p>The maximum number that can appear in this field is 4,294,967,296. After this number is reached, the number is reset to zero and the counter restarts.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data</p>

	<p>transport. For example, A_TPORBYTESSENT[0] represents the total number of bytes sent over the primary data transport.</p> <p>A_TPORBYTESSENT[] represents a whole number, restricted only by the number of characters you select when you add the field to your picture.</p> <p>E_TPORBYTESSENT[] represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.</p>
A_TPORDESC[0-2]	<p>The description of the specified data transport. This description also displays in the Data Sync Transport dialog box in the SCU. You can access this dialog box from the SCADA Configuration dialog box.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORDESC[0], represents description of the primary data transport.</p>
A_TPORDOGCOUNT[0-2] E_TPORDOGCOUNT[0-2]	<p>The number of times that the watchdog timer has checked the network connection between the SCADA pair for the specified data transport.</p> <p>Every time the watchdog updates, it is assumed that the connection is active. If after some period of time, the primary network does not receive a watchdog update from the partner SCADA Server, the connection is considered not running and the Watchdog times out.</p> <p>The Watchdog Timeout field is configured in the Timers area of the Data Sync Transport dialog box in the SCU. You access this dialog box from the SCADA Configuration dialog box.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORDOGCOUNT[0] represents the watchdog count of the primary data transport.</p>
A_TPORIP[0-2]	<p>The local TCP/IP network address of the specified data transport.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORIP[0], represents the local TCP/IP address of the primary data transport.</p>
A_TPORMSGREVD[0-2] E_TPORMSGREVD[0-2]	<p>The number of times that a communication message was received on the specified data transport.</p> <p>[0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORMSGREVD[0] represents the number of times a message was received over the primary data transport.</p>
A_TPORMSGSENT[0-2] E_TPORMSGSENT[0-2]	<p>The number of times that a communication message was sent on the specified data transport.</p> <p>[0] following the field name refers to the primary data transport. [1]</p>

	refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORMSGSENT[0] represents the number of times a message was sent over the primary data transport.
A_TPORMNAKCNT[0-2] E_TPORMNAKCNT[0-2]	The number of times that the specified transport did not acknowledge a communication message (sent a NAK). [0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORMNAKCNT[0] represents the number NAKs sent to the primary data transport.
A_TPORMNAKRCV[0-2] E_TPORMNAKRCV[0-2]	The number of times that the specified transport received a communication message that was not acknowledged (received a NAK). [0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORMNAKRCV[0] represents the number of NAKs received on the primary data transport.
A_TPORMSTATUS[0-2] F_TPORMSTATUS[0-2]	Displays the status of the network: Good, Bad, Undefined (disabled). [0] following the field name refers to the primary data transport. [1] refers to the secondary data transport. [2] refers to the tertiary data transport. For example, A_TPORMSTATUS[0] represents the network status of the primary data transport. For A_TPORMSTATUS[], the status is represented as words, such as Good, Bad, or Undefined. F_TPORMSTATUS[], the status is represented as a number, such as 1 for Good, 0 for Bad, or 2 for Undefined.

Field Formats

The format of the tag indicates the type of data that the field stores. The following table provides an overview of the available formats:

Field Formats

Format:	Description:	Used in...
A_	ASCII Format.	Data links and objects in pictures.
F_	Floating-point Format.	Data links, objects in pictures, and block-to-block references.
E_	15-Digit Precision Format.	Data links, objects in pictures, and block-to-block references. Valid values range from +/-3.40282300000000e+/-38, with 15 digits of accuracy.

Example Uses of Runtime Information Fields for Enhanced Failover

SCADASync tags contain diagnostic and network information that you can use to monitor and troubleshoot your Enhanced Failover configurations. For more information on SCADASync tags, refer to the [Runtime Information Fields for Enhanced Failover](#) section.

Example uses of SCADASync tags are outlined below.

Example 1: Monitor the Status of the Primary Node

When using the following tag in a datalink (with the A_ field), the status of the primary node in your Enhanced Failover configuration displays in run mode: STANDBY, ACTIVE, or MAINTENANCE. For example, if the primary node were the active node, this tag would display ACTIVE:

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].A_STATUS
```

When using the following tag in a datalink (with the F_ field), the status of the primary node in your Enhanced Failover configuration displays in run mode: 0 for STANDBY, 1 for ACTIVE, or 2 for MAINTENANCE. For example, if the primary node were the active node, this tag would display 1:

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].F_STATUS
```

Example 2: Monitor the Status of the Secondary Node

When using the following tag in a datalink (with the A_ field), the status of the secondary node in your Enhanced Failover configuration displays in run mode: STANDBY, ACTIVE, or MAINTENANCE. For example, if the secondary node were the standby node, this tag would display STANDBY:

```
Fix32.SecondaryPhysicalNodeName.SCADASYNC[0].A_STATUS
```

When using the following tag in a datalink (with the F_ field), the status of the secondary node in your Enhanced Failover configuration displays in run mode: 0 for STANDBY, 1 for ACTIVE, or 2 for MAINTENANCE. For example, if the secondary node were the standby node, this tag would display 0:

```
Fix32.SecondaryPhysicalNodeName.SCADASYNC[0].F_STATUS
```

Example 3: Determine the Version of iFIX Running on a Specified Node

The following example shows the version of iFIX running on the primary node:

```
Fix32.PrimaryPhysical.SCADASYNC[0].A_IFIXVERSION
```

In this example, the version that displays is: 5.8.*nnnn*, which is iFIX version 5.8. and *nnnn* is the build number.

Example 4: Display the Logical Node

The following example displays the logical node name configured for the SCADA pair, as defined in the SCU on the primary node:

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].A_LOGICALNODE
```

Example 5: Display the Primary Node Name

The following example displays the primary node name; however, it uses the secondary node name in the datalink to reference it:

```
Fix32.SecondaryPhysicalNodeName.SCADASYNC[0].A_PRIMARYNODE
```

Example 6: Display the Secondary Node Name

The following example displays the secondary node name.

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].A_SECONDARYNODE
```

Example 7: Display the Available System Disk

The following example displays the available system disk of the Windows system disk drive, in bytes, left on the primary node (using the A_ field):

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].A_SYSTEMDISK
```

The following example displays the available system disk of the Windows system disk drive, in bytes, left on the primary node (using the E_ field):

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].E_SYSTEMDISK
```

A_SYSTEMDISK represents a whole number, restricted only by the number of characters you select when you add the field to your picture. E_SYSTEMDISK represents a value with up to 15-digit precision that can be displayed, depending on how many digits you enable for viewing.

Frequently Asked Questions about Enhanced Failover

The following sections identify questions and answers to commonly asked questions when working with Enhanced Failover.

Question	Answer
Why does my SCADA node display error message number 1914, every time the active SCADA switches?	<p>When an iClient establishes a connection to an active SCADA Server node in run mode, the iClient starts to read data from that node. When the active SCADA Server node switches to the partner SCADA, the iClient momentarily loses its session with that node, causing this error to appear.</p> <p>You can suppress this error from appearing on screen. For more information on how to suppress this message and others, refer to the Reading Data from iFIX Pictures in iClients section.</p>
What kind of hardware setup do I need for Enhanced Failover?	<p>It is required to have at least one dedicated SCADA network (for UDP only). This network's components (LAN adapters, hubs, routers, switches, cables, and so on) should all be capable of running at 1 Gigabit. You must utilize a crossover network cable if the partner SCADAs are close to each other (for UDP only). You need to configure the active and standby nodes identically. For more information, refer to the Configure Computers for Enhanced Failover section.</p>
What is the SCADA Sync Monitor and how is it used?	<p>The SCADA Sync Monitor displays information about the primary and secondary SCADA Servers. For example, it describes how often database synchronizations occur, whether the networks are in good communication, debug log messages that occur during synchronization of the databases, SAC information, and the overall system health on both nodes.</p> <p>This tool is good for troubleshooting Enhanced Failover. For more information, refer to the Diagnostics with the SCADA Sync Monitor section.</p>

What are the log files available for the LAN Redundancy and Enhanced Failover features in iFIX?

- **SCADASync.log** – for reviewing log messages that occur during the SCADA synchronization process in Enhanced Failover.
- **ScadaRoleMgr.log** – for debugging the active to standby node switch in Enhanced Failover.
- **iFIX Alarm Types including Alarms to File, Alarm ODBC, Alarm History window** – for reviewing iFIX error logs if LAN Redundancy is used with Enhanced Failover.

For more information, refer to the [Log Files for Enhanced Failover Features](#) section.

Is there an iFIX security feature for Enhanced Failover? Yes. For information, refer to the Assigning Failover Security Privileges to Users section. There is also a security area available for Enhanced Failover. Refer to the [Security Area for Enhanced Failover](#) section for more information.

Maintenance Mode

Maintenance Mode is an Enhanced Failover feature that allows you to temporarily suspend synchronization between the two SCADA nodes in an Enhanced Failover pair in order to make changes to your iFIX database. For example, you could use Maintenance Mode to add a database block (using a pre-existing driver I/O address). Driver modifications are not recommended in Maintenance Mode. Any SCADA modifications using Maintenance Mode should be planned ahead of time to minimize disruptions to your network.

IMPORTANT: Maintenance Mode is the only valid and supported way to modify a database on the Enhanced Failover pair. In Maintenance Mode, modifications are done on the primary node. If you do not go into Maintenance Mode to make your changes, you may lose the changes you enter or corrupt the database.

You can initiate Maintenance Mode on the primary SCADA node either locally or remotely from an iClient. When you enter Maintenance Mode, SCADA synchronization temporarily stops; synchronization between the SCADA pair is suspended. Physical file synchronization of the process database (.PDB file) is included in this suspension of synchronization. After Maintenance Mode is enabled, you can make changes to the database on the primary node.

When iFIX security is enabled, you are encouraged to use an Enhanced Failover security area to restrict the remote usage of Maintenance Mode to specified users. When security is enabled on your iFIX nodes, Maintenance Mode can only be enabled if you have access to that Enhanced Failover security area. For information on the security area for Maintenance Mode, refer to the [Enhanced Failover Security Area](#) section.

NOTES:

- In Maintenance Mode, the Scan, Alarm, and Control (SAC) program is active on both SCADA nodes. This places an increased load on your PLC network, as the I/O drivers on both nodes are polling at the active rate. Both nodes will generate alarms.
- Since both nodes are SAC-active in Maintenance Mode, this can cause duplicate alarm entries (one from each SCADA node) in the Alarm ODBC service. In addition, Historian tags continue to collect from the primary SCADA node running in Maintenance Mode. You can use the Historian Administrator to force a switch to the redundant collector.

After entering Maintenance Mode, changes to the database can be made on the primary SCADA node only; however, the secondary node remains active and is fully runtime functional. In Maintenance Mode, all iClient applications (except the Database Manager) operate on the secondary SCADA node. All real-time operator interactions, such as alarm acknowledgement and outputs, are performed through the secondary SCADA node and are recorded in the secondary SCADA node's database.

IMPORTANT: Before exiting Maintenance Mode, be sure to **save** the database on the primary node. Failure to do so can result in database corruption or loss of changes.

Upon exiting Maintenance Mode, alarm acknowledgements and the simulation register changes made on the secondary SCADA node are copied to the primary SCADA node. Then, iFIX copies the database on the primary SCADA node to the secondary SCADA node, including the .PDB file. The primary SCADA node becomes the active node and the secondary SCADA node becomes standby. All iClient (View) node connections display the active SCADA node, which is now the primary node.

NOTE: Some file changes made during Maintenance Mode are not retroactively propagated. For example, if you entered Maintenance Mode to add a new alarm area, after you exit Maintenance Mode from the primary node, you will need to manually copy the *.AAD files from the primary SCADA to the secondary SCADA.

Enabling or Disabling Maintenance Mode

To enable or disable Maintenance Mode, use the SCADA Sync Monitor on the primary node, or the A_MAINTENANCEMODE or F_MAINTENANCEMODE fields of the SCADASync tag in an iFIX picture or an EDA application.

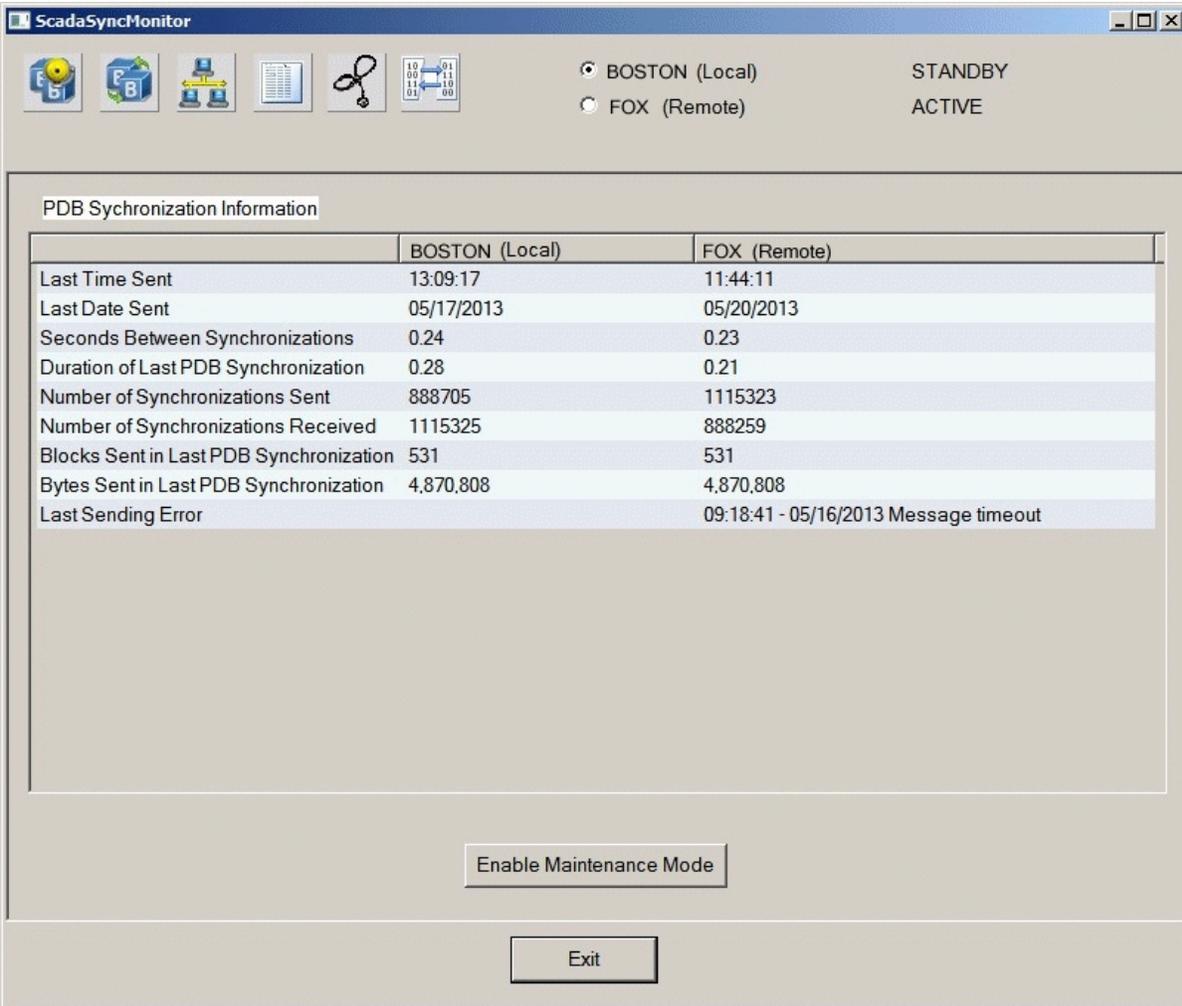
To enable or disable Maintenance Mode locally on the primary SCADA node, use either the SCADA Sync Monitor application (ScadaSyncMonitor.exe) or the SCADASync tag. The Enable or Disable Maintenance Mode button is available in SCADA Sync Monitor on the PDB Synchronization Information screen. The button is available only on the primary node. It does not display on the secondary node.

When iFIX security is enabled, the following two security checks are made when enabling or disabling Maintenance Mode. Unauthorized users are blocked and violations are logged to the Security log.

- The Manual Failover application feature is checked prior to enabling/disabling Maintenance Mode using the SCADASyncMonitor application. The Manual Failover application feature should be assigned to users or groups who are allowed to enable or disable Maintenance Mode using the SCADA Sync Monitor.
- The Enhanced Failover security area is checked prior to enabling/disabling Maintenance Mode using the SCADASync tag. This security area should be assigned to users or groups who are allowed to enable or disable Maintenance Mode using the SCADASync tag.

To enable or disable Maintenance Mode remotely from an iClient, use the SCADASync tag. For information on the SCADASync tag, refer to the [Maintenance Mode from Remote iClient](#) section.

The following graphic provides an example of the ScadaSyncMonitor screen with the Enable Maintenance Mode button displayed. For information on SCADA Sync Monitor, refer to the [Components of Enhanced Failover](#) section.



Maintenance Mode Steps

When using Maintenance Mode, the following events must occur:

IMPORTANT: It is usually a good idea to disable .PDB file synchronization from the secondary SCADA node to the primary SCADA node. Since we recommend that all database maintenance be performed on the primary node, there is usually no need to copy the .PDB files on the secondary to the primary. Also, the .PDB files on the primary may be overwritten by the (perhaps out-of-date) files on the secondary. So, the recommendation is to disable .PDB file synchronization on the secondary and leave it enabled on the primary. Disabling .PDB file synchronization on the secondary will not prevent the secondary from receiving .PDB files from the primary. It will only keep the secondary from sending its .PDB files to the primary. To do this, modify the ScadaSync.INI on the secondary only. For more information, refer to the [Customizing the Synchronization Process with SCADASync.ini](#) section.

1. Place the primary node into Maintenance Mode by clicking the Enable Maintenance Mode button in SCADA Sync Monitor, or by using the A_MAINTENANCEMODE or F_MAINTENANCEMODE fields of the SCADASync tag in an iFIX picture or an EDA application. Synchronization between the SCADA nodes is temporarily suspended.

NOTE: When working with large databases that synchronize frequently, it will take longer to switch to

Maintenance Mode when the SCADAs are in the middle of a synchronization. If the Primary was the Active SCADA when switching to Maintenance Mode then the ScadaSyncMonitor screen will show a status of 'PENDING MAINTENANCE MODE' on the Primary while a synchronization is still in progress. Do not make any changes to the database while in this state, as the Primary is still the Active SCADA.

2. In Maintenance Mode, all changes must be made to the database on the primary node. Enter your database changes on the primary node either locally from the server, or remotely from an iClient. When entering changes remotely, open the primary database on the iClient node (assuming you have the network privileges to do so) to make your changes.
3. Save your database on the primary node.
4. After your changes are completed, take the primary node out of Maintenance Mode by clicking the Disable Maintenance Mode button in SCADA Sync Monitor or by using the A_MAINTENANCEMODE or F_MAINTENANCEMODE fields of the SCADASync tag in an iFIX picture or an EDA application.

NOTE: As with switching into Maintenance Mode, an Enhanced Failover pair with a large database may take longer to exit Maintenance Mode and switch the primary back to Active.

5. Alarm acknowledgements and simulation register changes are copied from the secondary node to the primary node.
6. The databases are re-synchronized.
7. The primary node becomes the active node. The secondary node becomes standby node. All iClient (View) node connections display the primary SCADA node.

NOTES:

- Client applications running locally on the SCADA nodes are dependent on an operational iFIX networking path between the SCADA nodes. Ensure that after a disruption of the synchronization path followed by a disruption of the iFIX network path that both network paths are once again operational. When only the synchronization path is restored, and the iFIX network path between the SCADAs remains bad, the client applications on the local SCADA can only connect to the local SCADA. In this situation, the client applications on the standby SCADA are not able to "write" to the SCADA node. To check the iFIX networking path between the SCADA nodes, run NetHis.EXE on each SCADA node. The partner SCADA node should be listed as an established connection.
- Any database changes made by clients, EDA programs, or schedules to the secondary node are lost when Maintenance Mode ends. For example, if you added a block to the Secondary node database, that change would be gone when the primary node leaves Maintenance Mode and becomes active.
- For more up to date information on Maintenance Mode, refer to our Knowledgebase.

Maintenance Mode from Remote iClients

Maintenance Mode allows you to temporarily suspend synchronization between the two SCADA nodes so that you can make changes to your database while the Scan, Alarm, and Control (SAC) program is still running. For example, you could use Maintenance Mode to add a database block (using a pre-existing driver I/O address). Driver modifications are not recommended in Maintenance Mode. Maintenance Mode always runs on the primary node. For more information on how Maintenance Mode works, refer to the [Maintenance Mode](#) section.

The SCADA Sync Monitor application (SCADASyncMonitor.exe) cannot be used to enable or disable Maintenance Mode on a remote SCADA node because you can only access the SCADA Sync Monitor locally.

If you want to enable Maintenance Mode from a remote iClient, use the A_MAINTENANCEMODE or F_MAINTENANCEMODE fields in a SCADASync tag within an iFIX picture or an EDA application. When iFIX security is enabled, you are encouraged to use an Enhanced Failover security area to restrict the remote usage of Maintenance Mode to specified users. When security is enabled on your iFIX nodes, Maintenance Mode can only be enabled remotely if you have access to the Enhanced Failover security area. For information on this security area, refer to [Security Area for Enhanced Failover](#) section. For more information on how to set up security in iFIX, refer to the [Configuring Security Features](#) e-book.

Enabling or Disabling Maintenance Mode from a Remote iClient

To enable/disable Maintenance Mode from a remote iClient, create a picture that includes the A_MAINTENANCEMODE or F_MAINTENANCEMODE fields of the SCADASync tag. In this picture, select a data source address in the following format:

```
Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].field
```

where:

- *PrimaryPhysicalNodeName* is the physical node name of the primary SCADA node.
- *field* is either A_MAINTENANCEMODE or F_MAINTENANCEMODE

For example, the following addressing successfully enables or disables Maintenance Mode:

Node	Address
Primary	Fix32.PrimaryPhysicalNodeName.SCADASYNC[0].A_MAINTENANCEMODE

The following addressing fails:

Address	Result
Fix32.PrimaryPhysical NodeName.SCADASYNC[1].A_MAINTENANCEMODE	Fails because this addressing tries to put the primary node's partner (the secondary node) into Maintenance Mode.
Fix32.SecondaryPhysicalNodeName.SCADASYNC[0].A_MAINTENANCE MODE	Fails because this addressing tries to put the secondary node into Maintenance Mode. Maintenance Mode is only valid on the primary node.
Fix32.SecondaryPhysicalNodeName.SCADASYNC[1].A_MAINTENANCE MODE	Fails because this addressing tries to put the secondary node's partner (the primary node) into Maintenance Mode remotely.

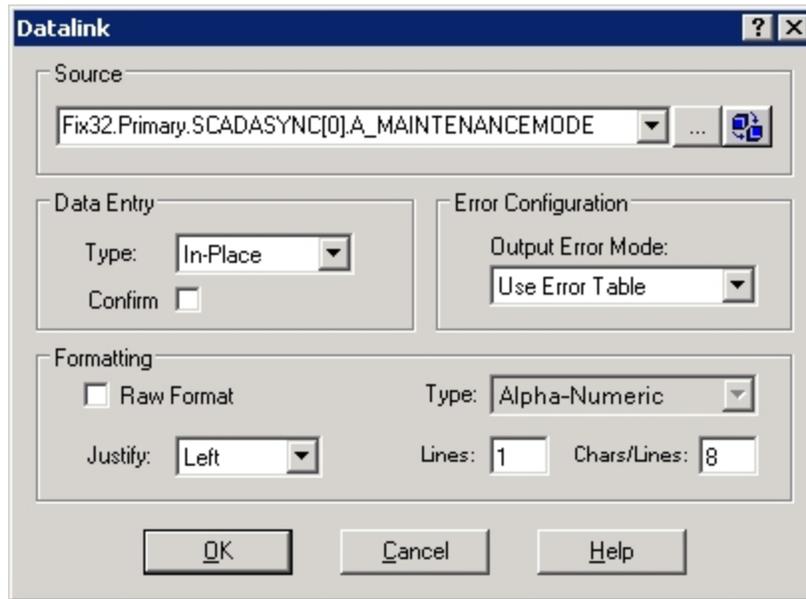
In run mode, when using:

- A_MAINTENANCEMODE, enter 'TRUE' to enable Maintenance Mode or 'FALSE' to disable Maintenance Mode.

- F_MAINTENANCEMODE, enter '1' to enable Maintenance mode and '0' to disable Maintenance Mode.

Be sure to use the physical node name configured in the SCU (the Local Node Name in the Local Startup Definition dialog box) for the primary node.

For example, here is a datalink added to a picture, with the In-Place data entry option enabled, so that you can edit this field (and change it from TRUE to FALSE, or vice versa) in run mode.



Once you put the primary node into Maintenance Mode, you can open the primary database on the iClient node (assuming you have the network privileges to do so), and make your changes.

IMPORTANT: Always make sure that you open the primary database and not the local one. Otherwise, your changes will not persist after you exit Maintenance Mode. Any file changes to the active secondary node are lost when Maintenance Mode ends.

NOTES:

- Maintenance Mode is only valid on the primary node.
- Always use the physical node name of the primary node.

For more information on other SCADASync fields you can use in your pictures, refer to the [Runtime Information Fields for Enhanced Failover](#) section.

Maintenance Mode Synchronization

In Enhanced Failover, Maintenance Mode allows you to temporarily suspend synchronization between the two SCADA nodes in order to make on-the-fly configuration changes to the process database. After entering Maintenance Mode, you can make modifications to the database on the primary SCADA node. During this time, the secondary SCADA node is fully runtime functional and carries all the iClients. Operator interaction from the iClients, such as alarm acknowledgments and outputs, are performed through the secondary SCADA node and recorded in the secondary SCADA database. When Maintenance Mode is exited, operator interactions on the database in the secondary SCADA node are synchronized

to the primary SCADA node before the primary SCADA node becomes active and starts to synchronize the database to the secondary SCADA node.

By default, Maintenance Mode synchronization and corresponding time-out parameters are enabled. To disable Maintenance Mode Synchronization, refer to the [Disabling Maintenance Mode Synchronization](#) section.

Alarm Acknowledgement Synchronization

Alarm acknowledgement synchronization uses the iFIX local area network connection, which must be a stable working connection between the SCADA nodes for the alarm acknowledgment synchronization to complete successfully.

A successful alarm acknowledgment synchronization returns the following message on the Overview page of ScadaSyncMonitor on the primary node:

```
Updated Alarm Acknowledgements
```

An unsuccessful alarm acknowledgment synchronization may return the following message on the Overview page of ScadaSyncMonitor on the primary SCADA node:

```
Updated Alarm Acknowledgments with Read Errors  
Updated Alarm Acknowledgments with Write Errors
```

Read errors occur when the primary SCADA node cannot read alarm acknowledgements from the secondary SCADA node. Check iFIX networking to ensure that the primary and secondary SCADA are connected. Write errors occur when the primary SCADA node cannot write alarm acknowledgements, perhaps because the tag it tried to write to does not exist.

Simulation Register Synchronization

Simulation registers are synchronized over the dedicated network for SCADA synchronization. This includes the SIM driver registers, SIM signal generators and parameters, and SM2 driver registers.

A successful simulation register synchronization returns the following message on the Overview page of ScadaSyncMonitor on the primary node:

```
Updated Simulation Registers
```

If the primary SCADA node does not receive simulation register synchronization from the secondary SCADA node within the timeout period (the default is 10 seconds), it exits Maintenance Mode without synchronizing. An unsuccessful simulation register synchronization indicates that the SCADASync connection may be broken and returns the following message on the Overview page of ScadaSyncMonitor on the primary SCADA node:

```
Maintenance Mode Synchronization Timed Out, Check Scada Sync Communication.
```

Database Manager in Maintenance Mode

When the primary SCADA node is in Maintenance Mode, iClients consider the secondary SCADA node to be the active SCADA node. The Database Manager behaves differently than the other iFIX applications on an iClient in that it can connect to the primary SCADA node in Maintenance Mode.

IMPORTANT: This connection between the Database Manager and the SCADA node continues even when there is a SCADA role change, which may result in a connection to a standby node. To prevent this situation, always enter Maintenance Mode *before* connecting to a SCADA node and always close the Database Manager before exiting Maintenance Mode.

When the Database Manager runs on a remote client, only one of the SCADA nodes is shown in the list of available nodes. When a SCADA node is in standby or when its partner is in Maintenance Mode, the SCADA node is considered unavailable.

When the Database Manager runs locally on one of the SCADA nodes, the local SCADA node is added to the list of available nodes. Both SCADA nodes are displayed in the list of available nodes. The local SCADA node is considered available even when it is in standby, or its partner is in Maintenance Mode. A warning message displays if you select the local SCADA node when the node is in standby or its partner is in Maintenance Mode.

IMPORTANT: If the Database Manager is run locally on the secondary SCADA node, take extra care to ensure that the changes made do not disrupt iClient operations and that any process database files saved will not be overwritten when Maintenance Mode is exited.

TIP: Check the Database Manager title bar, which shows the logical and physical name of the SCADA nodes and whether the connected SCADA node is the primary or the secondary node.

Disabling Maintenance Mode Synchronization

By default, alarm acknowledgements and simulation registers are synchronized when exiting Maintenance Mode; however, you can disable synchronization if you wish.

NOTE: These parameters are effective only on the primary SCADA node. They are ignored on the secondary SCADA node since the secondary does not enter Maintenance Mode.

► To disable alarm acknowledgment synchronization:

- Add the following line to the [SyncManager] section of the ScadaSync.Ini file on the primary SCADA node:

```
MMSyncAlarmAcks=0
```

► To disable simulation register synchronization:

- Add the following line to the [SyncManager] section of the ScadaSync.Ini file on the primary SCADA node:

```
MMSyncSimRegs=0
```

For the changes to take effect, you must restart iFIX after making either change.

Simulation Register Synchronization Timeout Parameter

You can add or change the following parameter in the [SyncManager] section in the ScadaSync.ini file on the primary SCADA node. This parameter disables or sets the number of seconds to wait for the simulation register synchronization to complete. For the change to take effect, you must restart iFIX after making the change.

NOTE: Absence of this parameter, or setting the parameter to a non-zero value enables the timeout.

Parameter	Description	Value	Default
MMSyncTimeout= <i>n</i>	Disables or sets the wait period for the simulation register synchronization to complete.	0 disables the timeout 1 to 300 indicates the number of seconds to wait	60 seconds

When the timeout is enabled, the primary SCADA node waits the specified amount of time for simulation register synchronization to complete before it exits Maintenance Mode. When the timeout is disabled, the primary SCADA node does not exit Maintenance Mode until simulation register synchronization completes. Simulation register synchronization may fail due to loss of the SCADA synchronization network

Client Operations

The following sections describe the operations for the iClient for Enhanced Failover scenarios:

- [Viewing Alarms on iClients](#)
- [Reading Data in iFIX Pictures on iClients](#)
- [Network Failure Detection on the iClient](#)
- [SCADAs With Enhanced Failover Detection on the iClient](#)

Viewing Alarms on iClients

The Alarm Startup Queue Service is enabled by default when you enable networking and SCADA. This ensures that the iClient receives all alarms after a SCADA failover occurs. The Alarm Summary will be correct after failover.

When an alarm occurs on a SCADA Server, the alarm is sent to all connected iClients. The iClient accepts alarms from the active SCADA node only. Alarms are not generated on the standby SCADA. In Enhanced Failover, only one SCADA node is generating alarms. During failover there may be a small window where both SCADAs are momentarily active, where both generate alarms to send to the iClient. During this period the iClient accepts alarms only from the active node(s).

You can view alarms in the Alarm History window on the iClient.

At the iClient, alarms and messages display the logical node name in brackets. In the following example, the logical node name is LNN.

```
04/29/98 22:49:45.1 [LNN] AI-1 HI 72.00
```

However, if the message is generated by the Database Manager or because of networking problems, node names within the alarm text display the physical node name.

Reading Data in iFIX Pictures on iClients

If you want to read data from a specific SCADA Server, you can access it by using its physical node name. The SCADA Server can be active or standby, but a session must be established to it. Data is not available on the iClient if communication with that SCADA Server is lost. You can read or write data to the active SCADA node. You can read data from the standby SCADA node but you cannot write data to it.

iFIX pictures, with links using a logical node name, always attempt to show data from the active SCADA regardless of whether it is the primary or secondary SCADA. This is done without requiring the picture to be opened, closed, or replaced.

When an iClient establishes a connection to an active SCADA Server node, it starts to read data from that node. If the active SCADA Server node becomes unavailable, the iClient loses its session with that node, and causes a message box to appear with following message:

To disable this message, you can edit the FilteredErrors.ini file, which is located in the C:\Program Files (x86)\Proficy\iFIX\Local directory, to include error number 1914. Once you have edited this file, you must restart the iFIX WorkSpace for the change to take effect.

When the iClient switches to a newly active SCADA node, the following events occur:

1. The standby node becomes the active node, and the active node becomes the standby node.
2. The links in the open pictures on the iClient display @ symbols (as the default) to indicate that the session with the previously active node has been temporarily lost.
3. The pictures resolve automatically using the information from the newly active node. This ensures data integrity.
4. The @ signs are replaced with process data from the newly active node. The node name referenced by these links does not change; it continues to display the name of the logical node.
5. An event message indicating that a failover has occurred is sent to all alarm destinations configured for the iClient when failover occurs.

NOTES:

1. You can change the default @ signs using the Comm Error setting on the Animations Data Error Defaults tab in the User Preferences dialog box of the iFIX WorkSpace.
2. The physical and logical names of a SCADA server are set in the SCU in the Local Startup Definition. The physical node name is set using the LocalNodeName field. The logical node name is set using the LocalLogicalName field.

Network Failure Detection on the iClient

The iClient retrieves data and alarms from the active SCADA node in run mode. If a SCADA failover event occurs, the currently active SCADA Server automatically switches control over to the newly active SCADA (the previous standby SCADA), and they switch roles. If an iClient does not switch to the newly active SCADA, an iFIX Notification window appears on the iClient until the switch to the newly active SCADA completes.

Another instance where the iFIX Notification window displays is when the iClient loses all iFIX network connections to the active SCADA, but still has an iFIX networking connection to the standby SCADA. The network connection between the SCADA pair that is being used for data synchronization is still established, and the iClient switches to the standby SCADA. When this occurs, an iFIX Notification message box appears on the iClient. Note that while in this condition, iFIX is receiving data, but that data may be out of date; you cannot execute a write from this iClient; you will not receive new alarms. The Notification window continues to display until the iClient switches to get its data from the active SCADA.

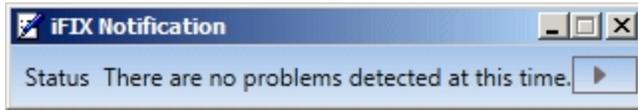
If an iFIX WorkSpace pop-up message appears, for instance to request to write a tag, it appears overlapping the iFIXNotification dialog box.

NOTE: The Minimize button, the first button in the upper right corner of this dialog box, reduces this dialog box to display the title bar only. The text "iFIX Notification" is the only text that appears in this title bar. Clicking the Restore button, the middle button in the upper right corner, restores the dialog to display the original state. You can also double-click the title bar to toggle between states.

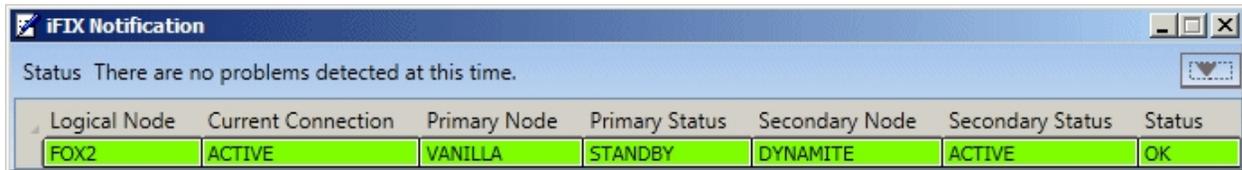
The iFIX Notification window closes within a minute after the iFIX networking connection to the active SCADA is restored.

Example of the iFIX Notification Window Under Normal Conditions

This is the message that appears when there are no issues. You can open this window at any time, by launching it from the system tray:



If you click the arrow for more information, the following shows an example of what appears when the failover nodes are in a good state:

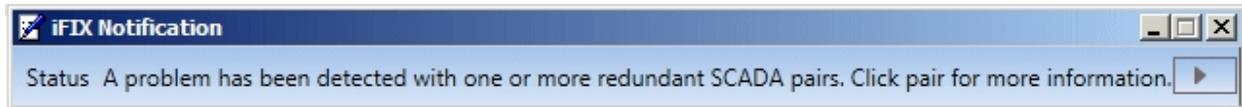


The screenshot shows a window titled "iFIX Notification" with a status bar that reads "Status There are no problems detected at this time." and a right-pointing arrow button. Below the status bar is a table with the following data:

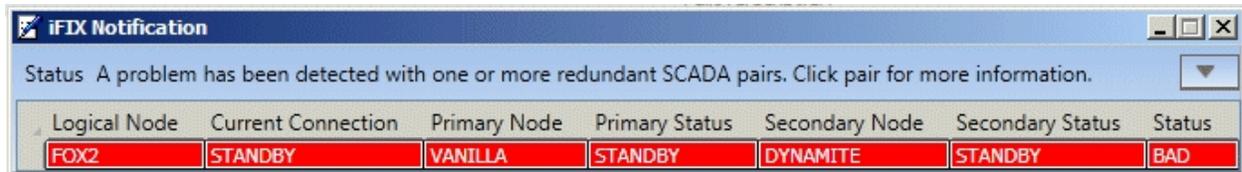
Logical Node	Current Connection	Primary Node	Primary Status	Secondary Node	Secondary Status	Status
FOX2	ACTIVE	VANILLA	STANDBY	DYNAMITE	ACTIVE	OK

Example of the iFIX Notification Window when a Change Occurs

This is an example message that appears when an issue occurs.



If you click the arrow for more information, the following shows an example of what appears in a problem state:



The screenshot shows a window titled "iFIX Notification" with a status bar that reads "Status A problem has been detected with one or more redundant SCADA pairs. Click pair for more information." and a right-pointing arrow button. Below the status bar is a table with the following data:

Logical Node	Current Connection	Primary Node	Primary Status	Secondary Node	Secondary Status	Status
FOX2	STANDBY	VANILLA	STANDBY	DYNAMITE	STANDBY	BAD

SCADAs with Enhanced Failover Detection on the iClient

Data is written to the active SCADA Server only. Data cannot be written to the standby SCADA Server. For example, if the active node is FOXBORO and the standby node is ALBANY, before a failover the iClient writes data to FOXBORO. After a failover, the iClient writes data to ALBANY.

When a failover occurs on the SCADA node, it is automatic and seamless. iFIX sends an alarm message whenever SCADA Server failover occurs. One of the few times a message appears on screen during the failover is when you do not programmatically suppress the SCADA connection error message

(error number 1914). You can suppress this error from appearing on screen using the FilteredErrors.ini file. For information on how to suppress this message and others, refer to the [Reading Data from iFIX Pictures in iClients](#) section.

When a failover event occurs, some VBA scripts may return an error if they are executing at the time of the failover. Real-time trends may show a small gap in the line chart. The Alarm Summary window should show the same number of alarms and acknowledge states after the failover occurs.

If you try to write data to a standby node, an error message appears. You can only read data from a standby node.

You cannot make database modifications to the standby SCADA. If you try to do so, a prompt appears, such as “Cannot write value. The SCADA node is in Standby mode” or “Cannot add a block. The SCADA node is in Standby mode.”

Index

1

1914 102, 114

1914 error code 56

A

active 18

alarm acknowledgement synchronization 18

Alarm History window 76

Alarm ODBC Service 21

alarm synchronization 13

B

Background Scheduler 41, 44

C

checklist 41

choosing communications protocol 14

Communication Status 88

D

data transport options 47

database and alarm synchronization 13

Database Dynamo Toolkit 39, 42

Debug Log 89

dedicated SCADA-to-SCADA network 10

differences 8

Disabling Maintenance Mode
synchronization 111

E

EDA 68

EDA applications 69

Enhanced Failover 6, 16, 39

description 5

diagnostics with SCADASync tags 91

diagnostics with SCADASyncMonitor 83

error messages 77

log files 75

Error Codes for redundancy and failover 77

error number 1914 114

F

Failure Detection 115

FilteredErrors.ini file 113

G

Gigabit-Ethernet card 39, 42

Global Memory Synchronization Status 91

I

I/O drivers 19

iClient 7, 16, 53, 68, 113-114

iClient switches 114

iClients 59

iFIXNotification.exe 30

Inactivity Timer 53

Integration Toolkit 41, 44

L

LAN Redundancy 7

limitations 11

loadable blocks 41, 44

logical node name 44

M

Maintenance Mode 110

- alarm synchronization 109
- database synchronization 110
- disabling alarm acknowledgement synchronization 111
- disabling Simulation Register Synchronization 111
- entering and exiting 103
- from a remote iClient 108
- Simulation Register synchronization 110

Mission Control 81

N

Network Status Display 62, 67

Network Status Server 67

NSD 60, 67

NSS 67

O

One Local Area Network (LAN) and One Dedicated LAN 33

Overall Partner Status 87

Overall System Health 90

P

physical node name 44

- in Maintenance Mode from remote iClient 107

primary 18

Productivity Pack 41, 44

Proficy Historian with Enhanced Failover 23

R

read data 113, 116

Recommendations 58-59

run mode operations 112

S

SAC 81

SCADA failover event 114

SCADA Sync Monitor 84

- dialog box 84

SCADASync.log 77, 89

SCADASyncMonitor.exe 75

secondary 18

standby 18

STK 41, 44

System Configuration Utility 47

T

troubleshooting 69

U

Updating the primary database from a remote iClient 107

W

write data 116