Enhanced Failover Basics

iFIX 5.0 and higher revised 3/12/2014

About This Guide

The purpose of this document is to provide users and developers with the basics of iFIX 5.0 and higher Enhanced Failover. Content will help with understanding, implementation, testing, and troubleshooting of iFIX Enhanced Failover.

It is recommended that all users and developers review the iFIX Electronic Books section on Enhanced Failover and Redundancy to ensure a fully comprehensive understanding.

Introduction to Enhanced Failover

The iFIX 5.0 and higher Enhanced Failover feature allows you to configure a secondary SCADA to take on the role of the primary SCADA node, if the primary node is unavailable.

The iFIX 5.0 and higher Enhanced Failover is significantly different from earlier versions of iFIX, and new features will have to be configured for an upgrade.

NOTE: *For more advanced redundancy, solutions such as Marathon or Stratus may need to be considered.*

This document includes:

- Enhanced Failover feature comparison between pre-iFIX50 and iFIX50 and above
- Enhanced Failover Terminology, Scenario explanation, and Key Facts
- Preparation to using Enhanced Failover
- Upgrade instructions from previous iFIX failover options
- System Configuration instructions for Enhanced Failover
- Enhanced Failover Tips
- Enhanced Failover SCADA database and driver modifications
- Methods of testing and verification of Enhanced Failover
- Troubleshooting and Error information

Pre-iFIX 5.0 Auto Failover vs. iFIX 5.0 and Higher Auto Failover

Previous to iFIX 5.0 the auto failover feature was very basic. The SCADA “pair” consisted to two independent SCADAS.

The only synchronization that was performed was for Alarm Acknowledgements.

The management of the scada pair was a manual effort to ensure they both operated identically to provide the best opportunity for success.

The client connections were typically managed with VBA script to ensure proper SCADA connectivity.

Auto Failover feature comparison pre-iFIX 50 vs. iFIX50 and above

Feature / function	**Pre-iFIX50**	**iFIX 5.0 and Higher**
SCADA pair aware of each other	No	Yes
Specific SCADA role per pair	No	Yes
Database synchronization	No	Yes
Alarm synchronization	No	Yes
Alarm acknowledgement synchronization	Yes	Yes
Dedicated synchronization path	No	Yes
Multiple synchronization paths	No	Yes
Simulation driver synchronization	No	Yes
NSD support	Yes	Yes

SDK	No	Yes
Duplicate alarms (such as in Alarms to ODBC)	Yes	No
Auto failover when disk space low	No	Yes
SCADA informs Client to switch to Active scada	No	Yes
Auto failover when disk space low	No	Yes
Auto failover when SAC unavailable	No	Yes
Maintenance mode for PDB changes	No	Yes
Automatic file copy when modified	No	Yes
Auto failover logging	No	Yes
Monitoring application	No	Yes

Enhanced Failover Topology

Enhanced Failover is a new design incorporating the concept of a SCADA pair working together. Enhanced Failover includes a true “Active” and “Backup” mode for the SCADA. Clients must be connected to the SCADA in “Active” mode to change data, acknowledge alarms, or write data to the PLC.

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 running, one node will be Active, and the other node will be Standby. The Active node functions as a normal SCADA node. SAC is processing the database, and alarms are being generated, etc. on the Active node. Additionally, the Active SCADA node periodically sends database and alarm information to its partner, the Standby node.

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 here. Instead, the standby SCADA receives database and alarm information from the active node.

Active SCADA – the active SCADA scans its database, communicates with the PLC, and generates alarms. Periodically, it sends its database to the Standby SCADA over the dedicated SCADA Synchronization network.

Client Connections

It is highly recommended 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. The mechanism to make this happen includes the use of Dynamic Connections, Network Status Display (NSD) tags and Logical SCADA names.

Dynamic Connections

Dynamic Connections are enabled on the scada allowing the scada to make a network connection to a remote client node and “pull” it to the Active scada. Dynamic Connections do not need to be enabled on the remote client nodes.

IMPORTANT NOTE: The requirement that Dynamic Connections must be enabled, has been removed if you have the latest SIMS installed and/or a newer version of iFIX installed. GE recommends that Dynamic Connection be disabled on Enhanced Failover SCADAS.

“Pulling” Clients to the Active SCADA

By default with dynamic connections enabled on the SCADAS when the Active role changes the new Active SCADA will connect to the clients and set their NSD tag to point to the new Active SCADA pulling the client to it. This is the preferred method for client connectivity with enhanced failover.

IMPORTANT NOTE: The requirement that Dynamic Connections must be enabled, has been removed if you have the latest SIMS installed and/or a newer version of iFIX installed. GE recommends that Dynamic Connection be disabled on Enhanced Failover SCADAS.

Forcing Clients to the Active SCADA

While automatically having the SCADA pull the clients to the Active SCADA using dynamic connections is the preferred method, optionally the clients could track the active SCADA and change their own NSD tags to ensure they are connected to the active scada.

This is similar to how the clients stayed connected to the SCADAS in the previous failover option.

Changing the client connectivity to the active SCADA could be done using VBA and a FIX schedule for instance. Dynamic connections on the SCADA side would be disabled. Care must be taken in developing the VBA code to ensure it is robust enough to ensure all clients connect correctly. The VBA code would have to account for the Active scada and then perform the appropriate action.

IMPORTANT NOTE: The requirement that Dynamic Connections must be enabled, has been removed if you have the latest SIMS installed and/or a newer version of iFIX installed. GE recommends that Dynamic Connection be disabled on Enhanced Failover SCADAS.

Inactivity Timer

In some instances it is beneficial to use the Inactivity timer to release resources that are no longer in use. This is useful in an environment that includes Webspace or Terminal Server client sessions.

IMPORTANT NOTE: GE recommends that the Inactivity Timer be enabled and on Enhanced Failover SCADAS and Terminal Servers.

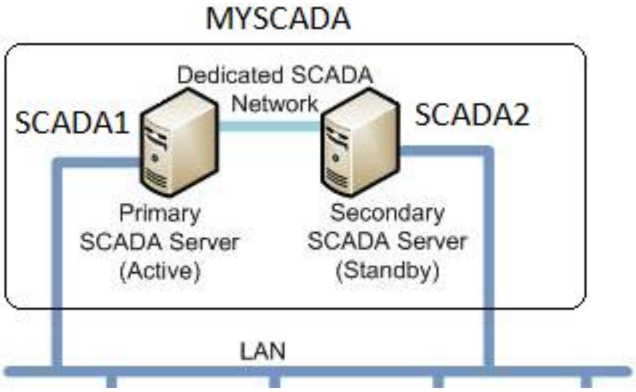
Network Status Display (NSD) tag

The Network Status Display tag is a special tag residing on each networked node that displays diagnostic, failover, and network information.

Logical SCADA name

iClients use the Logical node name to communicate with the Active SCADA node. Each Enhanced Failover SCADA node is defined with a unique physical name and a common logical name.

The following example shows the physical names as SCADA1 and SCADA2 and a logical name as MYSCADA, which is defined in both SCADA1 and SCADA2. The logical SCADA named MYSCADA will direct any request to the Active SCADA (either SCADA1 or SCADA2). For example, if an iClient node is reading the tag “MYSCADA.AI.F_CV” and SCADA1 is active the data would come from SCADA1.


MYSCADA
Dedicated SCADA Network
SCADA1
SCADA2
Primary SCADA Server (Active)
Secondary SCADA Server (Standby)
LAN

What is my SCADA Role?

Each node in an enhanced failover SCADA pair has a role, Active or Standby. In normal operations, one SCADA will be Active and the other SCADA will be Standby.

If A SCADA node cannot communicate or detects a problem with its partner, it becomes the Active.

If both SCADA nodes start up exactly at the same time the Primary node becomes active.

When using Failover Maintenance mode, both SCADAs will be Active.

Roles can also be changed manually by changing values of the NSD (network status display) tags. NSD tags provide the ability to force a SCADA to a particular role or to display information about the SCADAs or Clients.

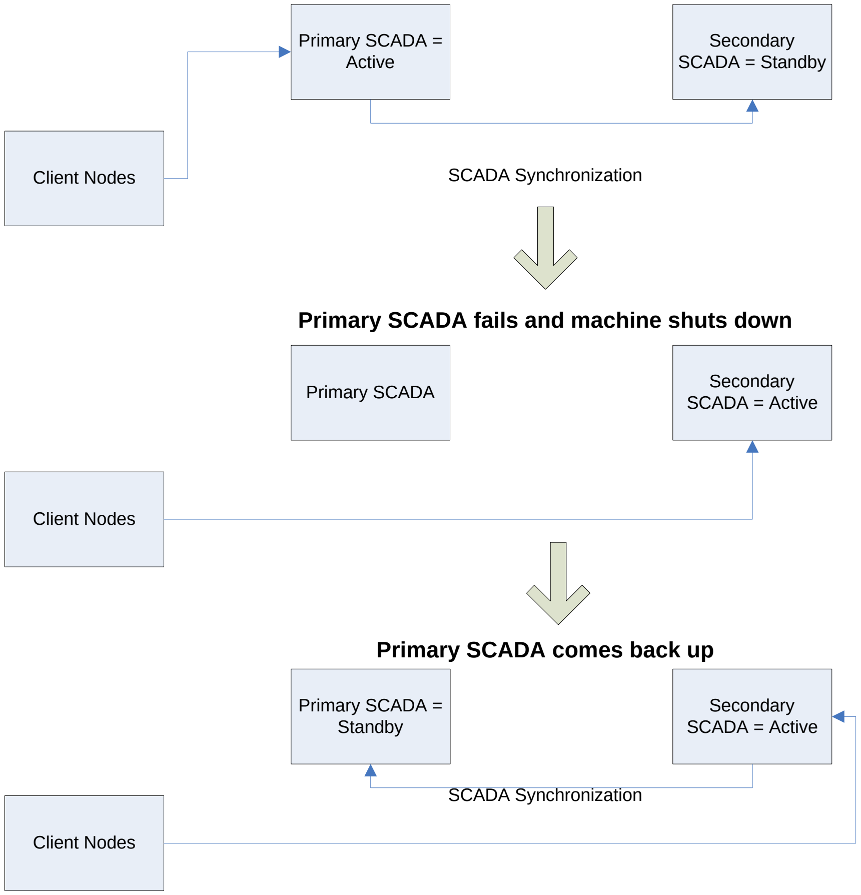
When does a SCADA Role automatically change?

- 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 such as disconnecting the iFIX networking cable on one of the SCADA computers.

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

Enhanced Failover Behavior

Scenario 1: Traditional Failover Scenario – Primary SCADA Failure



- The Primary is the Active and the Secondary is the Standby. Both SCADAs are healthy and running. The Client nodes are connected to the Active (Primary) SCADA.

- When the Primary SCADA machine fails or shuts down, the Secondary SCADA switches to the Active Mode and the Client nodes switch to the Secondary SCADA.

- When the Primary SCADA comes back up, it will start as the Standby SCADA until it is switched to the Active mode.

  NOTE: *The Primary SCADA does not automatically assume the Active role.*

- The Clients remain connected to the Secondary mode.

Scenario 2: Network issue between Clients and Active SCADA

If the “Active” SCADA client connection goes bad such as pulling the network cable out of the PC the Standby SCADA will change its role to Active.

The role change is a result of a major fix network disruption on the active scada. The clients will be pulled to the new Active SCADA.

Clients Connected to the Standby:

NOTE: Automatic Failover protects against a cable pull. Other network anomalies may not be recognized.

- The iFIX network connection between the Clients and the SCADAs uses one network path and the SCADA Synchronization uses a separate network path.

- Though not typical, there is a possibility of Clients losing the connection with the Primary “Active” SCADA and consequently connecting to the Secondary “Standby” SCADA.

- When this occurs, the Clients will be able to view all the data and alarms but will not be able to write data to the PLCs or acknowledge alarms.

- The client connectivity issue must be rectified or the SCADA roles will have to be manually switched to ensure all the Clients have read and write capability. The NSD tag F_SWITCHSCADAROLE can be used to manually switch roles.

Auto Failover Clients that stay connected to the Standby SCADA

Please note this document is to be used as general information. The behaviors described may change with subsequent versions, SIMS and testing.

Normal client connection operation

Both the client and the SCADA have a role in ensuring the clients are connected to the Active SCADA. Upon startup the client should connect to both SCADA physical names. This can be verified by running Network History (Nethis.exe). The connections should stay constant as long as the client is running.

Subsequently the client needs to resolve its “logical” connection to the Active SCADA.

Initially the “logical” connection could be either the Active or the Standby SCADA based on timing of the connections, etc but should quickly resolve itself to the real Active SCADA. The client still maintains its physical connections.

If a client does not resolve itself to the Active SCADA on its own the Active SCADA will “pull” the client to it (within 60 seconds by default).

If the Standby SCADA changes its role to Active the client should follow the Active SCADA.

If the client becomes connected to the Standby it should return to the Active SCADA within 60 seconds providing there is no real issue and all the connections are good.

Note: the default of 60 seconds can be modified in the Scadasync.ini file

Reasons that Clients stay connected to the Standby SCADA

This is typically the result of configuration and/or security. The following is a list of items to check:

- The Active SCADA is unavailable through the network. If the network path is not available from the client to the Active SCADA but is available to the Standby SCADA the client will connect to the Standby.

- Security enabled on the Client but not on the SCADA. If security is used it must be used on all nodes, clients and SCADAS.

- No default user logged into the SCADA (5.0 and higher). A user must be logged in at all times so the SCADA has security rights to access the clients NSD tags. This allows the Active SCADA to “pull” the clients.

- No default user logged into the client (5.0 and higher). A user must be logged in at all times so the SCADA is allowed to modify the clients NSD tags.

- Security Manual Failover feature not included for the logged in user. The logged in user on the SCADAS (FIX 5.0 and higher) must have this feature enabled and in the logged in user on the client (FIX 5.0 higher) must have this feature enabled.

- Client and SCADA security configurations are different. If the nodes are using a different set of security files or file location care must be taken to ensure the files are the same.

- Same name user logins on different nodes are not identical. Unpredictable results can occur if a user name is defined as a Windows user on the client and a FIX user on the SCADA even though the name and security rights are the same.

- Extra available paths enabled in FIX Networking. Unpredictable results can occur if more than one available path is enabled in the FIX Networking Advanced section. There should be only one available path enabled unless LAN Redundancy is enabled (not typical). This applies to all nodes. Any changes require a restart of FIX.

- Incorrect IP addresses in the Client Hosts file. Ensure the HOSTS file on the client node has correct IP addresses, SCADA node names and PC names defined.

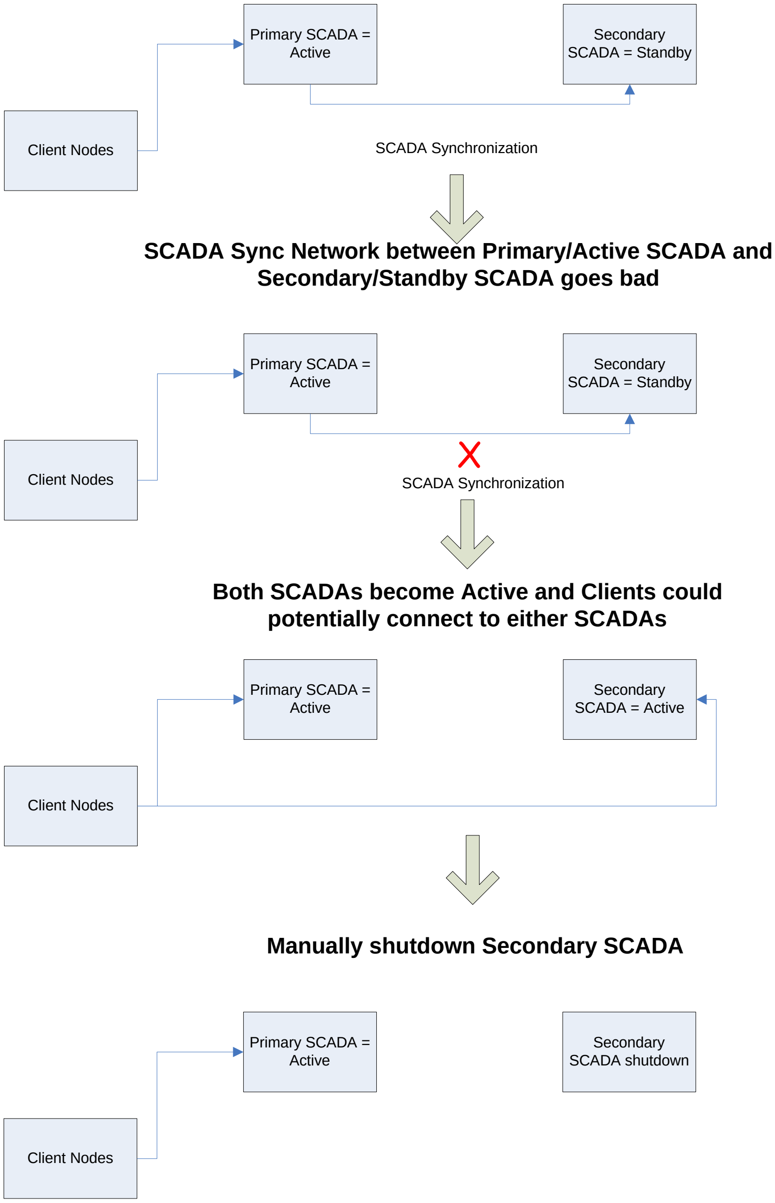
- Unused node entries in the LNT table on the SCADA. This issue is more likely when using Webspace or Terminal Server hosting the FIX clients. Note this scenario has been corrected with a SIM and the use of the Inactivity Timer.

Run Netdiag on the SCADA. Go to the LNT tab and review the entries. In general all the connected clients should have a status of OK. If there are other client connections that are not OK, may have a status such as 1914, they need to be removed form the list.

To automatically remove unneeded client connections enable the Inactivity setting in FIX networking on the SCADAS.

Set the value to 50 and restart. Any erroneous connections should now be cleaned up automatically.

Scenario 3: SCADA Sync Failure


Primary SCADA = Active
Secondary SCADA = Standby
Client Nodes
SCADA Synchronization
SCADA Sync Network between Primary/Active SCADA and Secondary/Standby SCADA goes bad
Primary SCADA = Active
Secondary SCADA = Standby
Client Nodes
SCADA Synchronization
Both SCADAs become Active and Clients could potentially connect to either SCADAs
Primary SCADA = Active
Secondary SCADA = Active
Client Nodes
Manually shutdown Secondary SCADA
Primary SCADA = Active
Secondary SCADA shutdown
Client Nodes

SCADA sync failure:

- The iFIX network connection between the Clients and the SCADAs uses one network path and the SCADA Synchronization uses a separate network path.

- If the SCADA synchronization network fails between the Primary and Secondary SCADA both SCADAs will be in the Active role.

- When the SCADA Sync network fails, the Secondary SCADA in the Standby role switches to the Active role.

- At this time the Clients could be connected to either of the two SCADAs. Both SCADAs are acting as independent SCADAs.

- When the SCADA Synch network is normalized the Primary SCADA is automatically the preferred SCADA to become the Active scada. The Clients will connect to the Primary as the Active scada.

- The SCADA roles will normalize as one Active and one Standby.

SCADA Node Handshaking

Early versions of Auto Failover role management were based on messaging and timing between the nodes. A more recent iteration of Auto Failover is “state” based. The SCADA nodes send commands to each other and wait for a response before finalizing the role.

Please check with GE Support to verify the SIM level needed to support this feature.

This allows for a more reliable role change however it may affect timing for applications that monitor the SCADA roles.

Note: The role resolution timing may change slightly. Custom applications monitoring role states should be retested with this new feature.

The following is an example of the “state” based role change:

Primary Node (ACTIVE) receives request to go STANDBY

Primary Node	**Action**	**Secondary Node**
Current role is ACTIVE		Current role is STANDBY
	The primary node SwitchScadaRole NSD tag is switched to STANDBY	
Primary Node switches to STANDBY		
	Primary sends “Go Active” →command to Secondary node	
		Secondary node receives “Go Active” command
		Secondary node switches from STANDBY to ACTIVE
	← Secondary sends “Go Active Response” to Primary	
Primary receives “Go Active Response” command		
	Primary sends “Reset Command” → command to Secondary	
		Secondary receives “Reset Command”
		Secondary clears Response
	Handshake Complete	
Current role is STANDBY		Current role is ACTIVE

Primary Node (STANDY) receives request to go ACTIVE

Primary Node	**Action**	**Secondary Node**
Current role is STANDBY		Current role is ACTIVE
	The Primary node SwitchScadaRole NSD tag is switched to ACTIVE	
Primary Node switches to ACTIVE		
	Primary sends “Go Standby” command → to Secondary	
		Secondary receives “Go Standby” command
		Secondary switches from Active to STANDBY
	←Secondary sends “Go Standby Response” to Primary	
Primary receives “Go Standby Response” command		
	Primary sends “Reset Command” → command to Secondary	
		Secondary receives “Reset Command”
		Secondary clears Response
	Handshake complete	
Current role is ACTIVE		Current role is STANDBY

Using NSD Tags for SCADA Status

The Network Status Display block (tag) is a system block available on all nodes. For example, some of the NSD fields are used to display the current status of an Enhanced Failover SCADA node, or to change its role. The following table describes these NSD fields.

Field	Writeable	Values	Description
A_SCADASTATUS	NO	ACTIVE STANDBY	Node is active. Node is standby.
F_SCADASTATUS	NO	1 2	Node is active. Node is standby.
F_SCADAREDUN	NO	0 1	Node is NOT an enhanced failover SCADA. Node IS an enhanced failover SCADA.
A_SWITCHSCADAROLE	YES	ACTIVE STANDBY	Set node to active. Set node to standby.
F_SWITCHSCADAROLE	YES	1 2	Set node to active. Set node to standby.

For example, an NSD data source to be used in a data link would be:

Fix32.MYSCADA1.NSD.A_SCADASTATUS (returns a value of “Active” or “Standby”)

Fix32.MYSCADA1.NSD.F_SCADASTATUS (returns a value of “1” or “2”)

NOTE: For more information on NSD tags please refer to the iFIX the Electronic Books section on Enhanced Failover and Redundancy | Monitoring Network Status.

iFIX 5.1and higher includes new enhanced SCADA sync fields similar to NSD tags.

Example: `Fix32.PrimaryNodeName.SCADASync[0].A_MAINTENANCEMODE`

These fields are discussed in the iFIX the Electronic Books section on Enhanced Failover and Redundancy | Troubleshooting Enhanced Failover | Runtime Information Fields for Enhanced Failover

Enhanced Failover Configuration and Implementation

Enhanced Failover Preparation

New Installations

For new installations it is recommended that all configuration and prep work be done with iFIX shut down. The exception is iFIX security changes, which requires iFIX to be running.

After the prep work and configuration is complete, the SCADAS can be started and failover can be tested.

Upgrades

Enhanced Failover is NOT a direct replacement for the previous iFIX failover. If you are upgrading an existing pair of SCADA nodes, time needs to be allotted for porting and validation.

SIMS

Install the latest Service Pack and all subsequent SIMs.

Hardware

Install the network cards before configuring FIX auto failover. If network cards are installed after configuring iFIX, re-check the SCU configuration for any changes in IP addresses. A crossover cable may be used for the dedicated SCADA sync connection.

Note: Removing or disabling/enabling NIC cards in FIX 5.0 and higher could alter the IP address to NIC card resolution incorrectly. The SCU may have to be rebuilt.

Keys

Enhanced Failover “SCADA Failover” is a keyed option. Ensure both SCADAs have the Auto Failover option enabled

Enhanced Failover Configuration

Enhanced Failover is configured in the System Configuration Utility (SCU)

FIX PDB and Driver Files

The FIX scada PDB and all driver files need to be exactly the same on both SCADAS. An exception may be unique items such s as a TSAP or NIC card slot definition.

Network Card Usage

Network cards 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.

NOTES:

- 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.
- The SCADA Sync NIC pair must be the same model, driver version and language.
- The SCADA Sync pair must be at least a 1GB card.
- To improve throughput when syncing large databases (over 20,000 tags) Jumbo Frames should be supported and enabled on the NIC card.
- All devices between the NIC cards such as routers should support the same desired configuration such as 1GB and Jumbo Frames.
- 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 an I/O 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 recommended to perform SCADA synchronization on a dedicated NIC. 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 then SCADA synchronization. Only ONE NIC should be enabled in the iFIX networking configuration (unless LAN Redundancy is used).

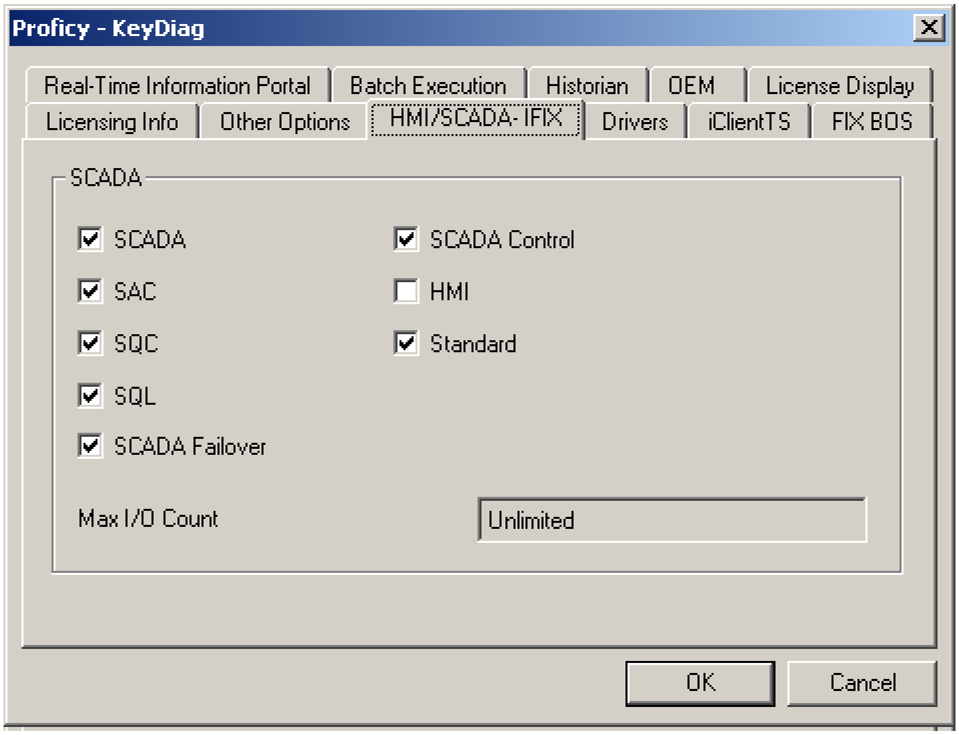
Enhanced Failover Preparation Check List

- ❑ Ensure the iFIX Enhanced Failover option is enabled on both SCADAS.
- ❑ If upgrading, backup both existing iFIX SCADAS.
- ❑ Ensure the network cards are installed properly on both SCADAs.
- ❑ Confirm that you gave the network card (NIC) a name. For instance, you can use iFIX, SCADA Sync, a company network name, and so on.
- ❑ Record the IP address for each NIC along with their name and use.
- ❑ It is recommended that both machines have the same NIC cards and NIC slot order.
- ❑ Ensure that all network cables and connections are correct.
- ❑ Use a dedicated network between the Primary and Secondary SCADAS for syncing.
- ❑ When using a crossover cable with NIC cards supporting 1GB and Jumbo frames a CAT6 type cable may be required.
- ❑ Install latest Service Packs, SIMs and I/O drivers on both scada's.
- ❑ Confirm the database (.PDB) & all driver files are the same on both SCADAS.
- ❑ Confirm the I/O drivers are listed in the same order in both SCUs, on both SCADAS.
- ❑ Validate that the SCADAS, I/O drivers, & clients function independently before configuring failover.
- ❑ Configure SCADA synchronization by disabling all the cards then only enable the card(s) needed for synchronization.
- ❑ Restart the SCADAS and test the Auto Failover functionality.
- ❑ Test the Client connectivity to ensure the Clients follow the Active SCADA.

Enhanced Failover Keys

Keyed Option

Both SCADAS require a key with SCADA Failover enabled, as shown in the following figure.



SCADA

☑ SCADA

☑ SCADA Control

☑ SAC

□ HMI

☑ SQC

☑ Standard

☑ SQL

☑ SCADA Failover

Max I/O Count: Unlimited

Enhanced Failover System Configuration Steps

Configuring a Logical SCADA name

Clients will connect to the SCADAS using the Logical name. Each SCADA will have the same logical name and a different Local node name.

1) Open the System Configuration Utility (SCU) on the Primary SCADA.

2) Select Configure | Local Start Up.

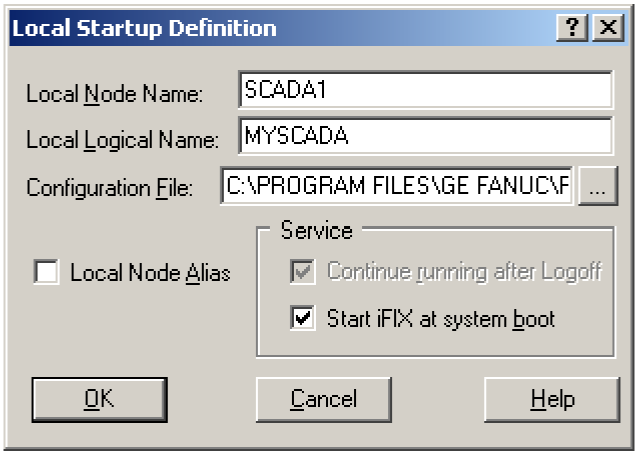
3) Type in your unique Local node name.

4) Type in the Local Logical name that will be used on both SCADA nodes.

5) Click OK.

6) Save the SCU file

7) Repeat the above steps on the Secondary SCADA.



Local Node Name: SCADA1

Local Logical Name: MYSCADA

Configuration File: C:\PROGRAM FILES\GE FANUC\F

☐ Local Node Alias

☑ Continue running after Logoff

☑ Start iFIX at system boot

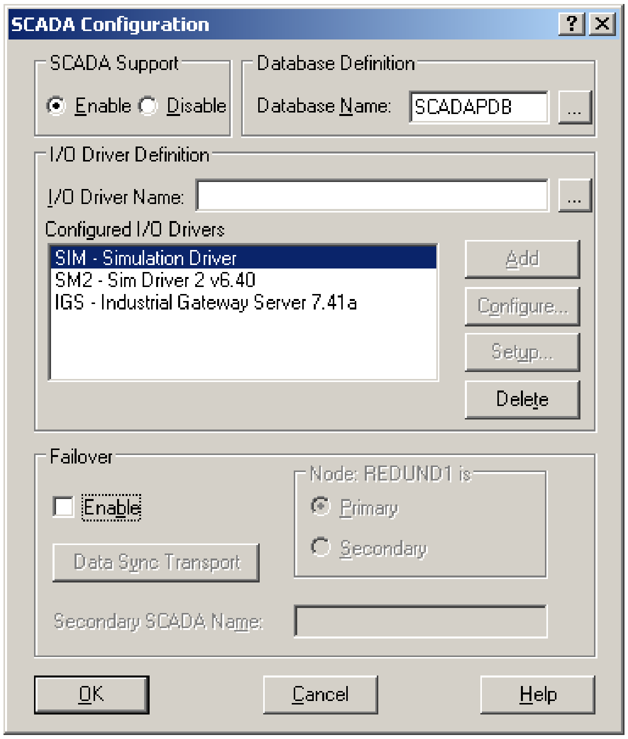
Configuring SCADA Drivers

The order of the defined drivers must be exactly the same in each SCADA System Configuration.

1) Open the System Configuration Utility (SCU) on the Primary SCADA.

2) Select Configure | SCADA.

3) Review and update the drivers in the Configured I/O Drivers list.



SCADA Configuration

SCADA Support: ● Enable ○ Disable

Database Definition – Database Name: SCADAPDB

I/O Driver Definition – I/O Driver Name:

Configured I/O Drivers:

SIM - Simulation Driver
SM2 - Sim Driver 2 v6.40
IGS - Industrial Gateway Server 7.41a

Failover: □ Enable

Node: REDUND1 is ● Primary ○ Secondary

Secondary SCADA Name:

Configuring Data Sync Transport

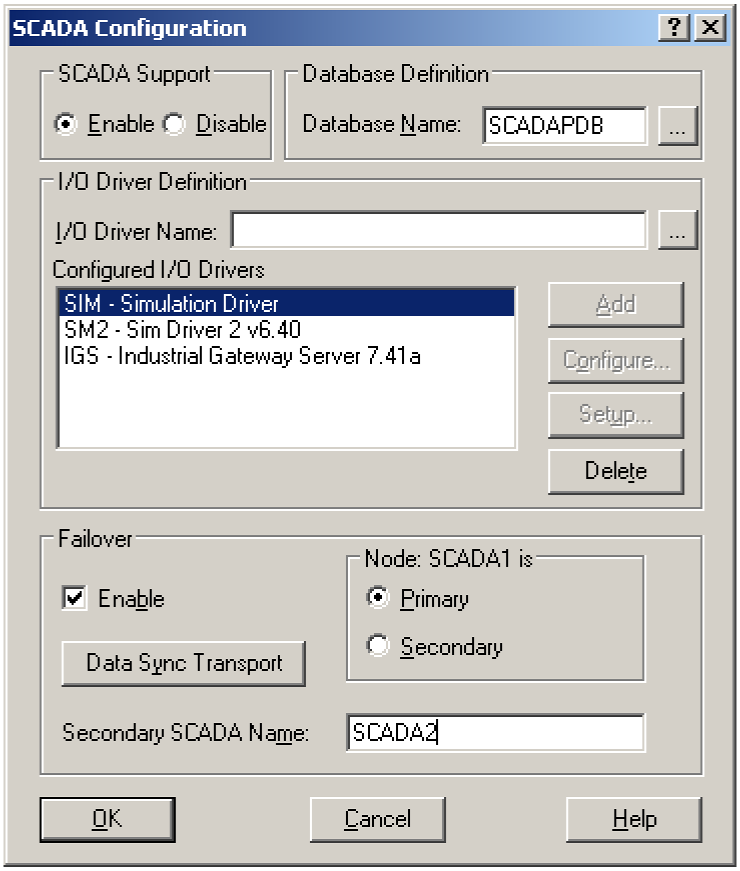
Before configuring the data sync transport it is important to understand what each network card is to be used for in the SCADA, the NIC card name and the corresponding IP address. A typical setup may use a dedicated NIC for the SCADA synchronization and a dedicated NIC for other network communication such as iFIX Client connections. This second NIC card can optionally be configured to be a backup for SCADA synchronization. Care must be taken to ensure the NIC IP addresses are assigned to their appropriate use.

1) Open the SCU and select Configure | SCADA.

2) Select Enable Failover option.

3) Select the option button to identify this SCADA (Primary or Secondary).

4) Enter the Secondary or Primary SCADA name (not the logical name).



SCADA Configuration

SCADA Support: ● Enable ○ Disable

Database Definition: Database Name: SCADAPDB

I/O Driver Definition: I/O Driver Name:

Configured I/O Drivers:
SIM - Simulation Driver
SM2 - Sim Driver 2 v6.40
IGS - Industrial Gateway Server 7.41a

Failover: ☑ Enable

Node: SCADA1 is ● Primary ○ Secondary

Secondary SCADA Name: SCADA2

5) Click the Data Sync Transport button.

6) Select and Enable the Network card that will be used for primary SCADA synchronization.

7) Enter the partner IP address.

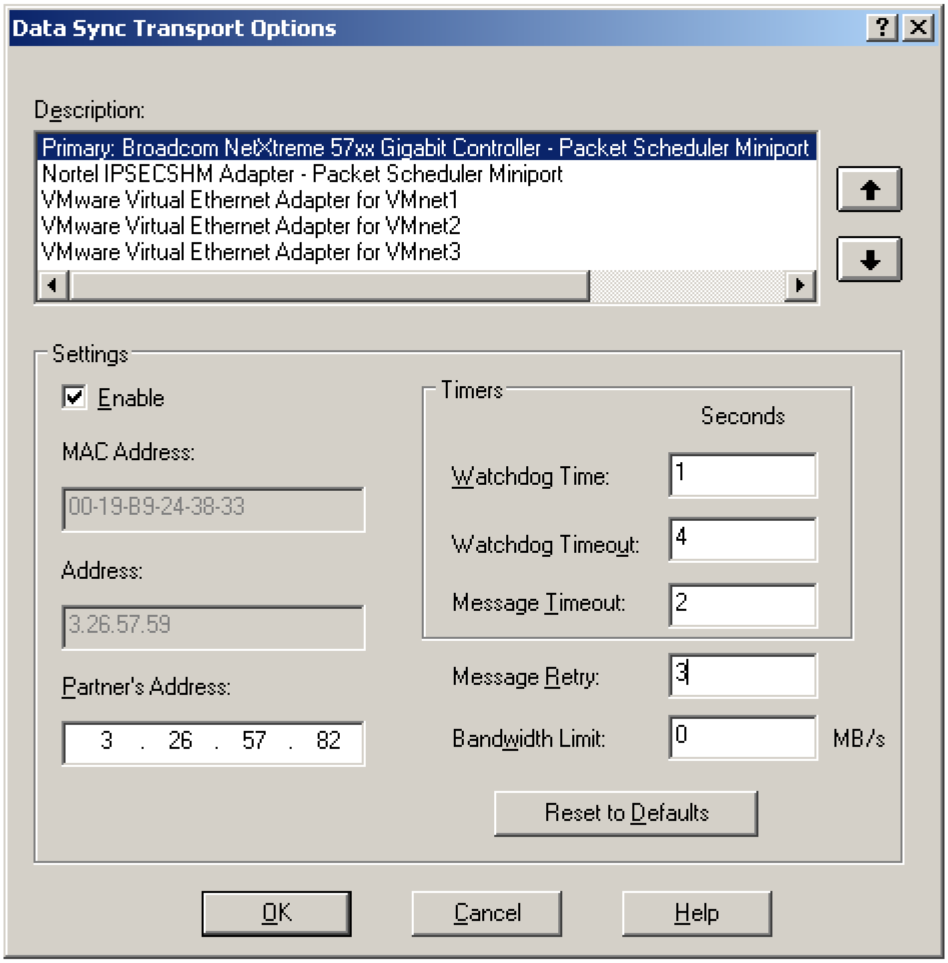
8) If a backup SCADA synchronization path is desired select and enable a Secondary Network card.

9) Enter the partner IP address.

10) Select and disable all other network cards.

11) Modify the Timer Values: Watchdog Time = 1, Watchdog Timeout = 4, Message Timeout = 2.

12) Click OK, and save the SCU file.



Data Sync Transport Options

Description:

Primary: Broadcom NetXtreme 57xx Gigabit Controller - Packet Scheduler Miniport
Nortel IPSECSHM Adapter - Packet Scheduler Miniport
VMware Virtual Ethernet Adapter for VMnet1
VMware Virtual Ethernet Adapter for VMnet2
VMware Virtual Ethernet Adapter for VMnet3

Settings

☑ Enable

MAC Address: 00-19-B9-24-38-33

Address: 3.26.57.59

Partner's Address: 3 . 26 . 57 . 82

Timers (Seconds)

Watchdog Time: 1

Watchdog Timeout: 4

Message Timeout: 2

Message Retry: 3

Bandwidth Limit: 0 MB/s

Configuring Networking

The SCADA will inform the view Clients what SCADA node is the Active node by using Dynamic Connections. On both primary and secondary:

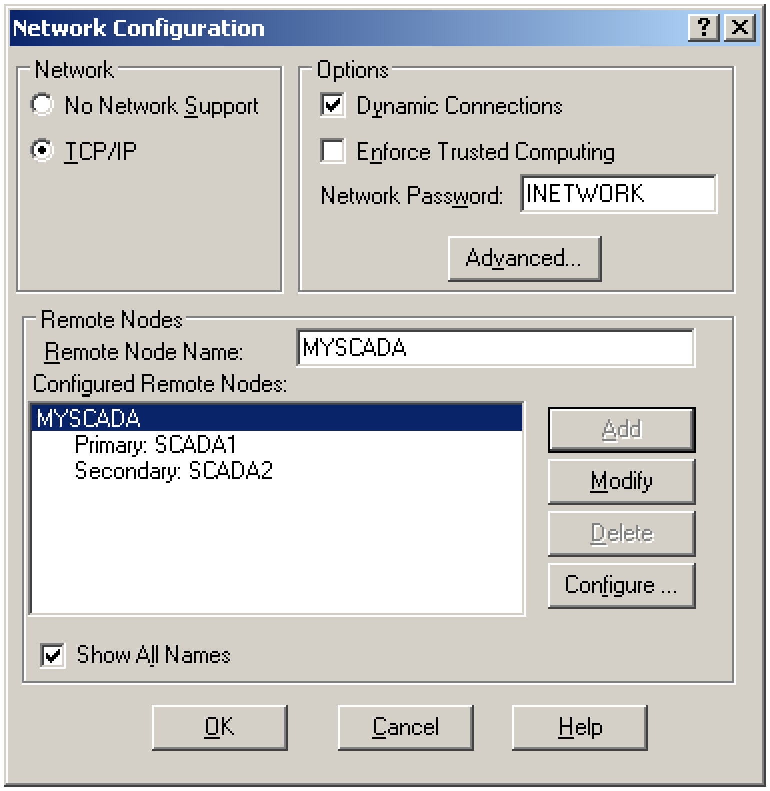
1) Open the System Configuration Utility (SCU).

2) Select Configure | Network.

3) Select Enable Dynamic Connections (This is only true for iFIX 5.0 with no SIMS)

   IMPORTANT NOTE: The requirement that Dynamic Connections must be enabled, has been removed if you have the latest SIMS installed and/or a newer version of iFIX installed. GE recommends that Dynamic Connection be disabled on Enhanced Failover SCADAS.

4) If the SCADAs are going to be Clients to each other, configure the remote node list.



Network Configuration

Network
○ No Network Support
● TCP/IP

Options
☑ Dynamic Connections
□ Enforce Trusted Computing
Network Password: INETWORK

Remote Nodes
Remote Node Name: MYSCADA
Configured Remote Nodes:
MYSCADA
Primary: SCADA1
Secondary: SCADA2

☑ Show All Names

5) Click the Advanced button.

6) Select YES to continue to the advanced section.

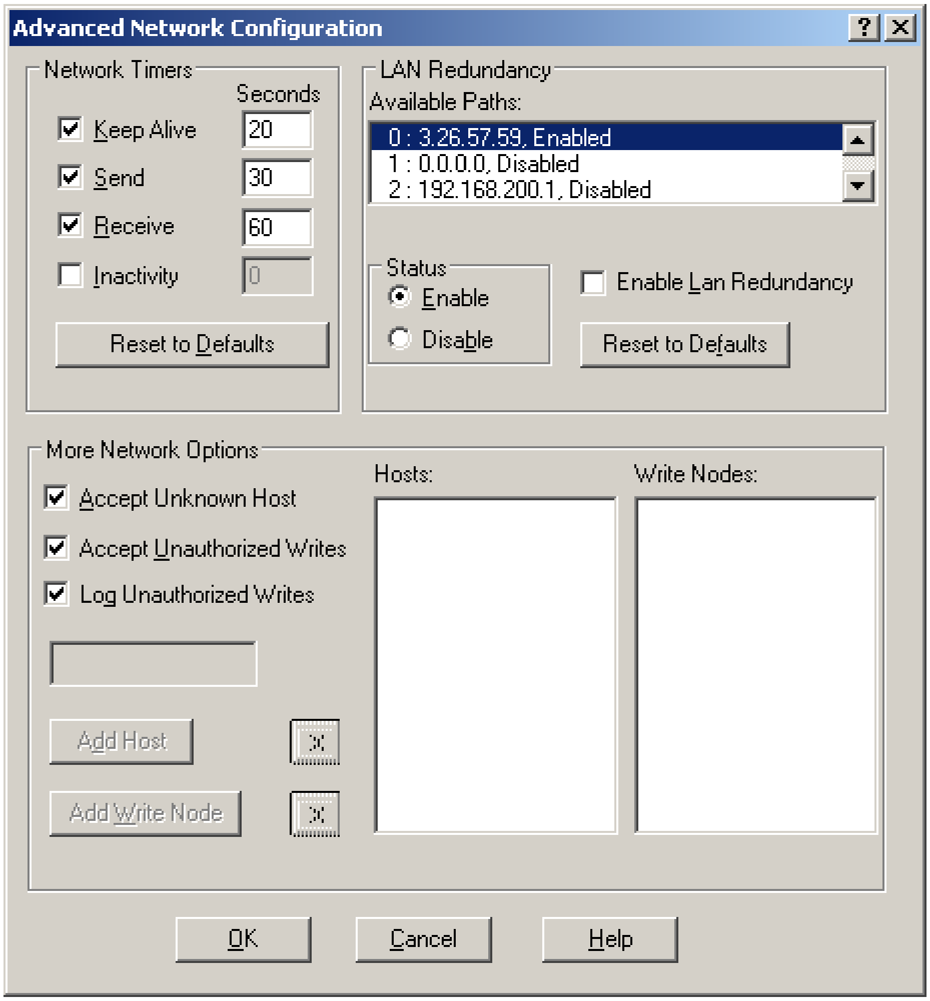
7) Inactivity is not required however may be beneficial when clients connect through Webspace or Terminal Services. Inactivity helps to remove connections no longer in use. The value should be set no lower than 150. GE recommends checking this and leaving the default value of 300.

8) Ensure only ONE IP is enabled in the LAN Redundancy Available Paths. This IP should be the IP designated for FIX Client connectivity.

9) Click OK until you get back to the main Security Configuration.

10) Select File | Save.

11) Close out of the Security Configuration.



Advanced Network Configuration

Network Timers

Seconds

☑ Keep Alive 20

☑ Send 30

☑ Receive 60

☐ Inactivity 0

LAN Redundancy

Available Paths:

0 : 3.26.57.59, Enabled
1 : 0.0.0.0, Disabled
2 : 192.168.200.1, Disabled

Status

● Enable

○ Disable

☐ Enable Lan Redundancy

More Network Options

☑ Accept Unknown Host

☑ Accept Unauthorized Writes

☑ Log Unauthorized Writes

Hosts:

Write Nodes:

Configuring Security

In FIX 5.0 and higher if FIX security is enabled there has to be a user logged in at all times on the SCADAS and the clients in order for the clients to be “pulled” to the Active SCADA.

The logged on user on the SCADA and the client must have the security "Manual Failover" application feature.

In FIX 5.1 if FIX security is enabled there has to be a user logged in at all times on the SCADAS and that user must have the security "Manual Failover" application feature.

The clients on FIX 5.1 are not required to be logged in and do not require the security "Manual Failover" application feature.

NOTE: If iFIX security is used it must be enabled on ALL nodes. A default user with access to the manual failover feature must always be logged onto the SCADA nodes.

1) In the SCU, select Configure | Security.

2) Select the proper security group or user.

3) Select Modify.

4) Select Modify Application Features.

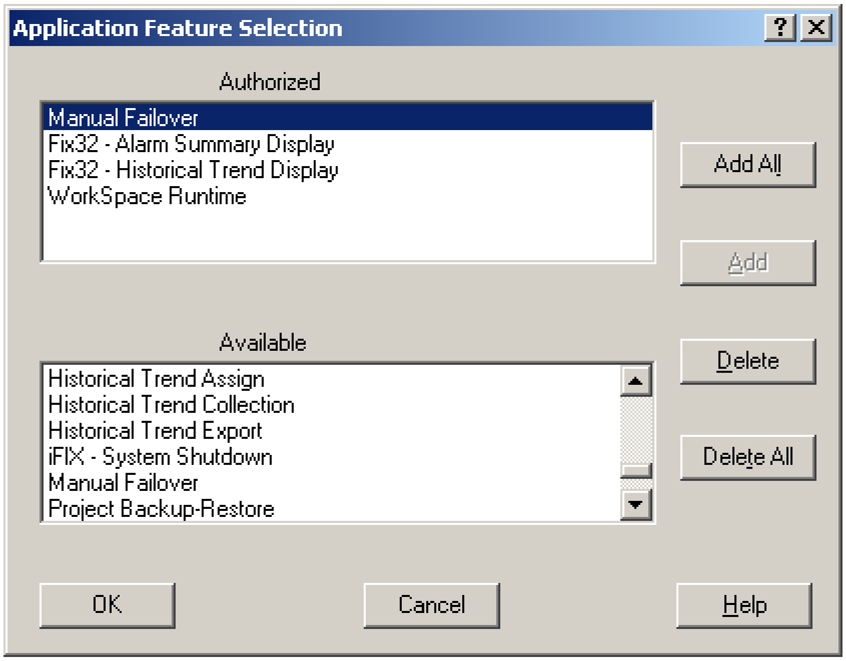
5) Add the application feature – Manual Failover.

6) Select OK until you get back to the main Security Configuration.

7) Select File | Save.

8) Close out of the Security Configuration.

9) Save and close the SCU.



Application Feature Selection

Authorized

Manual Failover
Fix32 - Alarm Summary Display
Fix32 - Historical Trend Display
WorkSpace Runtime

Available

Historical Trend Assign
Historical Trend Collection
Historical Trend Export
iFIX - System Shutdown
Manual Failover
Project Backup-Restore

Configuring INI Files used for Enhanced failover

When iFIX starts two new executables are started, ScadaSync.exe and ScadaRoleMgr.exe.

ScadaSync.exe performs the synchronization.

ScadaRoleMgr.exe manages the roles (Active or Standby) of the SCADA nodes.

Both executables are listed in the FIX.ini file under the section [PARTNER SCADA] to start up.

By default both executables create a log. ScadaSync.log and ScadaRoleMgr.log. Both logs are located in the FIX Local directory.

ScadaSync.exe reads the ScadaSync.ini file at startup to determine behavior.

ScadaRoleMgr.exe does not have an INI file and instead use switches in its command line to alter its behavior.

Modifying ScadaRoleMgr.exe behavior:

Edit the FIX.INI file located in the FIX Local directory.

Opening the FIX.INI will reveal the following default settings.

[PARTNER SCADA]

RUN=%SCADASYNC.EXE

RUN=%SCADAROLEMGR.EXE /L

Switches can be added to add functionality.

To have the log file append data add the switch **/A** (append).

To include addition log information add the switch **/V** (verbose)

To specify a startup delay in seconds add the switch **/D** (delay)

Note: /D allows one scada to wait for the partner scada status information for up to 20 seconds.

The startup delay command option should only be defined for the failover scada node that is defined to be the default STANDBY scada, typically the SECONDARY scada. Defining the startup delay on the SECONDARY scada will give the PRIMARY SCADA time to startup and take on the ACTIVE role.

[PARTNER SCADA]

RUN=%SCADASYNC.EXE

RUN=%SCADAROLEMGR.EXE /L **/A /V /D20**

Modifying ScadaSync.exe behavior:

Edit the SCADASYNC.INI file located in the FIX Local directory.

ScadaSync.ini is used by ScadaSync.exe to specify settings such as how fast to sync, how often to check to ensure the clients are connected to the Active scada, logging behavior and more.

Opening the SCADASYNC.INI will reveal the following default settings.

```
[SyncManager]

; EnableSIMFailureButtons=0

EnablePDBSyncButtons=1

[Transport0]

[Transport1]

[Transport2]

[ScadaRoleMgr]

; default: 60 seconds

ClientConnectionsCheckInterval=60

DelayAutomaticAfterManualSwitch=5

[FileSync0]

FIXDIR=PDBPATH

Inclusion="*.*"

Exclusion="*.TMP;*.EVS;~*.*;*.foo"

IdleTime=5000

Recursive=0
```

Modifying the ScadaSync.ini file

The most common modifications are to expand logging and to set the rate that ScadaSync.exe will sync the data.

Note: It has been determined when DelayAutomaticAfterManualSwitch (default = 5 seconds) and the TimeSyncRateMilliseconds are set to the same value the SCADA roles may bounce back after a manual role switch. To prevent this use a 1 to 2 ratio.

Note that the value of TimeSyncRateMilliseconds is in milliseconds (5000 equals 5 seconds) while the value for DelayAutomaticAfterManualSwitch is in seconds.

Example:
If TimeSyncRateMilliseconds=5000 then make DelayAutomaticAfterManualSwitch=10

Changing the Sync Rate:

Note: To determine the appropriate rate value auto failover must be up and running

Then open the ScadaSyncMonitor and review the “Duration of last PDB Synchronization”.

The rate should be double this value. If it takes 5 seconds to copy the PDB then the rate should be 10 seconds or longer.

Add the following line under the [SyncManager] section:

TimeSyncRateMilliseconds=10000

Changing Logging:

The default log ScadaSync.log is overwritten daily. To append the file add or modify the [LogFile] section.

Add the line:

DeleteOnStartup=0

To create Daily logs in place of the appended log add the line:

DailyLog=1

Note: Remove the line “DeleteOnStartup=0” if it exists.

To log more synchronization details add the line:

Type=Communication

A typical modified ScadaSync.ini may look like the following:

```
[SyncManager]

; EnableSIMFailureButtons=0

EnablePDBSyncButtons=1

TimeSyncRateMilliseconds=10000

[Transport0]

[Transport1]
```

```
[Transport2]

[ScadaRoleMgr]

; default: 60 seconds

ClientConnectionsCheckInterval=60
;(NOTE: In later versions of iFIX with the latest SIMS, this value should be 0).

;In addition, some special configuration is necessary to disable client-pulling by the SCADA. Skip this
;step if the network has older nodes and the SCADA nodes will still have Dynamic Connections
;enabled. Set the ClientConnectionsCheckInterval variable in the SCADASYNC.ini file (in the
;LOCAL folder) to 0 (zero).

DelayAutomaticAfterManualSwitch=20



[FileSync0]

FIXDIR=PDBPATH

Inclusion="*.*"

Exclusion="*.TMP;*.EVS;~*.*;*.foo"

IdleTime=5000

Recursive=0



[LogFile].

Type=Communication

DailyLog=1
```

Upgrading the Primary SCADA

- Shutdown iFIX, and backup the existing system.
- If both SCADAs cannot be shut down, direct all the Clients to existing Backup SCADA.
- Take the Primary SCADA off the network (remove the cables).
- Install NIC cards if needed.
- Ensure you have needed cabling such as a crossover cable for SCADA synchronization.
- Install the latest iFIX Service Pack, SIMs and latest I/O drivers.
- Refer to section Enhanced Failover System Configuration in this document.

  NOTE: *You will need the NIC IP addresses that will exist in the Backup.*
- Shut down the old Backup SCADA.
- Plug the Primary SCADA into the network.
- Start iFIX; the Clients should now connect to the Primary SCADA.
- Make iFIX security changes (if needed) to enable Manual Failover feature for all Clients.

The Primary SCADA should be up and running with the Clients connected to it.

Upgrading the Backup SCADA

- Shutdown iFIX, and backup the existing system.
- Copy the PDB and Driver configuration file from the Primary to the old Backup (Secondary).
- Disconnect the old Backup from the network (now referred to as the Secondary SCADA).
- Install all NIC cards needed.
- Install the latest iFIX Service Pack, SIMs and latest I/O drivers.
- The System Configuration File on each SCADA needs to have identical drivers and driver order.
- Refer to section Enhanced Failover System Configuration in this document.

  NOTE: *You will need the NIC IP addresses that will exist in the Primary.*
- Plug the Secondary SCADA into the network.
- Start iFIX on the Secondary; the Clients should stay connected to the Primary SCADA.
- The Secondary SCADA should be in Standby mode.

- Modify any custom code that manages failover using the NSD tags. New NSD tags (_SCADARUN, _SCADASTATUS, _SWITCHSCADAROLE) can be used.

- Open ScadaSyncMonitor.exe and verify SCADA synchronization is working

  NOTE: *See the section on Testing and Verification to understand how to monitor SCADA synchronization and SCADA status.*

Enhanced Failover SCADA Startup

After configuration is complete, it is time to start the SCADAs. With the SCADAs still shut down, copy the iFIX PDB and Driver files from the Primary SCADA to the Secondary SCADA.

Start the SCADAs. Typically the Primary is started first, then the Secondary. This allows the SCADAs to start in the preferred SCADA roles, the Primary as Active and the Secondary as Standby.

NOTE: Always allow a minute or two for the nodes to connect to each other ensuring all data and alarms settle out before changing Failover status. The partner scada will receive alarms from the Active scada. If the roles are changed too quickly not all alarms will have been transferred.

The SCADA should start as the Active node and all driver/PLC communications should be good. The Clients should all be connected to the Primary and have the ability to change and read data.

The Secondary SCADA should start up as the Standby node.

Enhanced Failover Tips

- FIXToHIST.EXE is started automatically. If not needed, comment it out from the FIX.INI. FixToHist is used when Historian tags are managed in the FIX PDB.

- Remove any shortcuts that launch iFIXNotification.exe. By default the shortcut is installed (in iFIX & iFIX 5.1) in the windows All Users startup folder. This application was removed and replaced with a new notification application in iFIX 5.5.

- If iFIXNotification was already started stop the task using task manager. IFIXNotification also start opc20ifix.exe. Stop this task as well unless implicitly using it.

- Currently, only the SIM and SM2 drivers support synchronization of I/O information.

- Drivers can be configured to START or STOP using VBA based on the SCADA role status.

- If using Historian, have the same collectors on both SCADAs and configure them for redundancy. Note that Enhanced Failover and Historian collectors do not know about each other. Historian redundancy is a separate configuration.

- You cannot write to or modify the Standby database.

- VBA scripts and EDA applications should use the “logical” node name to ensure they connect to the Active scada.

- Modify the FilteredErrors.INI file to suppress connection messages such as 1914.

- The clocks on both SCADAs should be synchronized.

- Dynamics connections must be enabled on the SCADAs but not required on the View Clients.

  IMPORTANT NOTE: The requirement that Dynamic Connections must be enabled, has been removed if you have the latest SIMS installed and/or a newer version of iFIX installed. GE recommends that Dynamic Connection be disabled on Enhanced Failover SCADAS.

- Ensure the same “loadable blocks” are installed on both SCADAs and in the same slots.

SAC and Driver Write Queues

SAC runs independently of the Driver. With Enhanced Failover, SAC will be either Running (on the Active SCADA) or Paused (on the Standby SCADA). The driver will stay running and connected to the SCADAs on both the Active and Standby SCADA.

SAC (Scan Alarm and Control), when running, SAC 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 are getting processed mainly depends 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 are not necessarily reflecting 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 1000’s of writes, have the queue count increase briefly, and then come back down, ideally close to 0.

Examples

Here are two examples that enforce the understanding that Driver queues and the Enhanced Failover mechanism are totally independent of each other.

Example 1:

The driver is in the running state on both SCADAs.

Let’s say that 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:

The driver is in the running state only on the Active SCADA (using script).

When the “failover” happens, using code one driver is stopped while the other driver is started.

When a driver is stopped either using code 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 SCADA Modifications

SCADA modifications should be planned. Based on the modifications needed, you may want to shut down iFIX or disable and disconnect SCADA synchronization.

NOTE: When one SCADA is shut down and the other is Active, upon starting iFIX the Active node will synchronize the PDB to the newly started Standby. Be careful not to make changes on the shut down system only to have them overwritten.

One approach would be to consider the Enhanced Failover SCADA system to be in various modes:

- Development

  All major changes such as driver changes and or replacing an existing PDB could be considered Development mode. IFIX should be shut down for these types of changes.

- Maintenance

  Enhanced Failover includes a maintenance mode. Maintenance mode temporarily turns SCADA synchronization off. Changes such as adding a database block (using pre-existing driver I/O address) or importing a PDB csv file can be done in Maintenance mode. Driver modifications are not recommended in maintenance mode.
  Refer to the iFIX Electronic Books Enhanced Auto Failover and Redundancy | SCADA Server Enhanced Failover | Maintenance Mode.

- “On the fly” modifications
  With SCADA sync active, minor changes such as adding a database block (using pre-existing driver I/O address) can be done. The changes are immediate to the partner node on the next sync.

- Running

  No changes are being made the system is running normally.

Maintenance Mode

Normal Synchronization Mode

SCADA synchronization performs two main tasks.

1) Performs a memory copy of the running PDB from the Active SCADA to the Standby SCADA

2) Performs a file copy when any files change within the PDB directory from the Active SCADA to the Standby SCADA. Note Scadasync.ini contains an “exclusion” list, which can be modified to limit which files are copied.

If both tasks have taken place a SCADA failover or a SCADA restart will be assured to have the correct data and configuration.

It is recommended when the SCADA pair is initially configured and the Primary SCADA is proven to work correctly to then manually copy the “working files” such as the process database (.PDB), alarm area database (.AAD) and driver configurations to the Secondary SCADA and ensure the Secondary SCADA works with those same files.

Once SCADA sync is configured and running a memory copy of the Active SCADA process database is periodically transferred to the Standby SCADA.

Any file changes within the PDB directory are copied to the Standby SCADA.

Example: If you add or change a database block and save the process database the new changes in memory and the actual PDB file will be copied to the Standby SCADA.

Maintenance Mode

Maintenance mode temporarily suspends synchronization between the two SCADA nodes and is only available on the Primary scada.

The Enable/Disable maintenance mode button is available in the SCADA Synchronization Monitor (SCADASyncMonitor.exe). This button is available on the primary node only.

Maintenance mode allows the developer to complete modifications on the Primary SCADA without syncing to the Secondary SCADA until maintenance mode is turned off.

Exiting maintenance mode will allow SCADA synchronization to resume. The Primary SCADA will stay Active and the Secondary SCADA will return to Standby. The Clients will switch back to the Primary (Active) SCADA.

Any modifications to the PDB must be saved or re-saved after maintenance mode is disabled in order for the file to copy to the Standby SCADA.

Important Notes:

Entering maintenance mode places both scada’s into the Active state. The clients should automatically switch to the new Active SCADA.

Both SCADA nodes role will be Active, ensure the all Clients have successfully switched to the Secondary SCADA before modifying the Primary SCADA.

Driver modifications are not recommended in maintenance mode.

File changes are not copied while in maintenance mode and not retroactively copied when maintenance mode is turned off.

Any file changes within the PDB directory such as Process Database changes, Alarm Area Database changes, etc must be manually copied to the Standby SCADA manually or re-saved after exiting maintenance mode.

Failure to manually copy modified files such as the PDB and AAD could allow the changes to be overwritten or become unavailable for use.

Since both SCADA nodes are Active in maintenance mode duplicate alarm entries may occur in the Alarm ODBC table.

Historian tags may continue to be collected from the SCADA in maintenance mode depending on how the collectors are managed.

See iFIX Electronic Books for more information.

Modifying I/O Drivers

When a SCADA becomes active the I/O addresses in the running FIX pdb get resolved against the running driver(s) configured I/O.

If there is a mismatch between the pdb and driver configuration the pdb tags can go off scan, drivers with auto-create enabled can create incorrect data blocks, etc.

To help ensure the I/O mapping on the auto failover SCADA pair do not get out of sync between the SCADAS the following steps can be followed to make driver changes.

It is understood that some developers may deviate from this process and should do so with caution. This document provides the most reliable method of making driver changes.

Ensure current back up files exists for the driver configuration and pdb file before making changes.

Step 1. Enter maintenance mode on the Primary SCADA. Both the Primary and Secondary SCADA will be active. Auto failover SCADA synchronization will stop. The clients should all be connected to the Secondary SCADA.

Step 2. Make the necessary modifications to the PDB and/or driver. Save all changes and ensure the changes perform as intended. Note: DO NOT take the Primary out of maintenance mode at this time.

Step 3. Copy the modified files from the primary to the Secondary SCADA. At this point the running PDB and driver file on the primary do not match what is running on the Secondary (the physical files should be the same). Note: DO NOT take the primary out of maintenance mode at this time.

Step 4. Shut down FIX and the driver on the secondary. If the driver is running as a service, stop the driver service. The FIX clients will connect to the Primary SCADA.

The modified physical files have already been copied however there could be node specific driver changes on the Secondary that need to be altered.

Example:
- Driver configuration file name could be different
- NIC slot defined within the driver configuration could be different
- TSAP definitions within the driver configuration could be different
- Make any node specific driver configuration changes that apply.

DO NOT start FIX on the Secondary at this time.

Step 5. Disable maintenance mode on the primary. The clients will remain connected to the Primary. With maintenance mode disabled the roles will be correct once the Secondary is restarted. The secondary PDB and driver files should match the Primary and are ready to load.

Step 6. Start up FIX and the driver on the Secondary SCADA. The Secondary should start as the standby SCADA. Ensure the PDB and driver starts as expected. Verify SCADA synchronization and subsequent manual failovers work correctly.

Verify that all of the new PDB and/or driver changes made on the primary exist as well on the Secondary.

Enhanced Failover Testing and Verification

After the SCADA pair is configured, the next step is to ensure failover is functioning properly. Typically, the developer needs to be able to create an event to cause a failover and have the ability to display and understand the results.

Common methods to view SCADA information:

- NetworkStatusOverview.grf

  Included with iFIX and can be used on the clients to display the current SCADA roles.

- SCADA Sync Monitor (ScadaSyncMonitor.exe)

  Used on the SCADA to view SCADA synchronization information.

- Custom picture or VBA scripting

  The developer can also create a custom picture containing NSD data links to view the data needed.

Useful NSD tags:

- F_SWITCHSCADAROLE

- A_SCADASTATUS

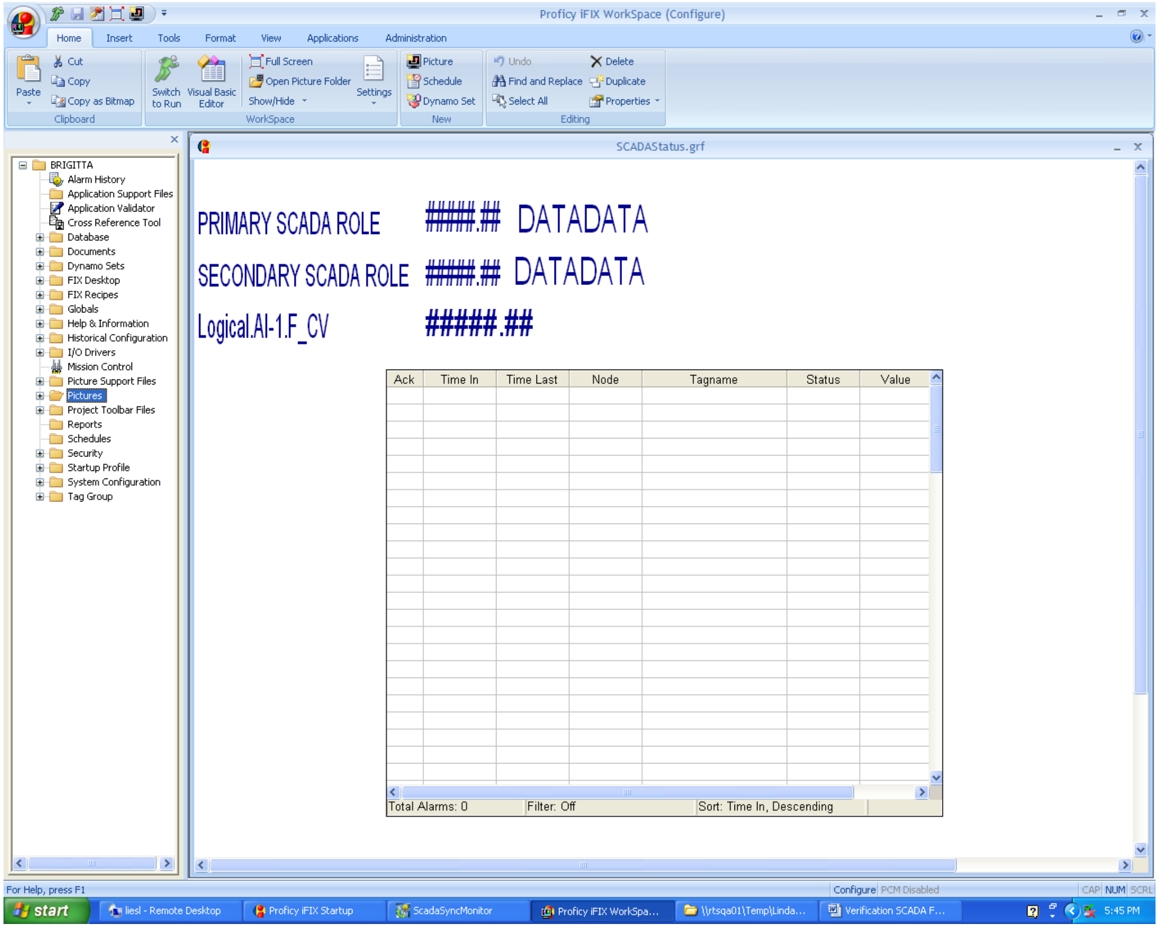
NOTE: *When using the NSD tags the Local SCADA name should be used, not the Logical SCADA name.*

Examples:

- FIX32.SCADA1.NSD. A_SCADASTATUS
  FIX32.SCADA2.NSD. A_SCADASTATUS
  Reading this tag displays the current SCADA role, Active or Standby.

- FIX32.SCADA1.NSD. F_SWITCHSCADAROLE
  Setting this tag to a value of 1 sets the SCADA to Active mode.
  Setting this tag to a value of 2 sets the SCADA to Standby mode.

Sample Picture



SCADAStatus.grf

PRIMARY SCADA ROLE ####.## DATADATA

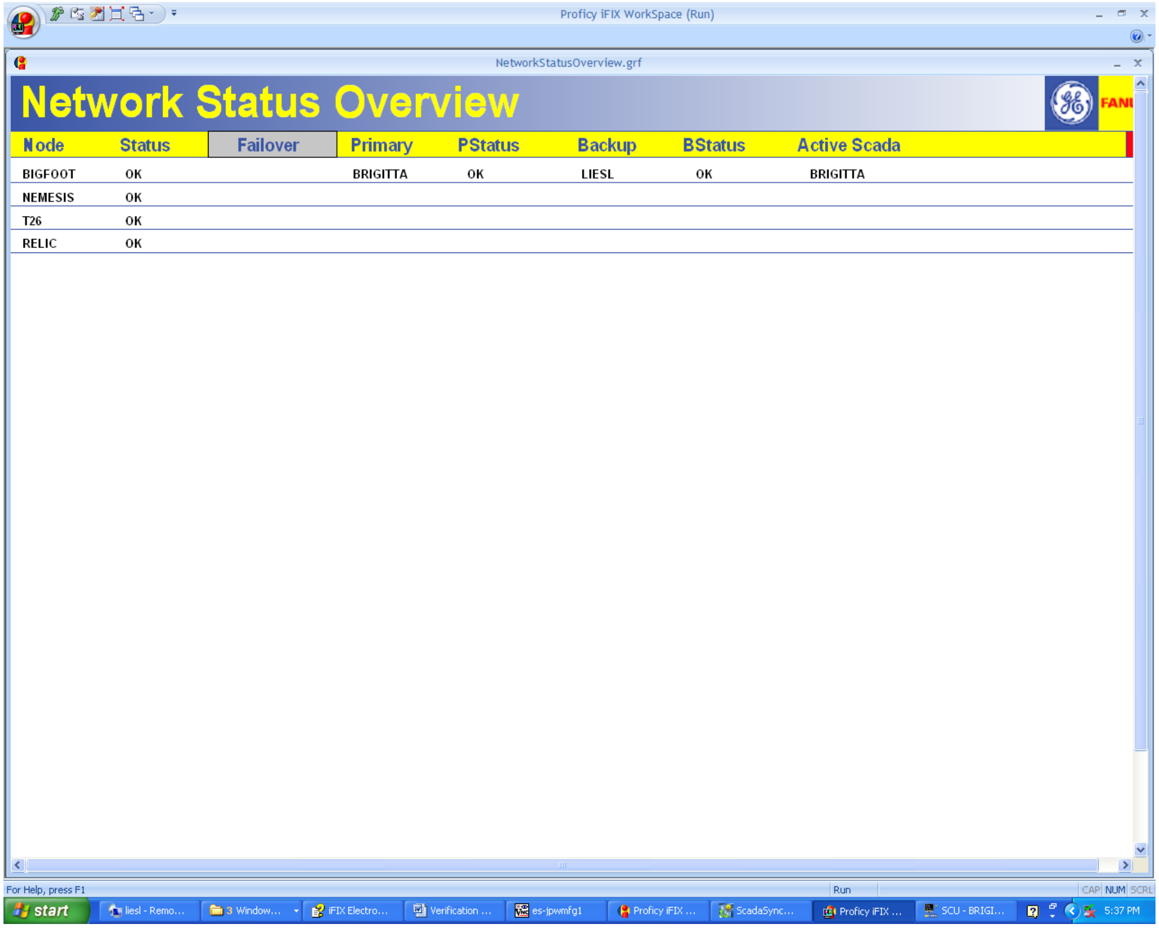
SECONDARY SCADA ROLE ####.## DATADATA

Logical.AI-1.F_CV #####.##

Ack	Time In	Time Last	Node	Tagname	Status	Value

Total Alarms: 0 Filter: Off Sort: Time In, Descending

Network Status Overview Picture



Node	Status	Failover	Primary	PStatus	Backup	BStatus	Active Scada
BIGFOOT	OK		BRIGITTA	OK	LIESL	OK	BRIGITTA
NEMESIS	OK						
T26	OK						
RELIC	OK						

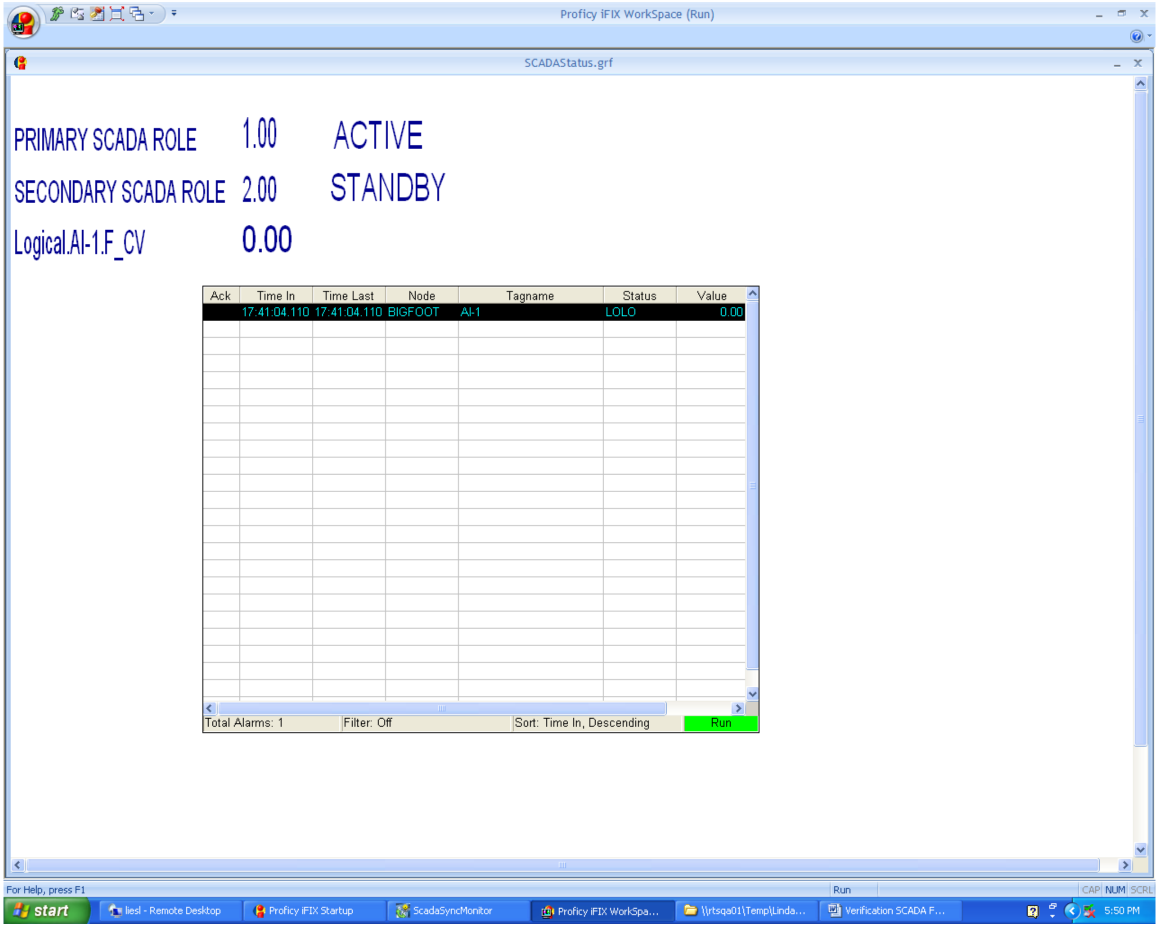
1. Look at the SCADAStatus picture created earlier on each Client (Primary, Secondary and View).

2. The PRIMARY SCADA ROLE value should be 1 (ACTIVE).

3. The SECONDARY SCADA ROLE value should be 2 (STANDBY).

4. The Datalink for the tag should have the correct value (value in Primary's PDB).

5. Alarm Summary should show any existing alarms and the same number of alarms should appear on each Client.



PRIMARY SCADA ROLE 1.00 ACTIVE

SECONDARY SCADA ROLE 2.00 STANDBY

Logical.AI-1.F_CV 0.00

Ack	Time In	Time Last	Node	Tagname	Status	Value
	17:41:04.110	17:41:04.110	BIGFOOT	AI-1	LOLO	0.00

Total Alarms: 1 Filter: Off Sort: Time In, Descending Run

6. On the Primary’s Client SCADAStatus picture:

    - Change the AI tag value via the Datalink to one that will generate an alarm.
    - Confirm the new data value and generated alarm appears in the picture on each Client.
    - Acknowledge the alarm from the Primary Client.
    - Confirm the acknowledgement check mark appears on each Client.
    - Change the AI tag value to one that will clear the alarm.
    - Confirm the new data value appears on each Client’s picture and the alarm is cleared.

7. Repeat the above steps from the Secondary Client and View node Client.

Using the Test Picture

Test manually switching the scada role:

1. On the Primary’s Client SCADAStatus picture, manually change the PRIMARY SCADA ROLE Datalink:

   Fix32.<Primary’s Local Node Name>.NSD.F_SWITCHSCADAROLE from 1 (ACTIVE) to 2 (STANDBY).

2. The SECONDARY SCADA ROLE Datalink Fix32.<Secondary’s Local Node Name>.NSD.F_SWITCHSCADAROLE value should automatically change from 2 (STANDBY) to 1 (ACTIVE) in the SCADAStatus picture on all Clients.

3. The ACTIVE SCADA on the NetworkStatusOverview.grf should switch to the Local Node Name of the Secondary SCADA on all Clients.

4. The alarms should continue to match on all Clients.

5. On the Secondary Client, switch the ACTIVE role back to the Primary by changing the SECONDARY SCADA ROLE Datalink value back to 2 (STANDBY).

6. The PRIMARY SCADA ROLE Datalink value should automatically change to 1 (ACTIVE).

7. The ACTIVE SCADA on the NetworkStatusOverview.grf should switch back to the Local Node Name of the Primary SCADA on all Clients.

8. The alarms should continue to match on all Clients.

9. You should be able to change the data value of the AI tag and have the new value appear on each Client, generate and acknowledge alarms on each Client.

Test shutting down iFix to cause a failover:

1. Primary SCADA should currently have ACTIVE SCADA Role.

2. Close down iFIX on the Primary SCADA.

3. The Secondary SCADA role should change to 1 (ACTIVE) on Secondary Client and View Client.

4. NetworkStatusOverview.grf should show the ACTIVE SCADA switch from the Primary Local Node Name to the Secondary’s Local Node Name.

5. The Status of the Primary will show error 1914.

6. The alarms should continue to match on the Secondary and View Client.

7. You should be able to change the data value of the AI tag and have the new value appear on each Client, generate and acknowledge alarms on Secondary and View Client.

8. Restart iFIX on Primary SCADA. Secondary SCADA should remain with the ACTIVE role and the Primary should have STANDBY role.

9. Open and run NetworkStatusOverview.grf and SCADAStatus picture on Primary Client. Client should point to the ACTIVE Secondary SCADA.

10. The alarms should match the alarms appearing on the Secondary Client.

11. You should be able to change the data value of the AI tag on Primary Client and have the new value appear on all Clients. You should be able to acknowledge alarms from Primary Client and see acknowledgement on other two Clients.

Test removing the FIX network cable (non FIX LAN Redundancy):

1. Pull one the iFIX Network cables from the ACTIVE Primary SCADA.

2. The Primary SCADA will remain ACTIVE. The Secondary should remain STANDBY.

3. Alarms should match on all Clients.

4. You should be able to change the data value of the AI tag and have the new value appear on each Client, generate and acknowledge alarms from all Clients.

5. Pull the second iFIX Network cable from the ACTIVE Primary SCADA.

6. The Secondary SCADA role should change to 1 (ACTIVE) and the Primary SCADA role should change to 2 (STANDBY).

7. NetworkStatusOverview.grf on the Secondary and View Clients should show the ACTIVE SCADA switch from the Primary Local Node Name to the Secondary's Local Node Name.

8. The Status of the Primary will show error code.

9. The Primary Client will have the Primary Local Node Name as the ACTIVE SCADA since it cannot reach the Secondary SCADA (no network connection). A pop-up notification will indicate that the Client is connected to the Standby node and data is read-only. Data is updated at a rate determined by the synchronization link.

10. The alarms should continue to match on the Secondary and View Client.

11. You should be able to change the data value of the AI tag and have the new value appear on each Client. New value will also appear on Primary Client if there is a separate DataSync network connection from the two LAN Redundant iFIX connections.

12. Plug both network cables back in Primary SCADA. Network connections should re-establish to Secondary and View Client.

13. Primary SCADA will have STANDBY role and Secondary will still have ACTIVE role.

Test DataSync:

1. One DataSync network connection setup.

2. Open Database Manager on Primary SCADA using Local Node Name and select PDB.

3. Open Database Manager on Secondary SCADA using Local Node Name and select same PDB.

4. On Primary Client, open the SCADAStatus picture and change the AI tag value.
5. Via Database Manager, confirm new value is updated to PDB on both SCADAs.
6. Within Database Manager on Primary SCADA, change value of tag.
7. Confirm new value is updated to Secondary’s PDB.
8. Within Database Manager on Secondary SCADA, try to change value of tag.
9. Should receive the error: “Can not write value. The SCADA node is in Standby mode.”
10. Pull DataSync cable from Primary.
11. Both SCADAs should go to ACTIVE.
12. View Client NetworkStatusOverview.grf should point to one of the ACTIVE SCADAs (could be either the Primary or Secondary).
13. Change tag value via SCADAStatus picture on Primary Client.
14. Only the PDB on the Primary SCADA should show new value.
15. Secondary SCADA PDB will still show old value.
16. Change tag to different value via SCADAStatus picture on Secondary Client.
17. Only the PDB on the Secondary SCADA should show new value.
18. Primary SCADA PDB will show previous new value.
19. Plug DataSync cable back into Primary SCADA.
20. Primary SCADA will remain ACTIVE. Secondary SCADA will go to STANDBY.
21. View Client and Secondary Client will switch ACTIVE SCADA to Primary’s Local Node Name on NetworkStatusOverview.grf.
22. Values from Primary’s PDB will be written to Secondary’s PDB.

Enhanced Failover Troubleshooting

The following section describes how to locate error messages. Also included is a troubleshooting matrix to help you resolve issues.

Errors Messages

Error messages can be found in:

- iFIX Alarm Typers (Destinations)

  Alarms to File, Alarm ODBC or the Alarm History window
- SCADASync.log

  Usually located in the folder: C:\Program Files\Proficy\Proficy iFIX\LOCAL
- ScadaRoleMgr.log

  Modify the FIX.INI file so the log file includes more information. See INI file section for more information.
- iFIX .EVT file

  Usually found in C:\Program Files\GE Fanuc\Proficy iFIX\ALM
- Modify the SCADASYNC.INI file so the log file does not get overwritten. See INI file section for more information.

Troubleshooting Matrix

Issue	Resolution
SCADA Failover feature is not enabled in the license for this node.	This error found in ScadaRoleMgr.log indicates that your key does not support the Enhanced Failover feature. Check your key in the Proficy License Viewer, and contact GE Fanuc to purchase an upgrade or replace a defective key. You will also get an Error popup message at iFIX startup indicating SCADA failover feature is not enabled in the license for your node. You must purchase the additional Enhanced Failover option (SCADA Failover) for all SCADA nodes if you plan to use SCADA Failover in iFIX 5.0 or higher.
PDB Sync Loadable Block <blockname> Not defined locally. PDB Sync Loadable Block <blockname> Not defined on remote node. PDB Sync Loadable Block Mismatch locally <blockname> version <ver> remote <blockname> version <ver>.	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.
Both SCADAs are active (as displayed in ScadaSyncMonitor or as indicated by messages in alarm services destinations).	Verify your Ethernet connection being utilized for SCADA Synchronization (preferably this is a dedicated LAN connection). On both SCADAS, in the Task Manager, verify that ScadaSync.exe and ScadaRoleMgr.exe are listed. On both SCADAS, in the SCU, check your Failover configuration. Check that the Data Synch Transport is configured for the appropriate LAN adapter and the Partner's Address is correctly defined.
iClient with logical node names cannot connect to a partner SCADA.	Make sure that the iClient is configured properly. Refer to the Configuring iClients section in the iFIX electronic books. Make sure the iClient machine can ping the SCADA node(s) using the iFIX node name. Verify the Hosts files are configured correctly on all nodes.

Issue	Resolution
The driver configuration is causing issues. For instance, blocks are going off scan, or question marks appear for data links (the default indication that there is no data, and is defined in the User Preferences).	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.
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.	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.
iClient nodes display error message number 1914, every time the active SCADA switches.	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. 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 of the iFIX e-books.
Connection Not Established With Node.	When any iClient loses its iFIX networking session with a remote node, this error to appears in alarm service destinations. Check your Ethernet connections.
iFIXNotification dialog displays for an extended length of time.	iFIXNotification dialog displays when iClient is only able to communicate with a standby SCADA node. Check your Ethernet connections being used for iFIX networking.

Issue	Resolution
Standby SCADA displays "Connection Failover: failover attempted" message every minute in alarm services destinations	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.
Scada Sync Monitor shows the IP address as 0.0.0.0 for the sync NIC card, the color may remain green	Windows Media Sense may be enabled. To disable: Start Registry Editor. Locate the following registry subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Add the following registry entry to the Parameters subkey: Name: DisableDHCPMediaSense Data type: REG_DWORD (Boolean)
Scada Sync Monitor shows both SCADAS as Active and the color is red	The scada's cannot see each other. This could be for a number of reasons: - The IP address associated with the NIC card definition in the FIX SCU data sync configuration is incorrect as compared to the control panel network configuration. Look closely at the IP / NIC definition in scada sync monitor. If incorrect the FIX SCU needs to be rebuilt from new. - The cable or switch between the scada's is not functioning correctly - The NIC card is set to Jumbo frames but the cable has not been updated to CAT6 - Scadasync.exe or Scadarolemgr.exe has exited unexpectedly on one of the scada's - settings within the NIC card do are mismatched - power savings settings are enabled on the NIC card - the SCADA was upgraded and still using the old FIX.INI that does contain entries to load Scadasync.exe or Scadarolemgr.exe - The SCU could have become corrupt, save the existing SCU to a different name. Using the original SCU as a guide build a brand new SCU file and save to the original file name. Restart the SCADA.

Issue	Resolution
SCADA Sync Monitor shows both SCADAS as Standby	The SCADAS cannot see each other. This could be for a number of reasons: - The IP address associated with the NIC card definition in the FIX SCU data sync configuration is incorrect as compared to the control panel network configuration. Look closely at the IP / NIC definition in SCADA sync monitor. If incorrect the FIX SCU needs to be rebuilt from new. - The cable or switch between the SCADAS is not functioning correctly - The NIC card is set to Jumbo frames but the cable has not been updated to CAT6 - Scadasync.exe or Scadarolemgr.exe has exited unexpectedly on one of the SCADAS - settings within the NIC card do are mismatched - power savings settings are enabled on the NIC card - the SCADA was upgraded and still using the old FIX.INI that does contain entries to load Scadasync.exe or Scadarolemgr.exe - The SCU could have become corrupt, save the existing SCU to a different name. Using the original SCU as a guide build a brand new SCU file and save to the original file name. Restart the SCADA.

Misc - Dispatching SCADA Alarms

Dispatching alarms from the SCADA to the clients can be improved by adding a registry setting.

Configurable Nam Sleep Interval

This feature will be implemented on the iFIX SCADA Nodes.

The purpose of the **Configurable Nam Sleep Interval** is to permit the end user to configure the sleep timer from which iFIX SCADA nodes dispatch alarms out of the MgrRcv queue of the Network Alarm Manager (NAM) to the attached Client nodes.

If the “NamSleepInterval” key does not exist, then the iFIX SCADA will distribute alarms to all attached clients using the default NAM sleep interval of 200 milliseconds.

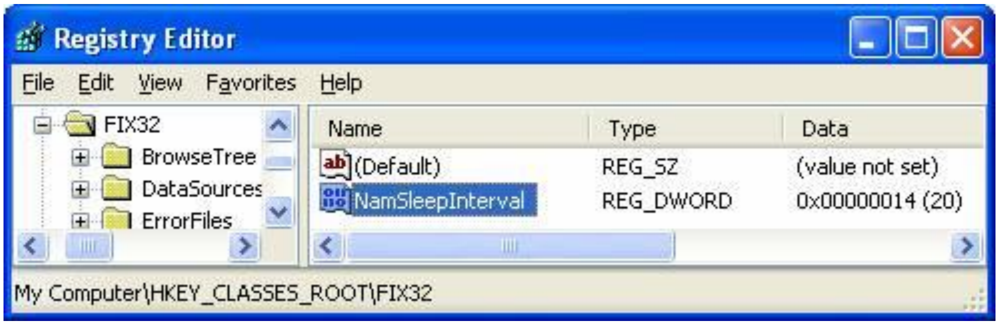
If the “NamSleepInterval” does exist, and contains a valid value between 1 and 1000, then the iFIX SCADA node will distribute alarms to the attached clients using the configured “NamSleepInterval”. If it contains an invalid value, then it will default to the default NAM sleep interval of 200 milliseconds.

Note: It is not recommended to go below the value of 50.

The NamSleepInterval is in units of milliseconds. Please be aware that using a small NamSleepInterval values may increase the rate at which alarms are distributed to clients, the overall system performance could suffer from a value being too small. Please test this value under a variety of operating conditions to ensure the system responds as you expect prior to putting it into a production environment.

To implement this feature, do the following

1. In the registry create a New…DWORD Value named “NamSleepInterval” in HKEY_CLASSES_ROOT\FIX32.



Name	Type	Data
(Default)	REG_SZ	(value not set)
NamSleepInterval	REG_DWORD	0x00000014 (20)

My Computer\HKEY_CLASSES_ROOT\FIX32

2. Make sure the base decimal is selected, then set the value of “NamSleepInterval” to any number from 1 to a 1000

3. Exit the registry.

- Accepts on the fly changes, the thread will check once every few minutes to see if there have been any changes made to the NamSleepInterval registry key and will change the Nam sleep time accordingly

  If the NamSleepInterval exists in the registry and if the value changes from the default 200ms, then an event message will be output to the iFix Event file indicating the new change