Honeywell

Experion PKS
Series C IEC 61850 Interface Module User's Guide

EPDOC-X374-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X374-en-431A	431	0	February 2015

Disclaimer

Contents

1 About this document

This document provides information about planning, installing, configuring and operating the hardware and software components associated with the IEC 61850 Interface Module (850M).

Revision history

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

Intended audience

This guide is intended for engineers who configure the following:

- Integration of IEC 61850 into the Experion system using the IEC 61850 Interface Module.
- Intelligent Electronic Device(IED) communication with C300 Controller.

Prerequisite skills

- Familiar with working in a Microsoft Windows operating environment.
- Familiar with Experion system topology and using Experion applications.
- Familiar with using Control Builder.
- Familiar with basic principles of IEC 61850 technology and standards.

Related documents

You may also refer to the following related Experion documents.

Document	Description
Overview	Provides a comprehensive overview of Experion, including basic concepts and terminology.
Control Building User's Guide	Describes how to perform tasks within the Control Builder application such as configuring hardware devices, continuous control strategies, and sequential control strategies.
C300 Controller User’s Guide	Provides information for planning, designing, installing, operating and troubleshooting C300 process controllers in an Experion system.
Control Hardware Planning Guide	Provides an overview of things you should consider when planning for the installation of your Series C cabinet.

2 Introduction

This section provides information about IEC 61850 control integration you must know before introducing it in an Experion network.

Related topics

“About IEC 61850” on page 10
“IEC 61850 control integration in Experion” on page 11
“850M functional overview” on page 13
“IEC 61850 terms and definitions” on page 14

2.1 About IEC 61850

This section gives an overview of the IEC 61850 protocol. It also lists the available IEC 61850 standards.

About IEC 61850 protocol

IEC 61850 is a global standard for the design of electrical substation automation. IEC 61850 is a part of the International Electrotechnical Commission's (IEC) technical committee reference architecture for electric power systems. It enables the integration of protection, metering, monitoring and control functions with one common protocol. It supports a comprehensive set of substation functions.

This protocol runs over TCP/IP networks or substation LAN using high speed switched Ethernet to obtain the necessary response times for protective relaying.

The IEC 61850 standards specification document is available in the IEC website (http://www.iec.ch).

IEC 61850 features

Some of the features of IEC 61850 include:

- Enables use of multi-vendor electrical devices on a common bus network facilitating integration, device engineering and fast response.
- Ensures easy introduction of newer devices into the electrical network without the need for removing the older devices.
- Supports large number of diagnostic parameters.
- Reduces costs of installation, commissioning and maintenance.

2.2 IEC 61850 control integration in Experion

This section gives an overview of IEC 61850 control integration and how it is used in the Experion environment.

The IEC 61850 control integration solution integrates the IEC 61850 MMS protocol and data model with C300 Controller using an 850M interface module for the data to be available for controller application.

The 850M is a hardware/firmware module in IEC 61850 control integration which provides an interface between an associated C300 Controller via Fault Tolerant Ethernet (FTE) and an IEC 61850 network.

The integration of IEC 61850 into Experion system supports MMS communication protocol options described in the IEC 61850 standard. (GOOSE communication is not supported). MMS communication for IEC 61850 is integrated using 850M and Experion SCADA interface. The 850M has direct access to IED data such as current and voltage measurements, status, interlocking.

Intelligent Electronic Device (IED) representation such as physical devices, logical devices and logical nodes (as defined in the IEC 61850 specifications) are integrated to the Control Builder and SCADA interface. Therefore all Experion system features including graphics, faceplates, alarms and event lists including time-stamped alarms and events (SOE), and historian capabilities are available for IED data.

The following figure explains IEC 61850 control integration in Experion.

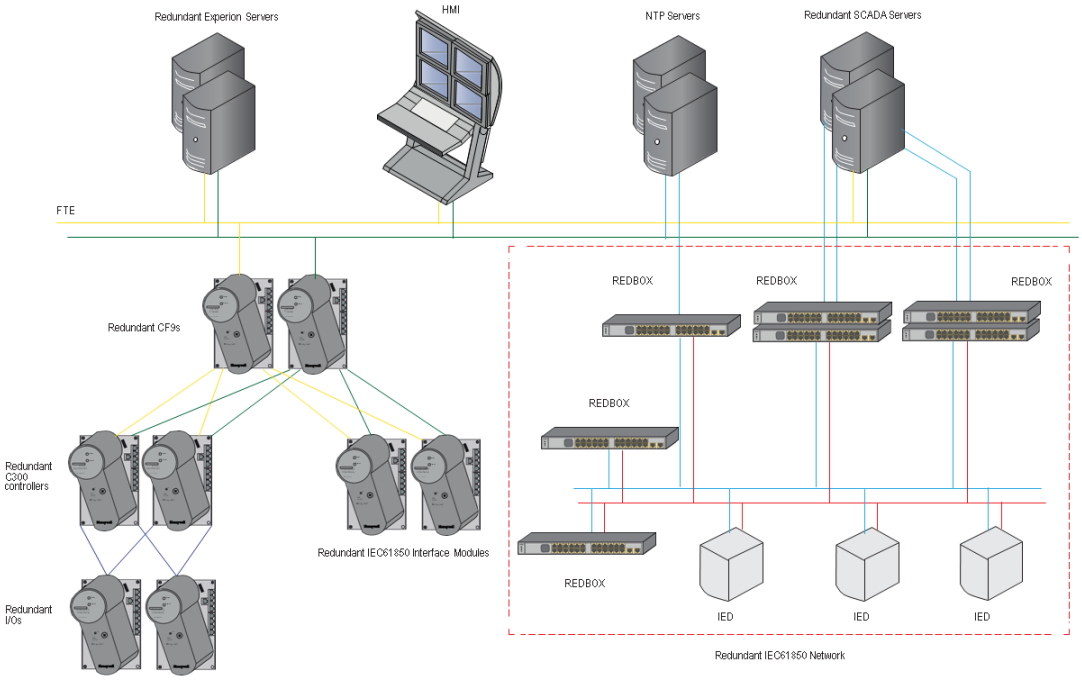


Figure 1: IEC 61850 control integration in Experion

850M supports the following functions.

- Redundancy
- Experion events and alarms
- Bulk edit and bulk build
- Peer-to-peer communications

IEC 61850 control integration overview

The 850M allows communication between C300 Controllers in the Experion system and IEDs at the controller level. This is achieved by providing an interface to IEC 61850 networks (850M) for the C300 Controller.

IEC 61850 control integration in Experion system offers the following:

- Reduces wiring by introducing IEC 61850 as a standard for Ethernet based communication solutions.
- Integrates process automation and power automation operations and control.
- Enables measure and control using IEC 61850 IEDs (MMS only).
- Improves access to electrical and process data from the entire plant.

Benefits of IEC 61850 control integration in Experion

- Experion control system is capable of operating in process and power generation plant automation.
- An Experion-based environment can be used across both process and electrical control systems resulting in lower engineering costs and more effective operation of the integrated systems.
- More electrical devices (IEDs) can communicate with a single C300 Controller than is possible using a PCDI-based interface to IEDs. This results in requirement of fewer C300 Controllers.
- The ability to reference IED data without manual mapping increases the ease with which systems are configured and decreases project engineering costs.
- The use of the C300 Controller-850M to control the responses of process equipment and controlled processes to disturbances in power generation and distribution in an installation.

2.3 850M functional overview

This section provides details of the representation of 850M in the Control Builder.

The following figure shows how icons are used for identifying Series C 850M hardware, and representing Intelligent Electronic Device (IEDs) as physical devices, logical devices and logical nodes (as defined in the IEC 61850 specifications) in the Control Builder Project tree.

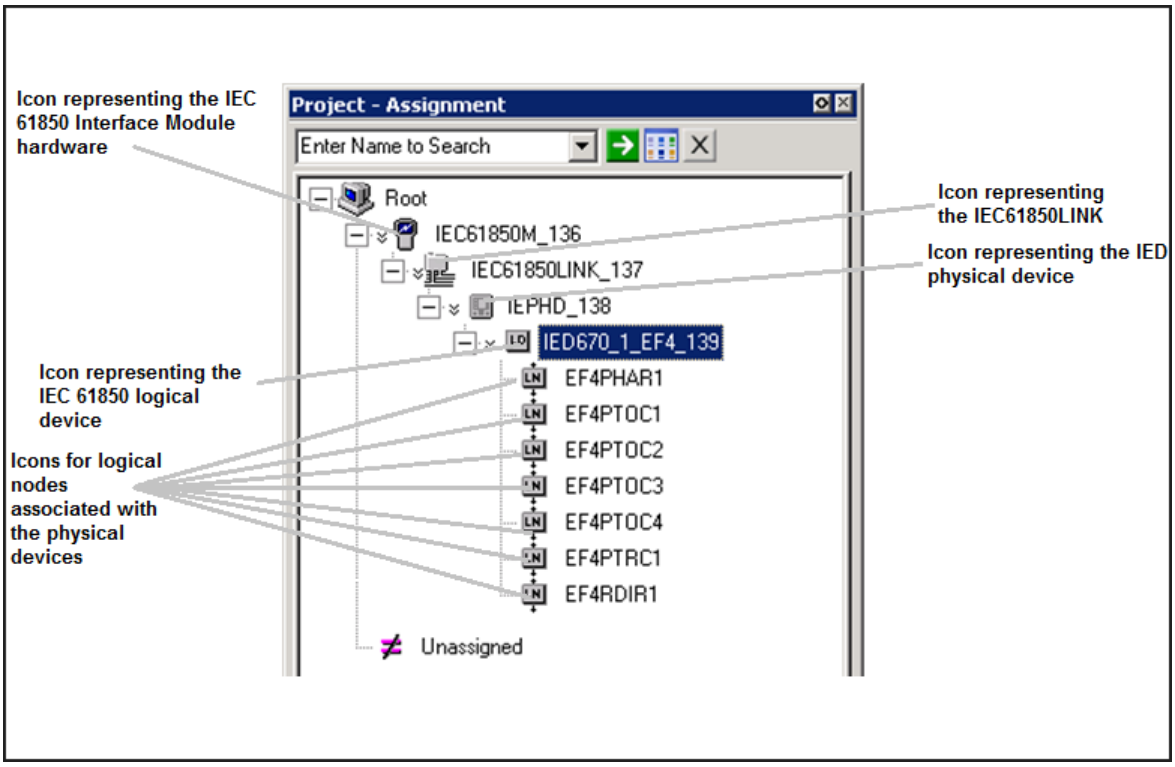


Figure 2: IEC 61850 hardware/function block hierarchy in Project tree

2.4 IEC 61850 terms and definitions

This section provides information about the terms and definitions associated with IEC 61850 control integration used in the document.

These are used throughout this guide in the following context.

Term	Definition
Client	850M is a client and only the client can initiate requests
Dual home	Dual-home/ dual homing is a network topology where a network device is built with more than one network interface.
GOOSE	Generic Object Oriented Substation Events A protocol defined in IEC 61850 which supports fast, reliable and simultaneous transmission of data across an entire substation network. Publication of data by a compliant device on the network to which it is attached should occur within a maximum delay of 4 ms.
HSR	High Availability Seamless Redundancy High Availability Seamless Redundancy protocol is a refinement of PRP standardized in IEC 62439-3 clause 5 which is specific to ring topologies and provides zero switch-over time.
IEC 61850	This is an IEC standard developed by IEC technical committee 57 in support of electrical substation automation. It defines a logical representation of devices complying with the standard and mapping of this logical representation to various protocols, currently including the following: • MMS • GOOSE • Sampled values This standard definition supports interoperability between devices from various third-party providers which are used in electrical substation (and other power distribution and management) automation systems.
HV	HV (High Voltage) Power distribution systems are divided into High Voltage (HV), Medium Voltage (MV) and Low Voltage (LV) power busses or transmission networks. High Voltage networks are used when power is transmitted over long distances.
ICD	IED Capability Description (ICD) This file describes the capabilities of a specific IED. It is provided by the manufacturer of the device. It contains the following sections. • IED • Communications *(optional)* • Substation (indicates the physical entities associated with the IED) *(optional)* The ICD is created using the Substation Configuration Language (SCL).
CID	Configured IED Description (CID) This files describes an instantiated IED with configuration parameters for that IED. It is used for communication between an 850M and an IED. It contains the following sections. • IED • Communications • Substation (indicates the physical entities associated with the IED) *(optional)* The CID is created using the Substation Configuration Language (SCL).
850M	This hardware/firmware module in IEC 61850 control integration provides an interface between an associated C300 Controller via Fault Tolerant Ethernet (FTE) and an IEC 61850 network.

Term	Definition
IEC61850LINK block	In Control Builder, the IEC61850LINK block represents the IEC 61850 network to which the 850M is connected.
IED block	The IED block represents a physical device on the IEC 61850 network to which the 850M is connected.
IED	Intelligent Electronic Device (IED) An intelligent control and messaging device used for interfacing substation automation controllers and networks to target electrical equipment such as relays, circuit breakers, and so on.
850M block	An 850M block is an Experion block representing this 850M platform.
LD block	Logical device block An LD block is an Experion block representing a logical device associated with and logically contained by an IED (which is represented by an IED block).
Logical Device/LD	Within the context of the IEC 61850 control integration, a logical device is a logical object contained by a physical device (IED). A physical device can contain (1 ... n) logical devices. This allows a physical device to act as data concentrator or gateway for multiple logically distinct devices. Each logical device contains a collection of logical nodes.
LN block	Logical node block An LN block is an Experion block representing a logical node contained within a logical device which is in turn contained by an IED.
Logical Node/LN	A logical node is a named grouping of data and associated services that is in some way related to a power system function.
LV	Low Voltage (LV) Power distribution systems often are divided into High Voltage (HV), Medium Voltage (MV) and Low Voltage (LV) power busses or transmission networks. Low Voltage networks are the last leg of a power distribution system, bringing power to equipment, motors and other consumers.
Load shedding	Load shedding is the act or process of disconnecting current sinks (consumers of electrical current/power) from an electrical power distribution system when demand for electrical power in the system exceeds supply. This would typically occur when an electrical generator is taken off line or unexpectedly goes offline.
MMS	Manufacturing Messaging Specification (MMS) This is an international standard, ISO 9506, under the auspices of ISO technical committee 184 (TC184), defining a messaging system to be used in the transfer of real time process data and supervisory control data between devices in a network. It defines the following major features: • A set of standard objects which must exist in every compliant device • Support for a set of standard operations on the above objects (for example, read, write) • A set of standard messages which are exchanged between a client and a server in order to monitor or control the standard objects referred to above • A set of encoding rules for mapping these messages to bit, byte and frame order and meaning when sent across a network. (This uses the Abstract Syntax Notation - ASN.)
MV	Medium Voltage (MV) Power distribution systems often are divided into High Voltage (HV), Medium Voltage (MV) and Low Voltage (LV) power busses or transmission networks. Medium Voltage networks are typically used when power is transmitted over medium distances and to power equipment with relatively high power demands.
NTP	Network Time Protocol NTP is a standardized internet networking protocol used for synchronizing computer clock times in a distributed network of computers.

Term	Definition
PRP	Parallel Redundancy Protocol PRP provides layer 2 network redundancy by sending two copies of the same frame over two independent networks. A Redundancy Control Trailer (RCT) is added to each frame (which includes a sequence number to support detection of duplicate messages so that one may be discarded.) It supports zero failover time.
Redbox	Redundancy box Redbox is a switch that enables non-HSR or non-PRP nodes like the 850M to connect to an HSR or PRP network.
Reference block	A Reference block is a new Experion block to be defined and implemented as part of the UIO Modular Configuration project. It serves as a proxy for a named parameter reference when the target block/parameter is not yet loaded. As a proxy, it supports simulation of the target parameter. When the target block/parameter is loaded, the intended association with the target parameter is created.
SAS	Safety and Automation System (SAS) A term used for describing both the *Safety Instrumented System* and *Process Control System* taken together as a component of the automation architecture of a manufacturing or production site. In turn, the process control system is composed of a basic process control system which include sub systems related to power distribution and management. • Power distribution control system • Power management system The power management system is responsible for load shed control.
Server	The IEC 61850 IED device that sends reports to clients and responds to I/O commands. The server can only respond to requests, and cannot initiate them.
SCD	Substation Configuration Description (SCD) This file describes the complete substation in detail. It contains template sections for the following: • The substation in its entirety • Communications • IEDs • Data types This description is specified using the SCL (Substation Configuration Language).
SCL	Substation Configuration Language (SCL) This is an XML-based description language and representation format defined by the IEC 61850-6 specification for use in producing various descriptor files associated with the IEC 61850 specification. Use of this standard language in defining descriptor files for IEC 61850 networks supports interoperability between different third-party devices and tools used on IEC 61850 networks.

3 Series C 850M Planning and Design

This section includes information and tasks associated with planning and designing an Experion system to include IEC 61850 devices.

Related topics

“General planning references” on page 18
“Identifying 850M components” on page 19
“IEC 61850 control integration topologies” on page 21
“IEC 61850 network device and IED support policy” on page 25
“Reviewing 850M performance data” on page 26

3.1 General planning references

This section provides information for planning and designing an Experion system and the FTE network.

Refer to the following documents for planning and design details for the Experion system in general and the Fault Tolerant Ethernet supervisory network.

- Control Hardware Planning Guide
- Server and Client Planning Guide
- Fault Tolerant Ethernet Overview and Implementation Guide
- IEC 61850 SCADA Configuration Guide

3.2 Identifying 850M components

This section identifies the 850M components required to provide an IEC 61850 interface with Experion.

The following table identifies the Series C 850M components required to provide an interface with an Experion system. The CC prefix in a model number means the component's printed wiring boards are coated to provide additional protection from the environment.

Component	Description	Model number
Series C 850M	Module mounts on non-redundant or redundant Input/Output Termination Assembly. Serves as a gateway between the Experion system (C300 Controller) and IEC 61850 network.	CC-P850A1
IEC 61850 usage licenses	Count of in-use IEC 61850 Interface Module per server.	TC-850L01
	1 module	
Input/Output Termination Assembly (IOTA) (IEC 61850)	Provides physical connection to Series C 850M. Mounts on carrier in Series C cabinet.	CC-T850A1
9 Port FTE Control Firewall Module	Provides FTE distribution to in-cabinet network nodes	CC-PCF901 CU-PCF901
9 Port Control Firewall IOTA	Provides connection for FTE cables from in-cabinet controllers and 850Ms.	CC-TCF901 CU-TCF901
FTE Cable	STP CAT5 Cable with RJ 45 connectors for FTE connections.	
	2 m (6.5 ft) (Y) = Yellow coded boots (G) = Green coded boots	51305482-102 (Y) 513054820202 (G)
	5 m (16 ft)	51305482-105 (Y) 513054820205 (G)
	10 m (33 ft)	51305482-110 (Y) 513054820210 (G)
	20 m (65.5 ft)	51305482-120 (Y) 51305482-220 (G)
Redundancy Cable	STP CAT5 Cable with RJ 45 connectors joining primary and secondary controllers.	51305482-xxx
IOTA Channel Supports	Aluminum channels that provide a mounting medium for the IOTA Channel.	CC-MCHN01
IOTA Channel	Assembly for mounting Series C hardware IOTAs. Channels contain power and grounding busbars are mounted onto IOTA channel supports.	CC-MCAR01
Power Supply, Non-redundant no Battery Back Up	24 Vdc, 20 Amp. power supply. Provides non-redundant power to Channel busbars and Series C IOTAs.	CC-PWRN01
Power Supply Redundant, no Battery Back Up	24 Vdc, 20 Amp. fully redundant power supply. Provides redundant power to Channel busbars and Series C IOTAs.	CC-PWRR01
Power Supply, Redundant with Battery Back Up	24 Vdc, 20 Amp. fully redundant power supply with battery back up. Provides redundant power to Channel busbars and Series C IOTAs.	CC-PWRB01

Component	Description	Model number
COTS Power Supply (Meanwell) Redundant, no Battery Back Up	24 Vdc, 20 Amp. COTS power supply. Provides redundant power to Channel busbars and Series C IOTAs	CU-PWMR20
COTS Power Supply (Meanwell) Non-redundant, no Battery Back Up	24 Vdc, 20 Amp. COTS power supply. Provides non-redundant power to Channel busbars and Series C IOTAs	CU-PWMN20
COTS Power Supply (Phoenix Contact) Redundant, no Battery Back Up	24 Vdc, 20 Amp. COTS power supply. Provides redundant power to Channel busbars and Series C IOTAs	CU-PWPR20
COTS Power Supply (Phoenix Contact) Non-redundant, no Battery Back Up	24 Vdc, 20 Amp. COTS power supply. Provides non-redundant power to Channel busbars and Series C IOTAs	CU-PWPN20

3.3 IEC 61850 control integration topologies

This section provides information about the different topologies for IEC 61850 control integration.

Network recommendations for creating IEC 61850 control integration topologies

- Configurations should not be created in which both the Experion process server and IEC 61850 SCADA server reside in the same physical node.
- The IEC 61850 network should not be directly connected to an L3 router. If access to L3 is required, it is recommended to use an L 2.5 router to connect FTE and IEC 61850 networks together. The L 2.5 router should connect to the L3 router.
- To disable Microsoft Windows Client and File Sharing options for the IEC 61850 ports on the SCADA Server:
  - Ensure lower MAC address is selected for FTE network installation. If Experion is installed on servers like Dell 320, then this machine consists of 4 built-in NIC interfaces, Use the first two NICs for FTE connection and other two NICs for IEC 61850 network connections. If you have additional dual NICs on 2 NIC built-in type servers, ensure that lower MAC address NIC is selected for FTE. With this setup, Experion installation automatically selects the lower MAC interfaces (1st two interface of built-in NICs) for FTE and System Management and also sets proper binding order that FTEMUX is on top.
  - Also, need to interface TCP/IPv4 metric on both the IEC 61850 interfaces to 5 and 10.
  - Disable NETBIOS on both IEC 61850 interfaces.
  - In addition, the IEC 61850 settings must not include a gateway address on either interface, assuming that there is a gateway address on the FTEMUX.
- Do not connect IEC 61850 network to the FTE ports.
- Enable the **Flow Control** option on the IEC 61850 switch ports connected to the 850Ms

3.3.1 IEC 61850 non-redundant Ethernet ring topology model

The following diagram portrays the non-redundant topology configuration for the various physical components for an 850M and the related Experion L2 nodes, L1 embedded nodes, and FTE and IEC 61850 network equipment.

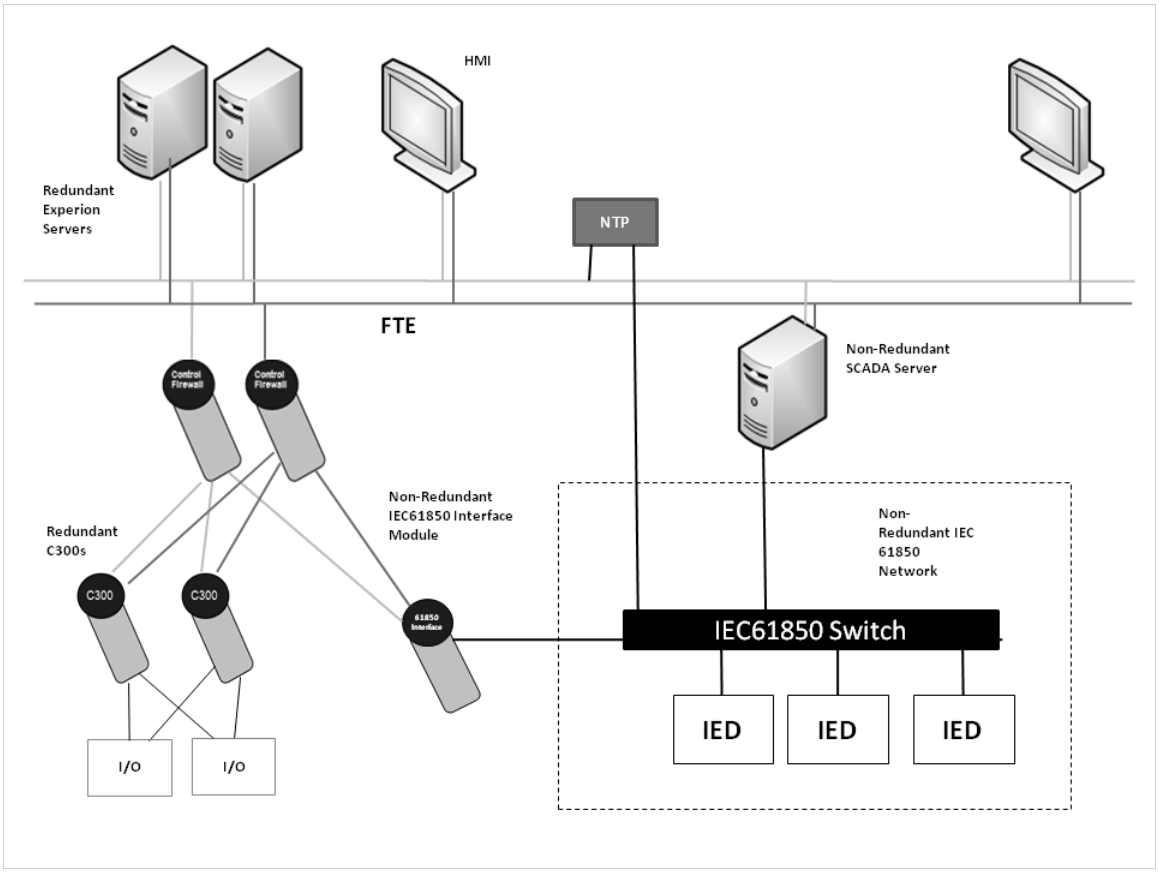


Figure 3: IEC 61850 non-redundant Ethernet ring topology model

3.3.2 HSR topology model

This diagram portrays the HSR ring topology configuration for the various physical components for an 850M and the related Experion L2 nodes, L1 embedded nodes, FTE and IEC 61850 network equipment.

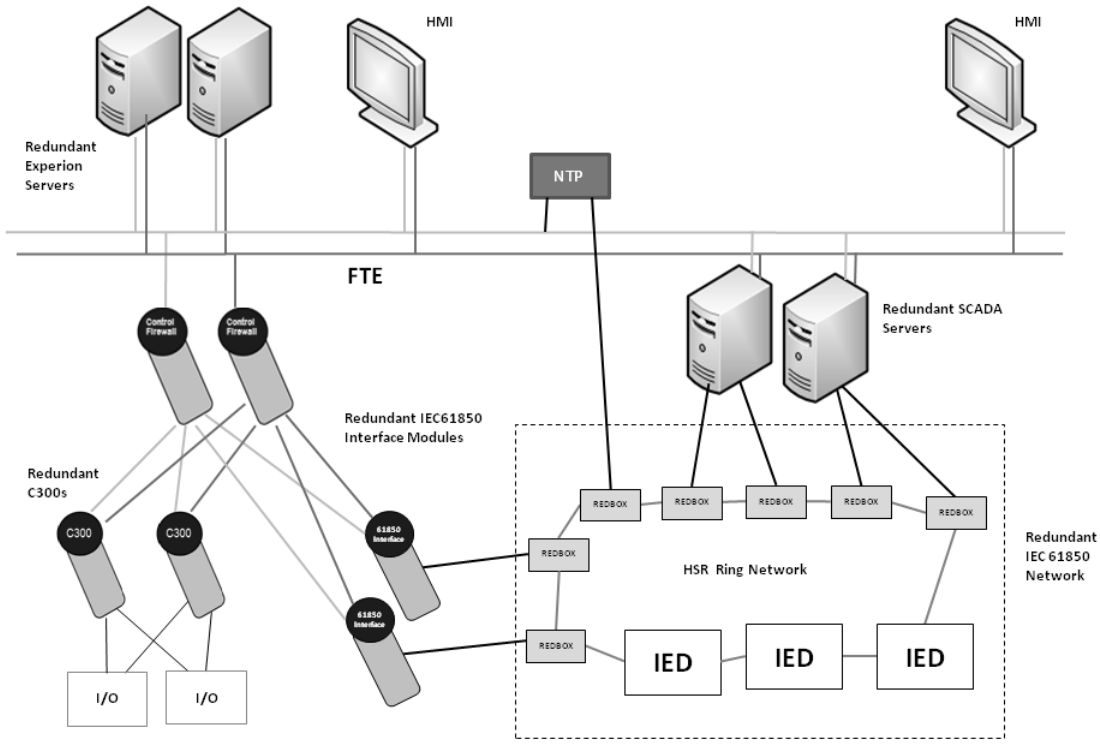


Figure 4: HSR topology model

3.3.3 PRP topology model

This diagram portrays the deployment PRP topology configuration for the various physical components for an 850M and the related Experion L2 nodes, L1 embedded nodes, FTE and IEC 61850 network equipment.

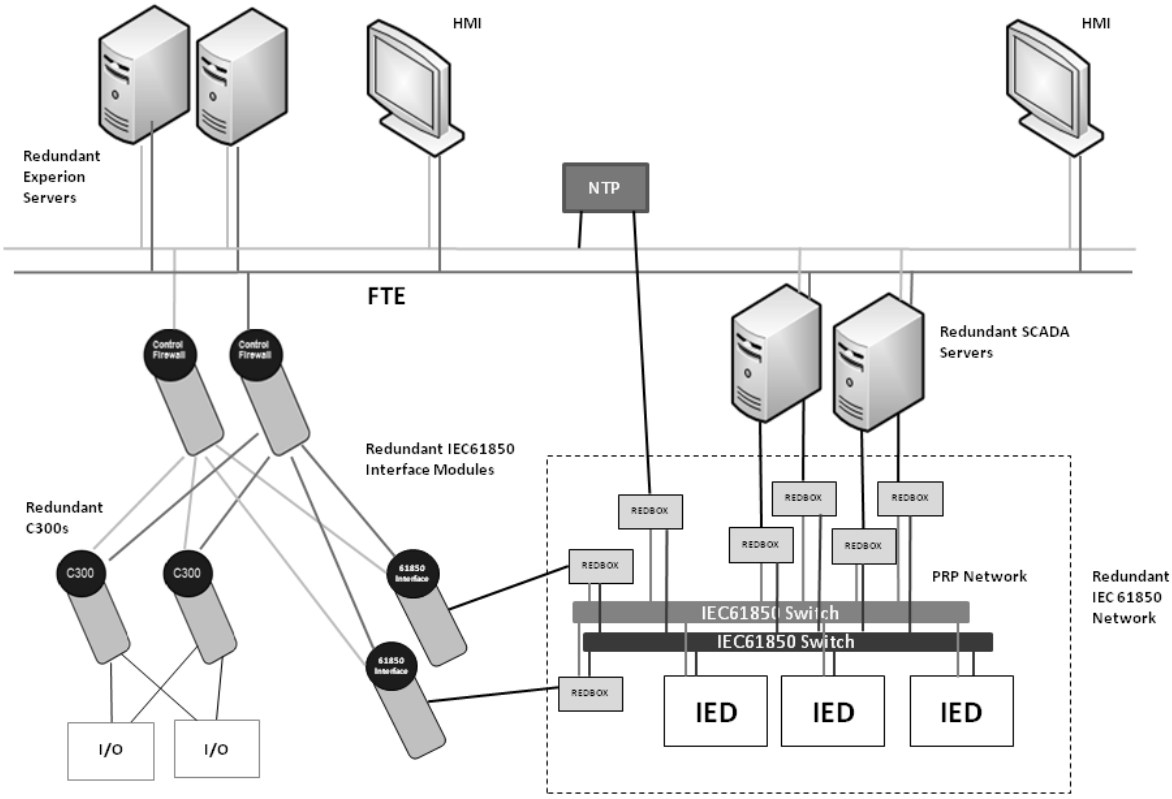


Figure 5: PRP topology model

3.4 IEC 61850 network device and IED support policy

850M supports IEC 61850 complaint switches and IEC 61850 edition 1 - compliant IEDs. It can connect to any IEC 61850 complaint switch using Redbox. Honeywell is not restricting users to IEDs or device types.

Following is a list of network switches and IED devices used by Honeywell for 850M integration and qualification, for your reference.

Device/switch model	Vendor	IEC 61850 edition	Communication ports
REU615-A (Voltage protection and Control)	ABB	1	Dual RJ45 ports for making HSR ring and single optic fibre port
RET615-D (Transformer protection and Control)	ABB	1	Single RJ45 port and connect through Redbox to be part of HSR ring or PRP network
REF620-A (feeder protection and Control)	ABB	1	Dual RJ45 ports for making HSR ring and single optic fibre port
REM615-A (Motor protection and Control)	ABB	1	Single RJ45 port and connect through Redbox to be part of HSR ring or PRP network
REF615A (feeder protection)	ABB	1	Single RJ45 port and connect through Redbox to be part of HSR ring or PRP network
RSP25	Hirschman	N/A	Redbox
PT-G503-PHR-PTP-HV	MOXA	N/A	Redbox
PT7528	MOXA	N/A	IEC 61850 compliant switch
PT7728	MOXA	N/A	IEC 61850 compliant switch
GE Multilin M60 – Motor Protection System	GE	N/A	IEC 61850 compliant switch
SEL 787 – Transformer Protection Relay	• Siemens Sepam Series • Schneider	N/A	IEC 61850 compliant switch

3.5 Reviewing 850M performance data

This section provides information on 850M performance-related data.

The following table lists some 850M performance related data.

Performance	Capacity
Number of 850Ms per cluster	64
Number of IEDs with which C300 Controller exchanges data	32
Number of C300 Controllers per 850M	5
Number of 850Ms per C300 Controller	3
Number of IEDs resident on an IEC 61850 network	Unlimited
Number of connected IEDs per 850M	32
Number of Function Blocks per 850M **Attention** The number on logical devices and logical nodes is a function of the number of Function Blocks representing logical devices and logical nodes that can be loaded (based on memory consumption).	850
850M Communications memory size	28 MBytes
850M Function Block memory size	16 MBytes

Tip

For information on IEC 61850 SCADA system interface performance data, refer to the *IEC 61850 SCADA Configuration Guide*.

4 Series C 850M installation and upgrades

This section includes the tasks associated with installing and upgrading 850M hardware and software components.

Related topics

“Installation considerations” on page 28
“Installing 850M” on page 29
“Upgrading 850M firmware” on page 30

4.1 Installation considerations

Attention

This equipment must be installed in accordance with the requirements of the National Electrical Code (NEC), ANSI/NFPA 70, or the Canadian Electrical Code (CEC), C22.1. It is intended to be mounted within an enclosure or suitable environment acceptable to the local authority having jurisdiction, as defined in the NEC, or authorized person as defined in the CEC.

Electrostatic discharge can damage integrated circuits or semiconductors if you touch connector pins or tracks on a printed wiring board. Follow these guidelines when you handle any electronic component:

- Touch a grounded object to discharge static potential,
- Wear an approved wrist-strap grounding device,
- Do not touch the wire connector or connector pins,
- Do not touch circuit components inside a component,
- If available, use a static safe workstation,
- When not in use, keep the component in its static shield box or bag.

WARNING

Unless the location is known to be non-hazardous, do not perform the following when the component is powered.

- Connect or disconnect cables
- Install or remove fuses, terminal blocks, and so on

Considerations

- However, ensure that the 850M and it's associated C300 Controllers should be physically secured in locked cabinets.
- While installing the SCADA server dual home, ensure that you connect the FTE network to the lower MAC address NIC card, and IEC 61850 network can be connected to the other available NIC cards.

4.2 Installing 850M

Attention

Though the IOTA used for IEC 61850 is same as the C300 Controller in terms of physical layout, the labeling is different for the model number and communications ports. see section “Identifying 850M components” on page 19, for information on labelling and model numbers.

To install 850M

Installing the 850M hardware is same as the C300 Controller hardware. Refer to the *C300 Controller User's Guide* installation.

Ensure you perform the “Dual home configurations for SCADA server” on page 34 after installation.

4.3 Upgrading 850M firmware

The Series C Firmware Load Tool (CTools) utility is used to upgrade firmware in Series C hardware components.

Refer to *Upgrading Firmware in Series C Components* section in the *Control Hardware and I/O Module Firmware Upgrade Guide* for details about using CTools to upgrade firmware in Series C components.

5 Configuration

Related topics

“Experion System configuration” on page 32
“SCADA configuration” on page 33
“Dual home configurations for SCADA server” on page 34

5.1 Experion System configuration

Refer to the *Server and Client Configuration Guide* for information on configuring the Experion server.

5.2 SCADA configuration

Refer to the *IEC 61850 SCADA Configuration Guide* for information on configuring the Experion SCADA server.

Attention

SCADA server in DUAL home network cannot be configured as NTP time source for IEC 61850 network. It is recommended to use direct NTP source as defined in section “Time management in IEC 61850” on page 108.

5.3 Dual home configurations for SCADA server

- Ensure that the lower MAC address is selected for FTE network installation. As the Dell servers like Dell 320 have four built-in NIC interfaces, ensure to use the first two NICs for FTE connection and other two NICs for IEC 61850 network connections. If you have installed additional dual NICs on two NIC built-in type server, ensure that lower MAC address NIC is selected for FTE. With this setup, Experion installation automatically selects the lower MAC interfaces (first two interface of built-in NICs) for FTE and system management and also sets proper binding order that FTEMUX is on top .
- Disable the IP routing between the FTE interfaces and the IEC 61850 interfaces.
- Disable Microsoft Windows Client and File Sharing for the IEC 61850 ports on the SCADA server.
- Change the TCP/IPv4 interface metric on both the IEC 61850 interfaces to 5 and 10, and disable netBIOS on both IEC 61850 interfaces.
- Do not include a gateway address on either IEC 61850 interface with an assumption that gateway address is already defined on the FTEMUX.

To verify IP routing is disabled

1 Choose **Start > All Programs > Honeywell Experion PKS > Server > Diagnostic Tools > Experion Command Prompt**.
The **Experion Command Prompt** window appears.

2 Type `ipconfig /all` and press ENTER.
The IP configuration details are listed.

3 In the **Windows IP Configuartion** section, ensure that the value of **IP Routing Enabled** is set as **No**.

To disable Microsoft Windows Client and File Sharing for the IEC 61850 ports on the SCADA server

1 Choose **Start > Control Panel**.
The **Control Panel** window is displayed.

2 Perform one of the following depending upon your operating system.

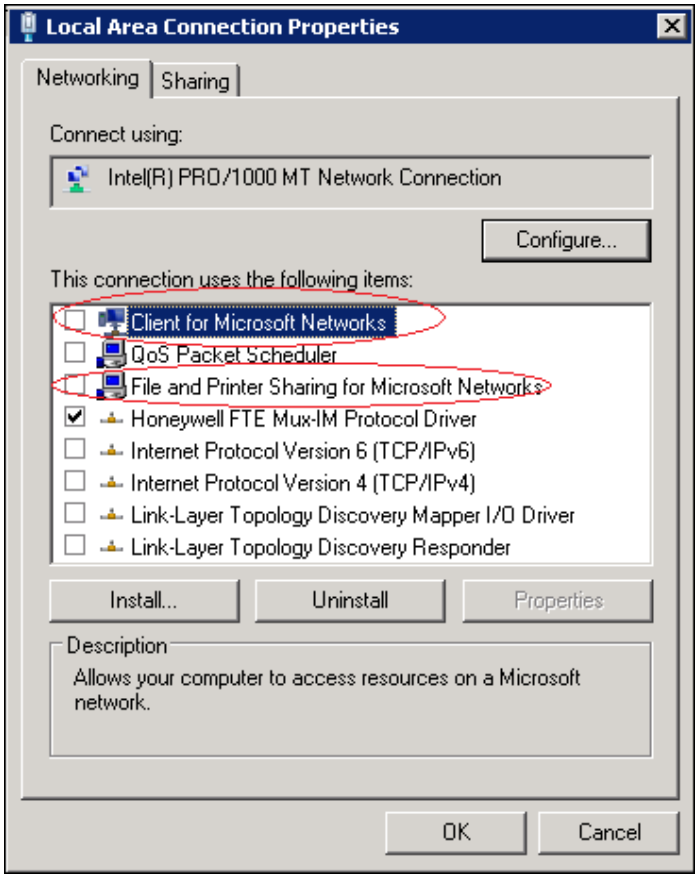
Option	Description
Windows 7	Click **Network and Internet > Network and sharing Center > Change Adapter Settings**.
Windows Server 2008	Click **Network and sharing Center > Manage Network Connections**.

The **Network Connections** window is displayed.

3 Right-click the network connections and choose **Properties**.
The **User Account Control** dialog box is displayed.

4 Click **Continue**.

5 In the **Networking** tab, disable the following options.
- Client for Microsoft Networks
- File and printer sharing for Microsoft Networks



6 Click **OK**.

To change the TCP/IPv4 interface metric and disable netBIOS

1 Choose **Start > Computer**.

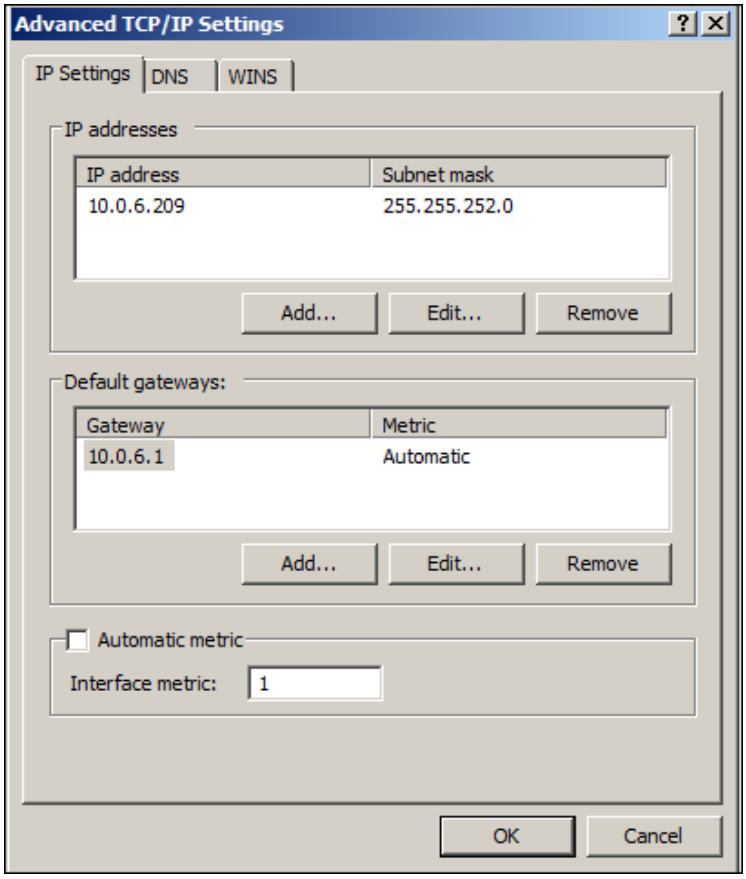
2 Right-click **Network** and choose **Properties**.

3 Right-click on the **DHEB Network connection** and choose **Properties**.

4 Select **Internet Protocol (TCP/IP)** and choose **Properties**.

5 Click the **Advanced** button on the **Internet Protocol (TCP/IP) Properties** window.

6 In the **Interface Metric** box, specify **5** for one IEC 61850 interface.



7 Click the **WINS** tab.

8 Click **Disable NetBIOS over TCP/IP** and then click **OK**.

9 Click **OK** on the **Internet Protocol (TCP/IP) Properties** dialog box.

10 Click **OK** on the **DHEB Network Properties** dialog box.

11 Repeat the above steps to change the **TCP/IPv4 interface metric** on the other IEC 61850 interface to **10**.

6 Series C 850M Configuration

This section includes the tasks associated with configuring IEC61850M.

Refer to the *Control Building User's Guide* for basic functionality details about calling up, navigating and interacting with the application. Also, note that menus, selections, tree views, and configuration forms may vary depending upon the licensed options installed on your system.

Related topics

"Configure IEC 61850 network" on page 38

This section includes information and tasks associated with creating and configuring IEC61850M, IEC61850LINK, IED, logical devices and logical nodes used in control strategies created in Control Builder.

"Configure control strategies" on page 60

This section describes tasks to create a control strategy to control IED parameters through a C300 Controller.

"Converting non-redundant 850M to redundant 850M" on page 65

This section includes information and tasks associated with converting a non-redundant 850M to a redundant 850M.

"Converting redundant 850M to non-redundant 850M" on page 67

This section includes information and tasks associated with converting a redundant 850M to a non-redundant 850M.

6.1 Configure IEC 61850 network

This section includes information and tasks associated with creating and configuring IEC61850M, IEC61850LINK, IED, logical devices and logical nodes used in control strategies created in Control Builder.

Related topics

“Creating an 850M” on page 38
“Configuring IEC61850LINK” on page 40
“Creating templates for logical devices and logical nodes” on page 41
“Creating and configuring an IED” on page 49
“Editing IED block parameters” on page 52
“Adding or associating logical devices to an IED” on page 54
“Assigning logical devices” on page 57
“To instantiate logical nodes associated with a logical device” on page 57
“Checking IED configuration” on page 58

6.1.1 Creating an 850M

This section includes tasks to create an instance of 850M (IEC61850M) block and add it to the Project tree.

Considerations

- You cannot add an IEC61850M block to the Project without configuring the applicable IP addresses for the FTE network and NTP servers.
- The 850M uses a consecutive odd/even pair of IP addresses on the IEC 61850 network. The 850M uses fixed IP addresses on the IEC 61850 network such that the lower (odd) IP Address is used on the 850M with the lower (odd) device index and the higher (even) IP address is used on the 850M with the higher (even) device index.
- You can only view IEC61850M blocks in **Project** set for the **Assignment** view. The **Assignment** view shows the relationship among all blocks while the **Containment** view only shows templates that contain other templates or Control Modules (CM), Sequential Control Modules (SCM), and basic blocks. To toggle the view, right-click in an open area of the tree window and choose **Assignment View** or **Containment View** from the list, as applicable.
- You can configure an IEC61850M block in the Control Builder Project without installing the hardware. However, it is recommended that the FTE communications drivers and hardware for the system be installed, configured and running. You must specify the IEC61850M's IP address and device index number on its configuration form. The IEC61850M represents a hardware module and the block configuration specifies the communication path to the hardware, similar to other Series C controllers.
- Each IEC61850M block is automatically assigned a unique default tag name when it is created. If your system includes multiple IEC61850Ms, you can adopt a more structured syntax for naming them.
- The IEC61850M includes a temperature sensor that monitors its ambient temperature. If the module's ambient temperature exceeds the configured *Temperature High Alarm* value, it triggers an alarm. The module's temperature sensing function automatically compensates for wild swings in the ambient to minimize alarms.
- Considerations for **Tag Name**
  - Must not exceed 16 characters
  - Must contain at least one letter (A-Z)
  - Must not contain an embedded space or leading space
- Considerations for **Item Name**
  - Must not exceed 40 characters

  - Must contain at least one letter (A-Z)
  - Must be unique among children of the same containment parent in the Enterprise Model Builder hierarchy
  - Must conform to the standard convention for names within the system
- You can disable the alarm for the battery function.
- The subnet mask must consist of all 1's followed by all 0's, with at least two 0's in the lower bits. Ensure that you perform the following steps if you enter invalid subnet mask address.
  1. Delete the 850M platform function blocks from the Monitor tree.
  2. Edit the primary platform function block on the Project tree.
  3. Change the IEC 61850 mask to a valid mask (for example, 255.255.255.0).
  4. Reload the primary and secondary platform function blocks.

Prerequisites

- You have started Configuration Studio and launched the Control Builder application.
- You have logged on with sufficient privileges to create control strategies using Control Builder.
- You have configured the applicable IP addresses when you set up your FTE network.
- The 850M network should be different from FTE subnet.

To create an IEC61850M instance

1 On the **File** menu, click **New > Interface Modules > IEC61850M-IEC61850 Interface Module**.
The parameter configuration form for the IEC61850M instance is displayed.

2 In the **Tag Name** text box, enter the preferred block tag name or accept the default value.

3 In the **Item Name** text box, enter the name of the item this object is associated to the Enterprise Model Builder hierarchy.

4 Click the **Continue** button to the right of **Associated Asset** text box to call up the Point Selection dialog. Select an asset from those configured in the Enterprise Model Database to set the Scope of Responsibility (SOR) for the device/IEC 61850 point.

5 Click the **Device Index** text box and enter the device index number set on the IEC61850M's IOTA/C300 IOTA.

> **Attention**
> Ensure to set the device index to an odd number.

6 Configure the **IEC 61850 Network IP Address** with the IP address of the device in the IEC 61850 network.

7 Click **Alarming Enabled** to enable the alarming option for the block.

8 Click **Disable Battery Alarm and Soft Fail** to disable battery-related soft failures and events.

9 Click the **Temperature High Alarm (deg. C)** text box, and enter the preferred threshold at which an alarm is generated for IEC61850M hardware temperature, or accept the default setting of 80 deg. C.

10 Click the **CPU Free Low Alarm Limit (%)** text box, and enter the required threshold at which an alarm is generated for IEC61850M CPU availability, or accept the default value of 20 percent.

11 If IEC61850M is a part of the redundant pair, select the **Module is redundant** check box.
For redundant IEC61850M, the **Secondary Tag Name** is a combination of configured *Tag Name* and *SEC* suffix.

12 Refer to the *Control Building User's Guide* and/or the online help to complete configuration data on the **Server History, Server Display, Control Confirmation**, and **Identification** tabs. The **Statistics** and **Version** tabs only contain read-only parameters. Refer to the “Viewing 850M operation status in Control Builder” on page 114 for information on **Statistics** and **Redundancy** tabs.

13 When you complete entering configuration data, click **OK** to close the configuration form and then add icon for non-redundant or redundant IEC61850M to the **Project** tree.

14 If you have redundant IEC61850M configuration, perform the following steps.

a Right-click the secondary IEC61850M icon, and choose **Module Properties** from the list.
The **Parameters configuration** form is displayed.

b Configure as required and click **OK** to close the form.
The IEC61850M block instance is created and displayed under the Root node in the **Project** tree.

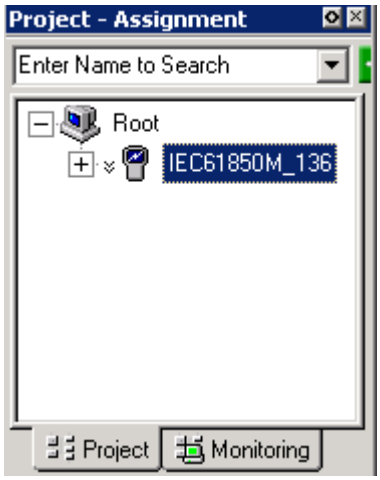


Figure 6: Instance of IEC61850M block under Root node in Project tree

On expanding the IEC61850M instance, the IEC61850LINK block is displayed. The IEC61850LINK instance is created together with the IEC61850M instance.

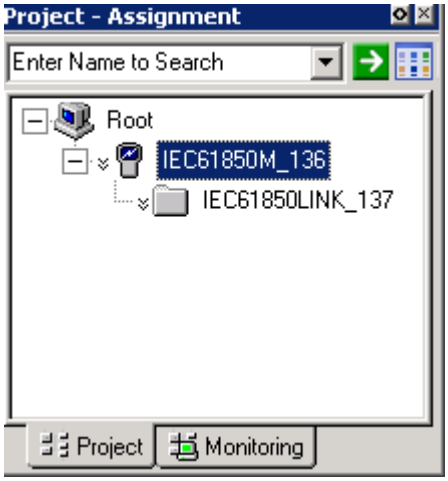


Figure 7: Instance of IEC61850LINK in Project tree

6.1.2 Configuring IEC61850LINK

This section includes tasks to configure IEC61850LINK values.

Considerations

- Ensure to click the + sign in front of the IEC61850M icon to open its directory tree and represent the IEC61850LINK icons. With the Hierarchal Building license option, you must have the **Assignment View** active to view IEC61850M and IEC61850LINK blocks.
- In a redundant IEC61850M, the IEC61850LINK blocks are shown with the primary IEC61850M block only.

- Considerations for **Tag Name**
  - Must not exceed 16 characters
  - Must contain at least one letter (A-Z)
  - Must not contain an embedded space or leading space
- Considerations for **Item Name**
  - Must not exceed 40 characters
  - Must contain at least one letter (A-Z)

Prerequisites

You have added an IEC61850M block to the Project tree.(“Creating an 850M” on page 38)

To configure IEC61850LINK values

1. Right-click the IEC61850LINK icon and choose **Module Properties** from the list.
   The **IEC61850LINK Block Parameters** form is displayed, with the **Tag Name** text box highlighted.
2. In the **Tag Name** text box, enter the preferred block tag name or accept the default value.
3. In the **Item Name** text box, enter the name of the item this object is associated to in the Enterprise Model Builder hierarchy.
4. In the **Description** text box, and enter the preferred description. The description appears in the detail displays and group displays associated with this block.
5. Refer to the *Control Building User's Guide* and/or the online help to complete configuration data on the **Server History, Server Display, Control Confirmation, and Identification** tabs. Refer to the “Viewing 850M operation status in Control Builder” on page 114 for information on **Statistics** and **Memory** tabs.
6. After entering the configuration data, click **OK** to close the **IEC61850LINK Block Parameters** form.

6.1.3 Creating templates for logical devices and logical nodes

This section describes tasks to create templates for logical devices and logical nodes using ICD/CID files. This section also describes tasks to recreate missing logical device(s) templates. You can recreate missing logical device(s) templates by selecting the missing logical device(s) from the ICD/CID file in the **IEC 61850 IED Device Description Import** dialog box and importing it back to the Control Builder.

Considerations for creating templates

- Ensure that an approved antivirus application is installed on the node used to import ICD/CID files.
- The ICD/CID file must be stored in the following directory location.
  - Default path: `C:\ProgramData\Third Party Files\SCL files\`
  - Custom installation path: `<UserSelectedDirectory>\Third Party Files\SCL files\`
- You need not perform this task if a block for the given device type already exists in the Control Builder Library database.
- It is recommended to use the ICD files for template creation. If you use ICD/CID file, you have ensure to use appropriate device to import the template. Otherwise, the template is not created.
- Considerations for the **Manufacturer** field.
  - **Manufacturer** name is used for creating Library name in Control Builder. Hence, it is a mandatory field.
  - Maximum number of characters allowed is 40, which is the maximum number of characters allowed for Library name in Control Builder.
  - According to Control Builder tag naming criteria, the following characters are not allowed for **Manufacturer** field.

    `~!@#$%^&*+-=(){}[]|\\:;'<>,.?/ \"\t

- Considerations for the **Type** field.
  - Default value of Template Prefix is the value in the **Type** column.
  - You can also configure the **Template Prefix** if required.
  - The **Type** field is used for generating logical device template name. Hence, it is a mandatory field.
  - The logical device template name displayed in the library tree is formed as **<Template Prefix> <InstName attribute of LDevice>** is a numeric value starting from 1. For example, the device type is IED670 and the logical device instance name is EF4_1, then the logical device template name is formed as IED670_1_EF4_1.
  - Maximum number of characters allowed for vendor template in Control Builder is 16. Hence, to accommodate the above naming schema, maximum number of characters allowed for device type is 6.
  - According to the Control Builder tag naming criteria, following characters are not allowed for **Device Type** field.

    `~!@#$%^&*+-=(){}[]|\\:;'<>,.?/ \"\t

Prerequisites

You must have the ICD/CID file for the IED device from vendor's IED configuration tool.

To create a template

1 You can open the **IEC 61850 IED Device Description Import** dialog box in one of the following ways.

Option	Description
IEC 61850 IED Device Description Import icon	In the Control Builder, click on the **IEC 61850 IED Device Description Import** icon.
From the File menu	On the **File** menu, click **New > Type > IEC 61850 Device**.

The **IEC 61850 IED Device Description Import** dialog box appears.

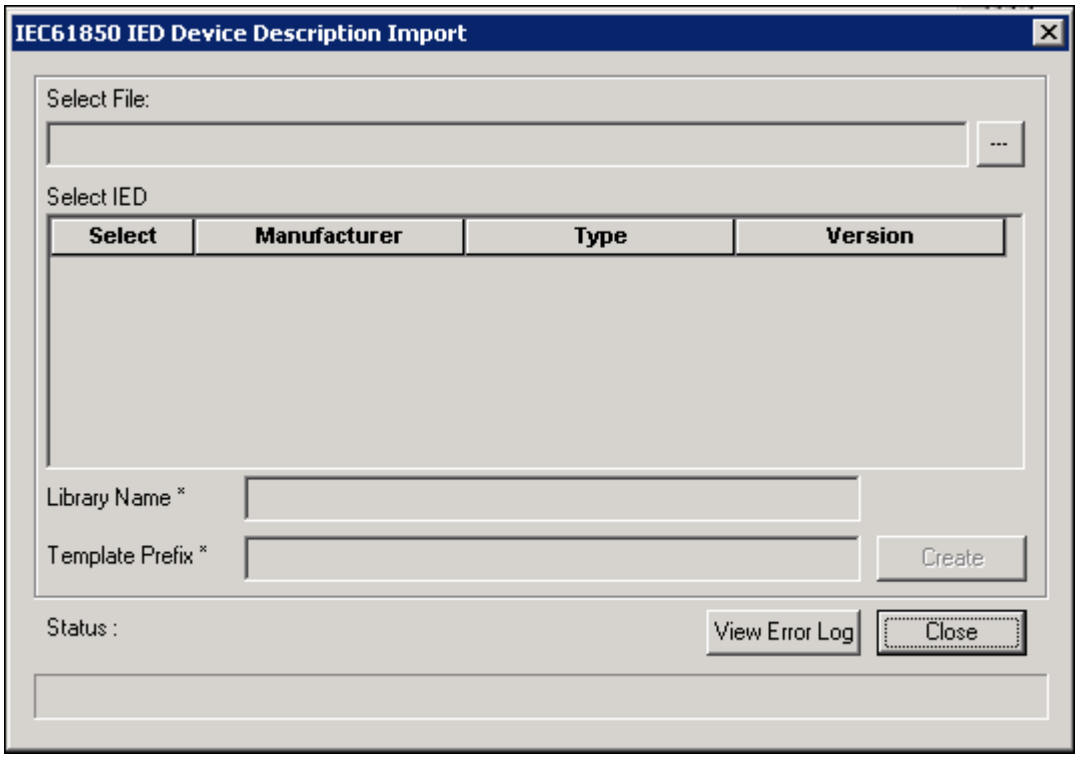


Figure 8: IEC 61850 Device Type dialog box

2 Click ... to browse for the applicable ICD/CID file, and navigate to the location of the required file.

Attention

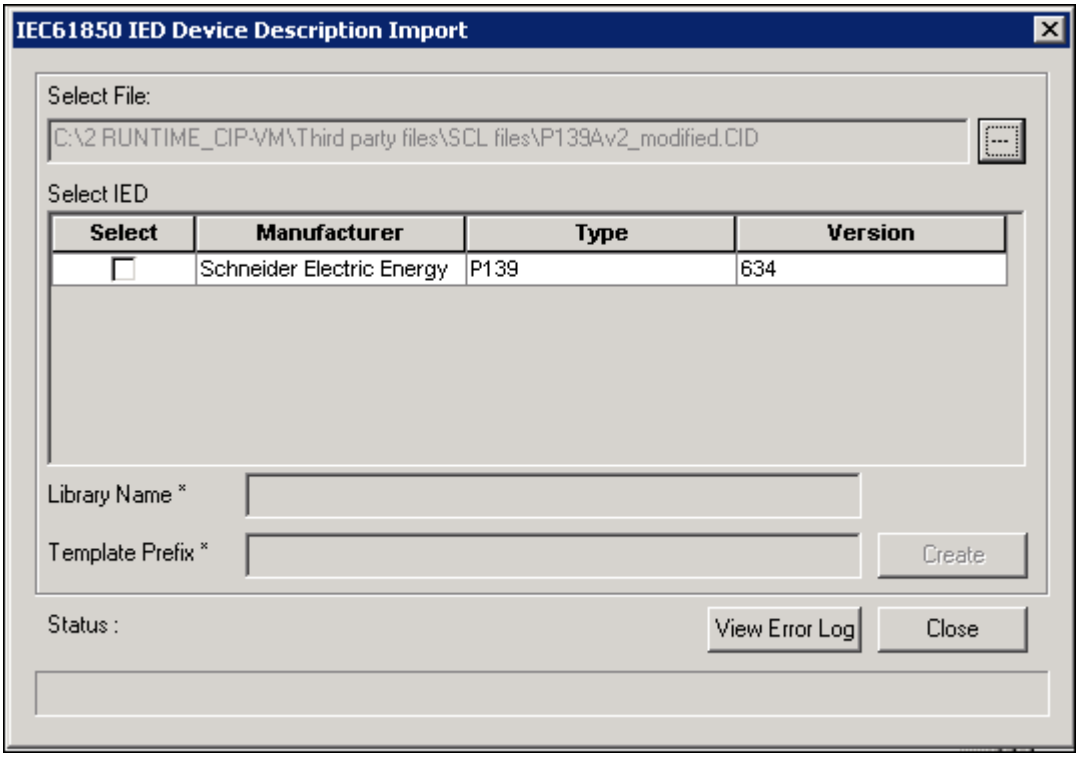
These files are saved in the following location. Ensure that this folder or sub-folder is NOT excluded from virus scanning.

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *%User Selected Path%\Third party files\SCL files*

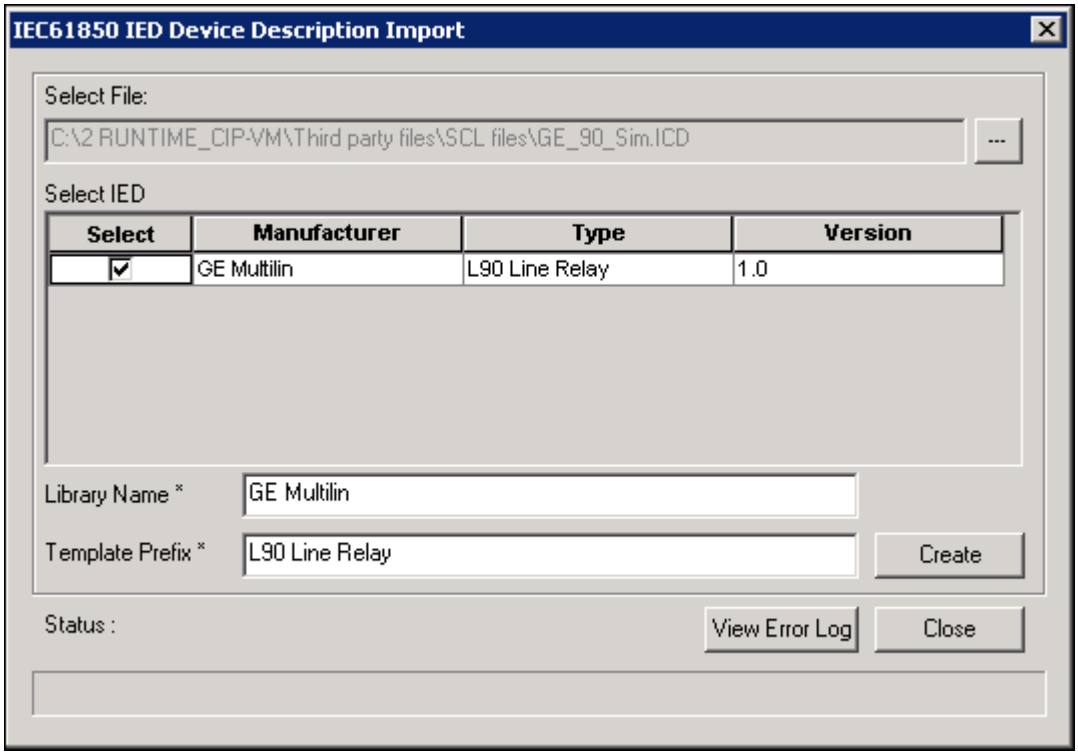
Examples of the directory path:

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *C:\2 RUNTIME_CIP-VM\Third party files\SCL files*

After the ICD/CID file is selected, the details of the manufacturer and the device type are displayed in the **Device Information** section.



3 Select the ICD/CID files you want to import.
The **Library Name** and **Template Prefix** fields display the information from the ICD/CID files.



4 Click **Create**.

The creation of logical device templates of an IED in the Control Builder library begins. The progress bar displays the current status of logical device template creation. The **Status** field displays one of the following status during template creation.

Status	Description
In Progress	Logical device template creation is in progress
Saving changes	Logical device templates are getting saved in ERDB
Completed	Logical device template created successfully
Failed	Logical device template creation failed
Cancelled	Logical device template creation is cancelled by the user

5 After completion, the **Status** field in the progress bar displays the status as **Completed**.

6 Click **Close**.

In the **Library** tree, a new device block type is created and the ICD/CID files with logical devices and logical nodes are listed. The logical nodes associated with the logical devices are listed under their respective logical device template.

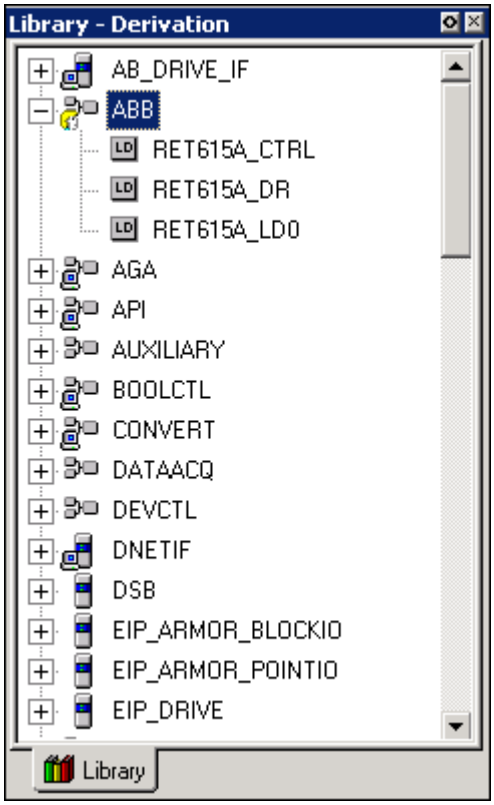


Figure 9: Logical devices and logical nodes in Library tree

The **File** menu is also updated with the menu options to instantiate the newly created templates for the logical devices. All the IEC 61850 logical devices are listed in the **File >New >IEC 61850 Devices** menu.

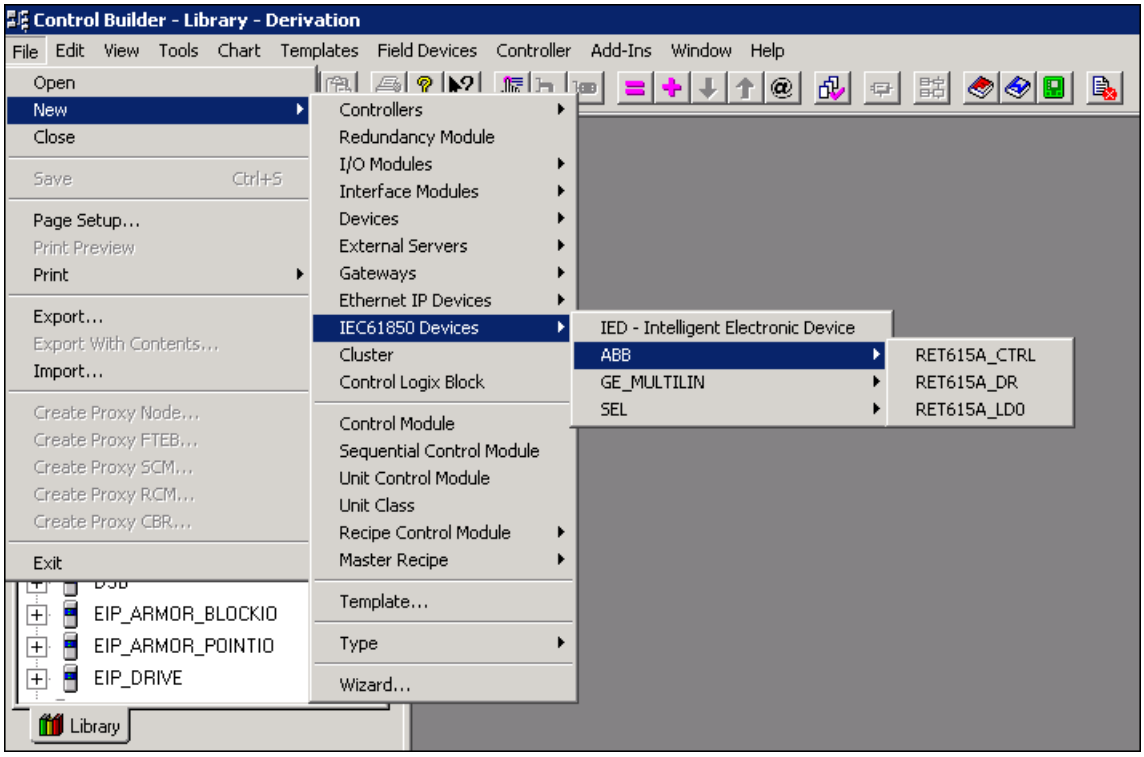


Figure 10: Logical devices and logical nodes in File menu

To recreate a missing logical device template

1 On the **File** menu, click **New > Type > IEC 61850 Device**.
The **IEC 61850 IED Device Description Import** dialog box appears.

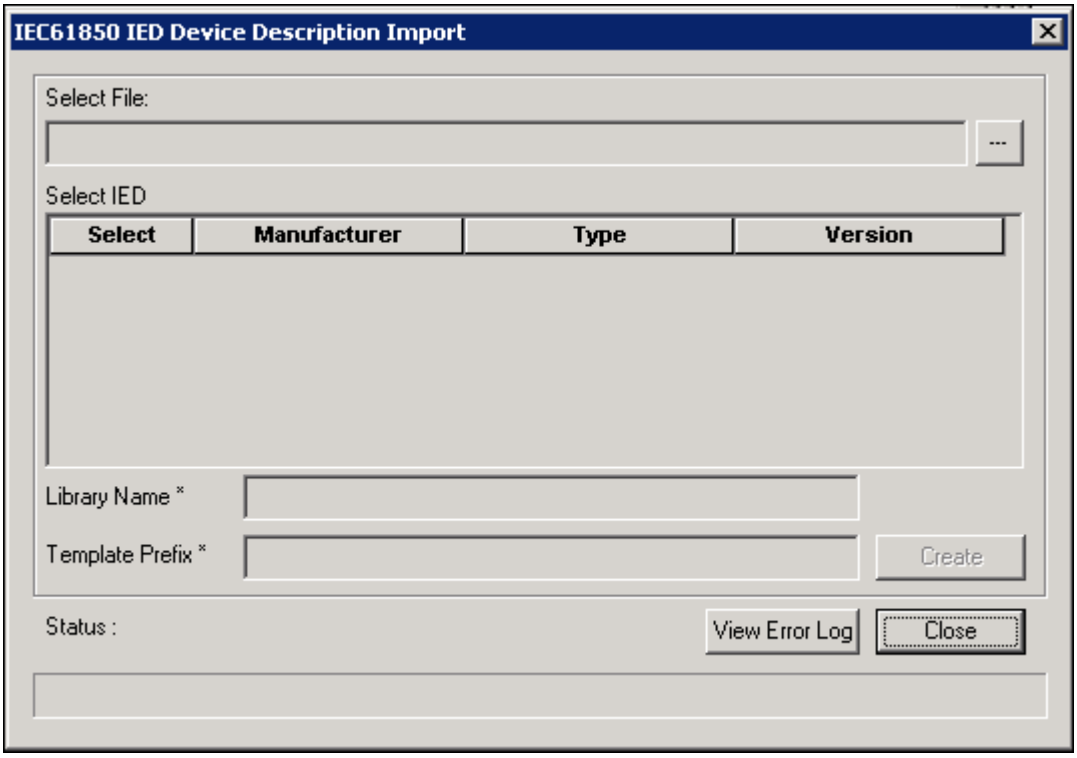


Figure 11: IEC 61850 Device Type dialog box

2 Click ... to browse for the ICD/CID file, and navigate to the location of the file which contains the definition of the missing logical device(s).

Attention

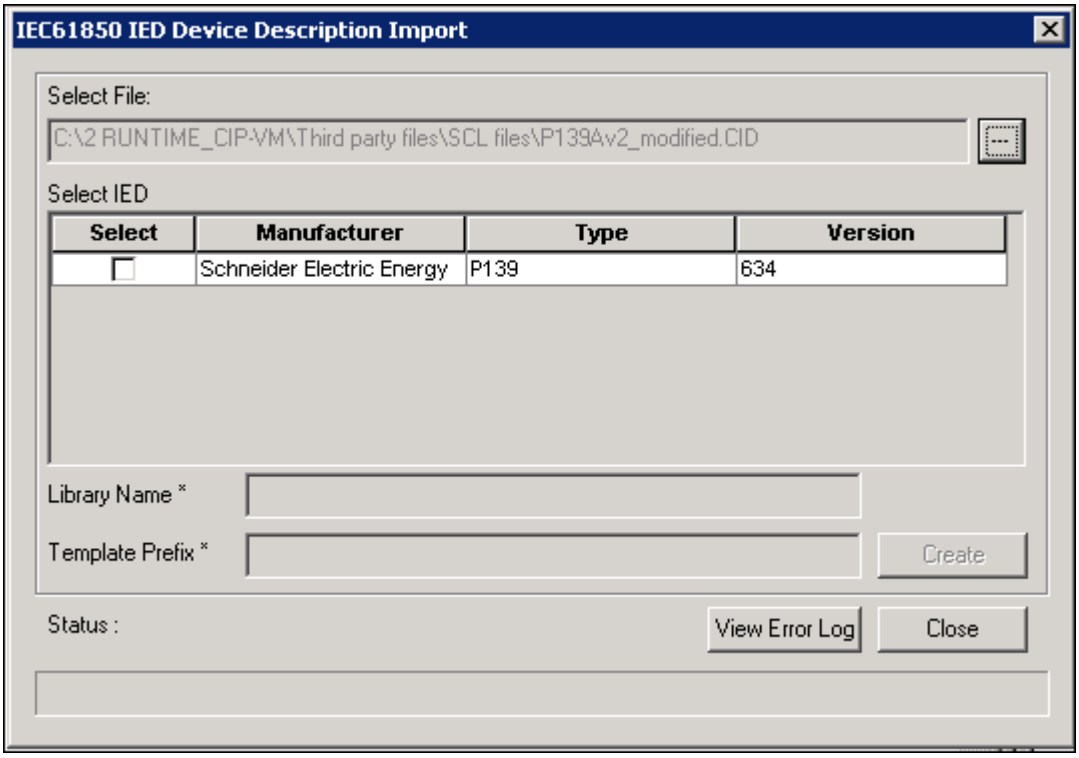
These files are saved in the following location. Ensure that this folder or sub-folder is NOT excluded from virus scanning.

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *%User Selected Path%\Third party files\SCL files*

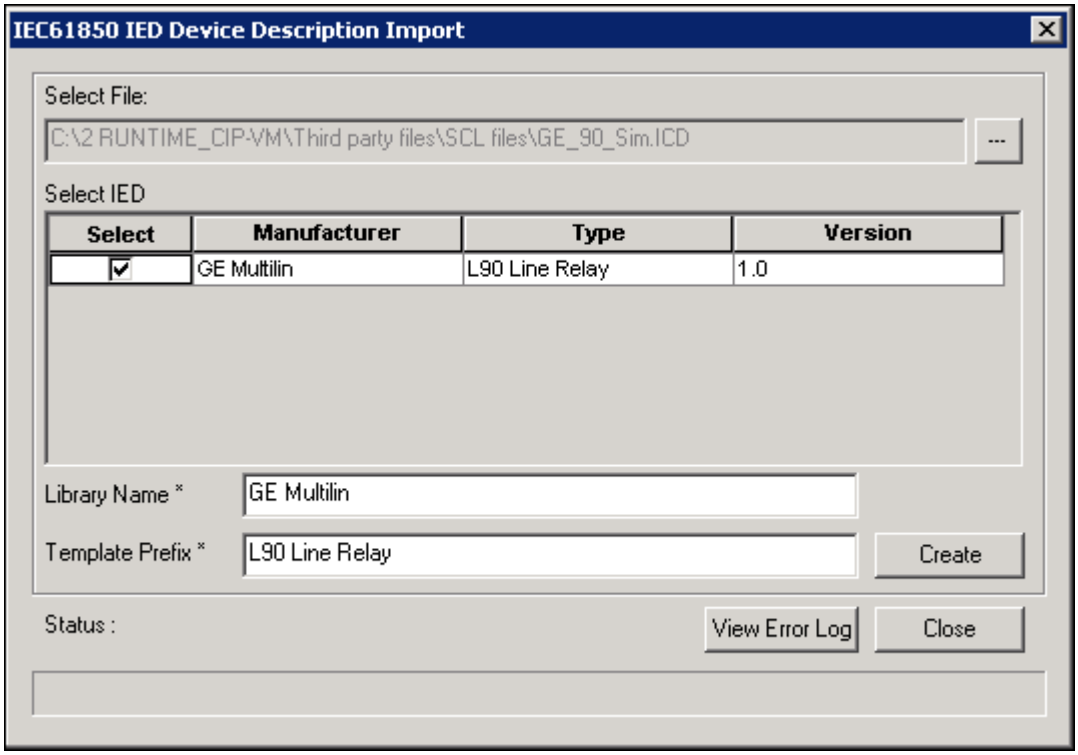
Examples of the directory path:

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *C:\2 RUNTIME_CIP-VM\Third party files\SCL files*

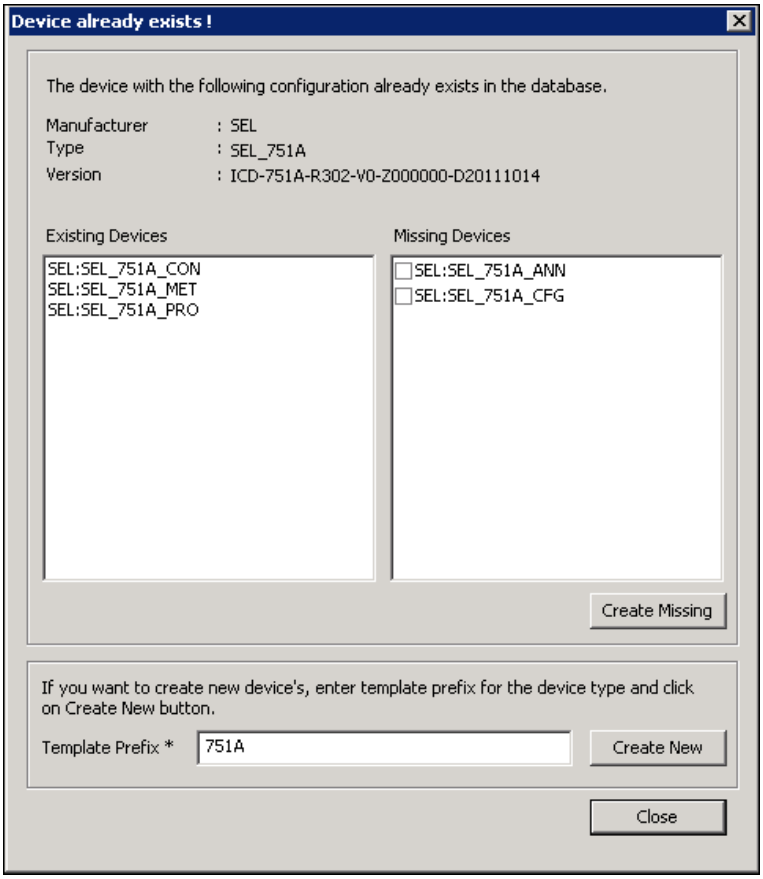
After the ICD/CID file is selected, the details of the manufacturer and the device type are displayed in the **Device Information** section.



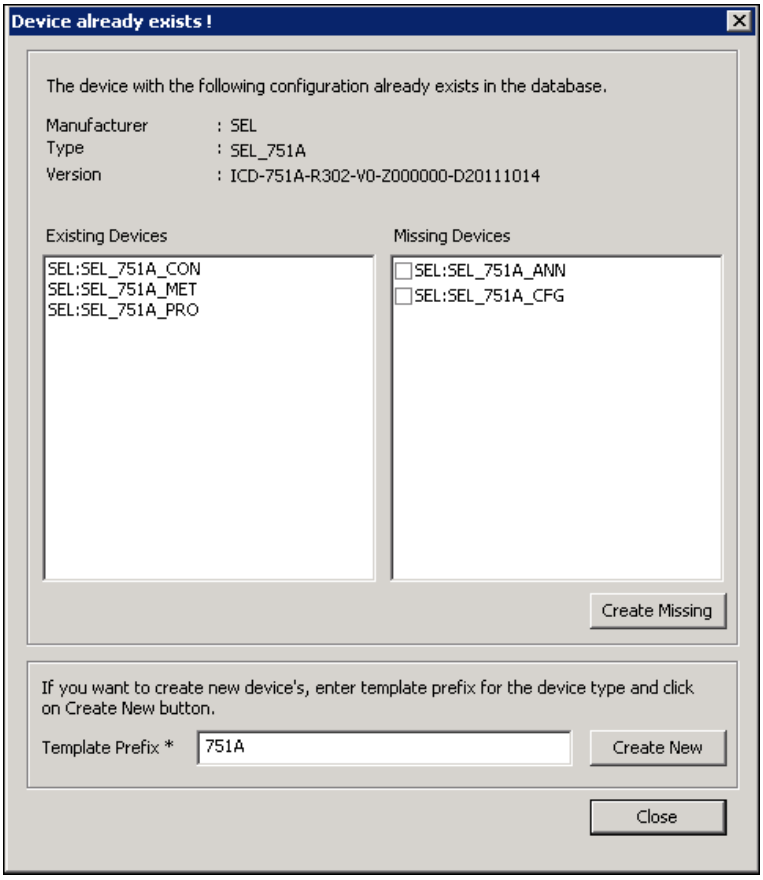
3 Select the ICD/CID files you want to import.
The **Library Name** and **Template Prefix** fields display the information from the ICD/CID files.



4 Click **Create**.
The **Device already exists** dialog box appears. The missing logical devices are listed in the **Missing Devices** column.



5 Select the required logical device(s), and click **Create Missing**.
The ICD/CID file is imported and the missing logical device is added in the Library tree.



6.1.4 Creating and configuring an IED

This section includes task to create an instance of Intelligent Electronic Device (IED) and add it to the Project tree.

An IED instance can also be created from the *Library* by dragging and dropping an IED instance to the Project tree.

Considerations

Ensure that an approved antivirus application is installed on the node used to import ICD/CID files.

To create an IED instance

1 On the File menu, click **New >IEC 61850 Devices > IED - Intelligent Electronic Device**.
The Parameter configuration form for the IED instance appears.

2 In the **Tag Name** text box, enter the preferred block tag name or accept the default value.

3 In the **Item Name** text box, enter the name of the item this object is associated to in the Enterprise Model Builder hierarchy.

4 In the **Keyword Description** text box, enter the preferred description. The description appears in the detail displays and group displays associated with this block.

5 Refer to the *Control Building User's Guide* and/or the online help to complete configuration data on the **Server History**, **Server Display**, **QVCS** and **Identification** tabs Refer to the “Viewing 850M operation status in Control Builder” on page 114 for information on **Statistics** tab.

6 When you complete entering configuration data, click **OK** to close the configuration form.
A new instance of the IED is created in the **Project** tree under the **Unassigned** category.

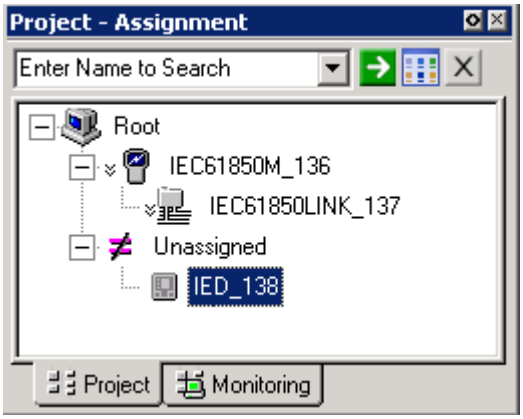


Figure 12: IED instance in Project tree

7 Drag and drop the IED instance under the **Unassigned** tree to the IEC61850LINK instance in the Project tree.

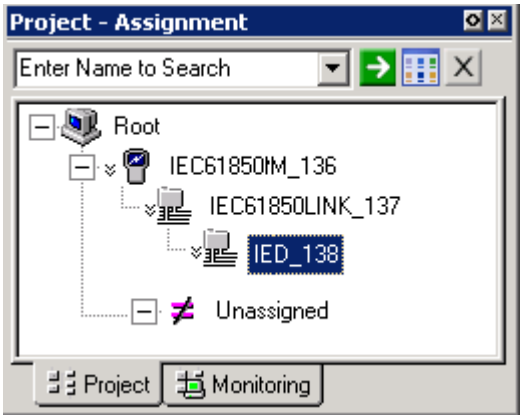


Figure 13: IED instance assigned to IEC61850LINK

Tip
You can also assign an IED instance to an IEC61850LINK using the "To instantiate logical nodes associated with a logical device" on page 57.

8 Associate an ICD/CID file to the IED instance.

a Right-click an IED instance (assigned to an IEC61850LINK), and choose **Associate ICD/CID**.
The **Associate ICD/CID-*<IED name>*** dialog box appears.

b In the **Select New Association** section, click ... to browse for the applicable ICD/CID file, and navigate to the location of the required file.

Attention
These files are saved in the following location. Ensure that this folder or sub-folder is NOT excluded from virus scanning.

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *%User Selected Path%\Third party files\SCL files*

Examples of the directory path:

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *C:\2 RUNTIME_CIP-VM\Third party files\SCL files*

c Select the required file and click **Open**.
The list of available ICD/CIDs are listed in the **Available IEDs** section.

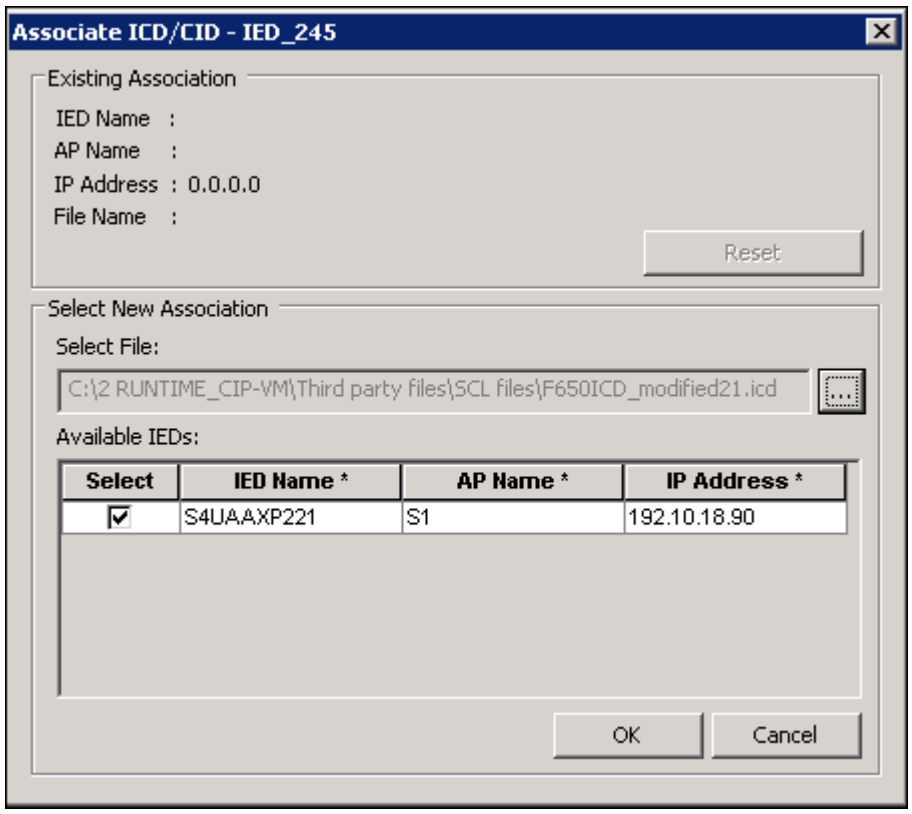


Figure 14: List of available IEDs in an ICD/CID file

d Select the IED you want to associate to this IED instance by clicking the check box in the **Select** column, and click **OK**.

- The Select Configuration form associated ICD/CID file is configured on IED instance. All related parameters are updated on the IED instance.
- The following message appears after all the IEDs are successfully imported.

Figure 15: Message displayed after successful import

9 Open the parameter configuration form for the IED instance, and select the **Main** tab.

- The **Device Configuration**, **Device Information**, **CID information**, **IED Information**, and **Logical Device Information** sections display the information of associated ICD/CID file, as shown in the figure.
- The **Assigned Instances** column in the **Logical Device Information** section displays the assigned logical device to that IED.

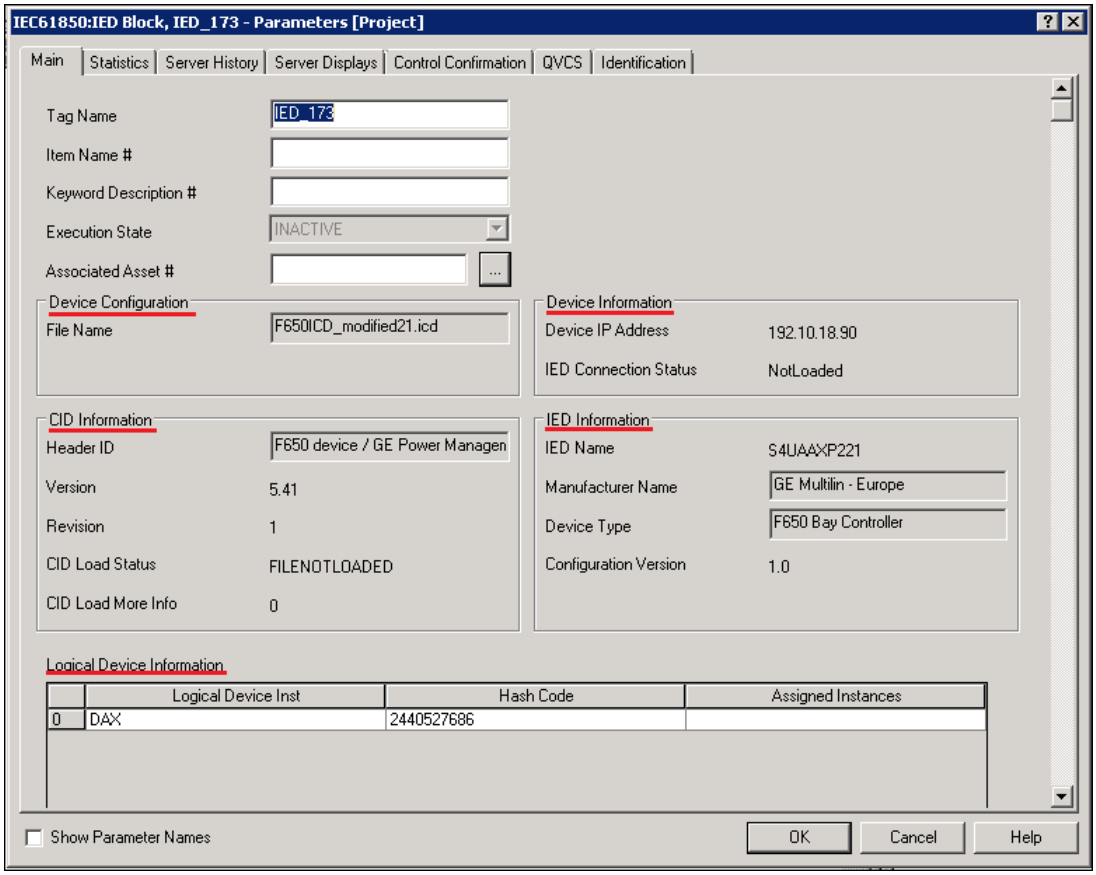


Figure 16: ICD/CID file association details in the Main tab

6.1.5 Editing IED block parameters

This section describes tasks to edit IED block parameters to an IED instance.

You can either reconfigure IED block parameters or associate new set of IED block parameters to an IED instance.

Considerations

- You cannot reconfigure IED with a ICD/CID file of different IED name or IP address or IED type if the IED has a logical device associated to it.
- You cannot reconfigure IED with ICD/CID file with different IED name or IP address or IED type if the IED is loaded.
- If you have the modified version of an ICD/CID file which is compatible with an IED instance, you can associate the new ICD/CID file.
- Ensure that an approved antivirus application is installed on the node used to import ICD/CID files.

Prerequisites

You must have templates of the logical devices and logical nodes for IED block available in the Library tree. (“Creating templates for logical devices and logical nodes” on page 41)

To edit IED block parameters

1 Right-click the IED instance (assigned to an IEC61850LINK), and choose **Associate ICD/CID**.
The **Associate ICD/CID-<*IED name*>** dialog box appears.

2 You can edit the IED block parameters using one of the following methods.

Option	Description
Associate a new ICD/CID file	Go To Step "3" on page 53 **Attention** When you associate a new ICD/CID file, the existing IED block parameters are replaced with the new IED block parameters.
Reconfigure IED block parameters	1. Click the **Reset** button. The following message appears after all the IEDs are successfully removed.  **Figure 17: Message displayed after successful reset** 2. Associate a new ICD/CID file. Go To Step "3" on page 53

3 In the **Select New Association** section, click to browse for the applicable ICD/CID file, and navigate to the location of the required file.

Attention

These files are saved in the following location. Ensure that this folder or sub-folder is NOT excluded from virus scanning.

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *%User Selected Path%\Third party files\SCL files*

Examples of the directory path:

- Default path: *C:\ProgramData\Third party files\SCL files*
- Custom installation path: *C:\2 RUNTIME_CIP-VM\Third party files\SCL files*

4 Select the required file and click **Open**.
The list of available IEDs are listed in the **Available IEDs** section.

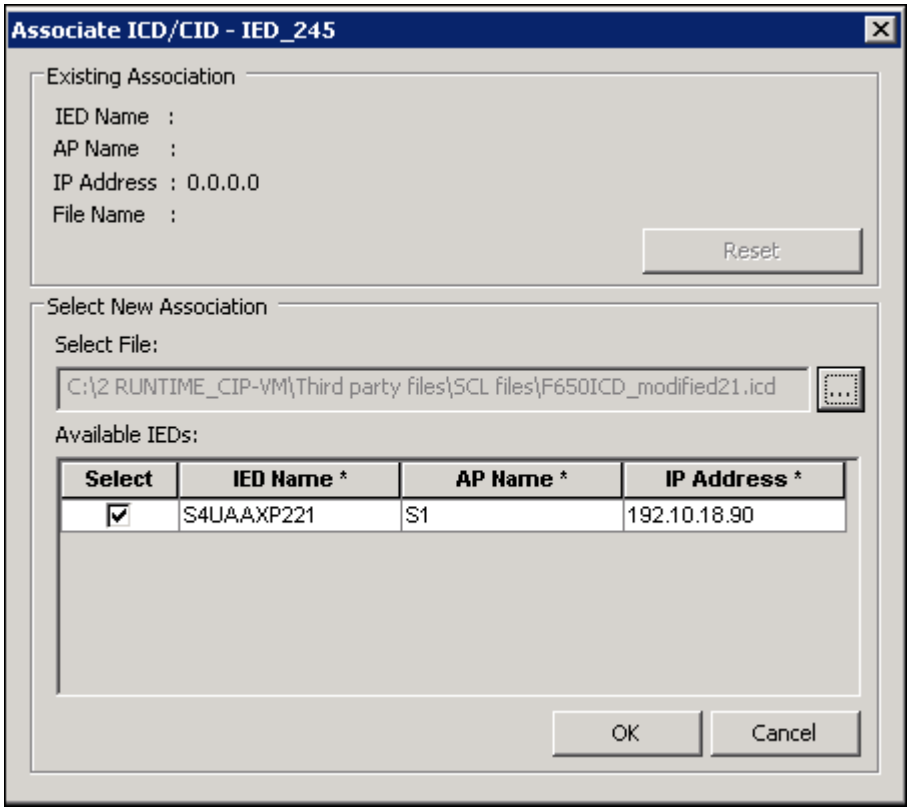


Figure 18: List of available IEDs in an ICD/CID file

5 Select the IEDs you want to associate to this IED instance by clicking on the check box in the **Select** column, and click **OK**.

- The Control Builder library begins importing the ICD/CID file .
- The following message appears after all the IEDs are successfully imported.

Figure 19: Message displayed after successful import

6.1.6 Adding or associating logical devices to an IED

This section includes tasks to add or associate a logical devices to an IED.

Considerations

- Use drag and drop or menu selections method to assign a logical device to an IED in the **Project** tree.
- It is recommended to check the block configuration parameters after the device is assigned to IED.

Prerequisites

- You must have templates of the logical devices and logical nodes for IED block available in the **Library** tree. (“Creating templates for logical devices and logical nodes” on page 41)
- You must have PHD configured with appropriate CID files to add a logical device to IED device from **Project** tree.

To use drag and drop method to add/associate logical devices to an IED

1 In the **Library** tree directory, click + sign in front of the required IED type to show stored device block types.

2 Drag the IED icon to an open area in the **Project** tree. (Note that cursor appears with + sign, when positioned in a valid location).

The **Name New Function Block(s)** dialog box is displayed.

3 In the **Destination** text box, enter the IED name or accept the default IED name.

4 Click **Finish**.

The device instance with given name is created in Project tree under the **Unassigned** category.

5 Drag and drop the logical device instance on to the IED device instance in the Project tree.

To use the File menu method to add/associate logical devices to an IED

1 On the **File** menu, click **New > IEC 61850 Devices**. Select a logical device associated to an IED.

The **Parameters configuration form** for the selected logical device appears with the **Text Name** text box highlighted.

2 In the **Tag Name** text box, enter the required name of the device or accept the default name.

3 In the **Item Name** text box and enter the name of the entity that this object is associated with in the Enterprise Model Builder hierarchy.

4 In the **Description** text box and enter the required description for the device.

5 Refer to the *Control Building User's Guide* and/or the online help to complete configuration data on the **Server History, Server Display, QVCS, Control Confirmation and Identification** tabs.

6 When you complete entering configuration data, click **OK** to close the configuration form.

The device instance with the given name is created in the Project tree under the **Unassigned** category. The logical nodes associated with the logical device are created and assigned under the logical device.

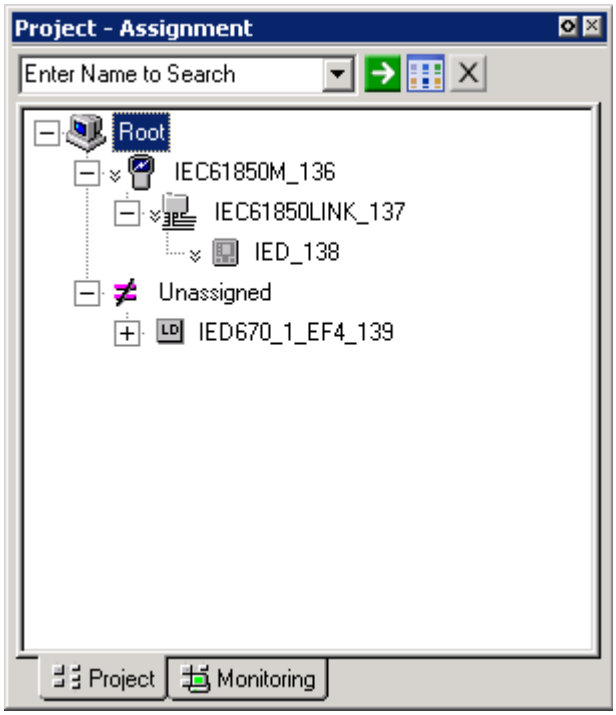


Figure 20: Logical device instance in Project tree.

7 Drag and drop the logical device instance into the Project tree.

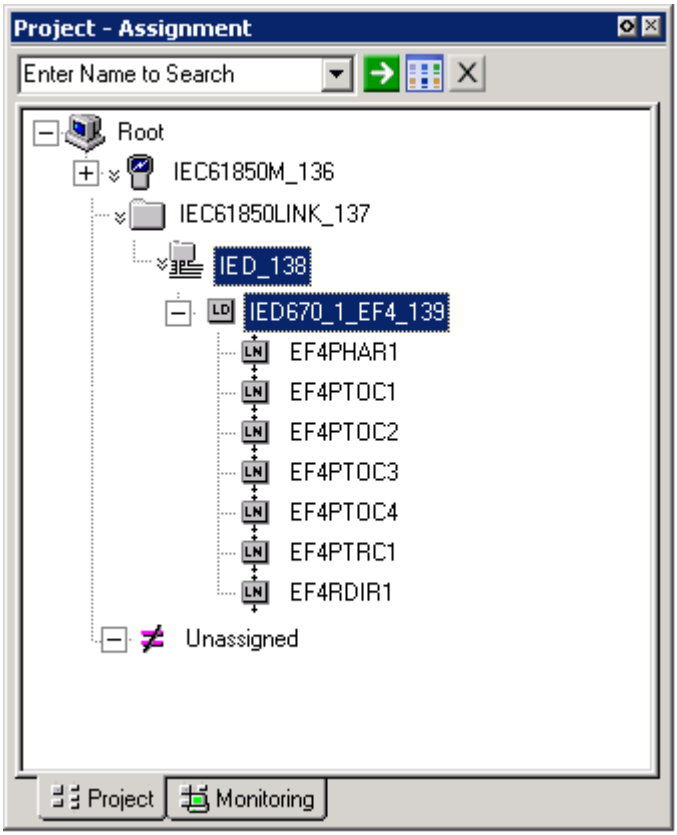


Figure 21: Logical device instance in the Project tree

Tip
Logical devices can also be assigned using “Assigning logical devices” on page 57.

6.1.7 Assigning logical devices

This section describes tasks to assign logical devices to an IED instance.

Considerations

- If duplicate address error message appears, refer to section “Checking IED configuration” on page 58 for details on changing the device's network node address. The device addresses can be set to the default value of 20.
- Number of logical devices and logical nodes per 850M is 850 approxmiately.

Attention
The number of logical devices that are loaded and logical nodes that are assigned will consume memory and reach the 850M limit. If IEDs have large logical node definitions, we may attain the limit much before the maximum limit number.

Prerequisites

An IEC61850M block is created in the **Project** tree, and has an IED instance associated to it.

To assign logical devices to an IED instance

1. Click **Edit > Execution Environment Assignment** or click the  in the tool bar.
   The **Execution Environment Assignments** dialog box appears.
2. Click the **Devices** tab.
   The IEDs in the **Project** tree are listed.
3. Select the logical device you want to associate to an IED.
4. Verify that the required IED is selected in the **Assign To** list box.
5. Click **Assign→** to assign the selected logical device to the selected IED.
6. Ensure that the logical device is added to the **Assigned Modules** list box with the assign state icon  .
7. Drag and drop the logical device instance on to the IED device instance in the Project tree.
8. Repeat the above steps to assign other logical devices.
9. Click **Close** after assigning the required devices.

6.1.8 To instantiate logical nodes associated with a logical device

Considerations

- Number of logical devices and logical nodes per 850M is 850 approximately.

Attention
The number of logical devices that are loaded and logical nodes that are assigned will consume memory and reach the 850M limit. If IEDs have large logical node definitions, we may attain the limit much before the maximum limit number

- Logical nodes cannot be removed from the associated logical devices if they are loaded.

1. In the **Project** tree, double-click a logical device instance.
   The **Parameters Configuration** form appears.
2. In the **Logical Nodes** tab, select or remove the logical node you want to associate/dissociate with this logical device instance, by clicking on the check box in the **Create** column.

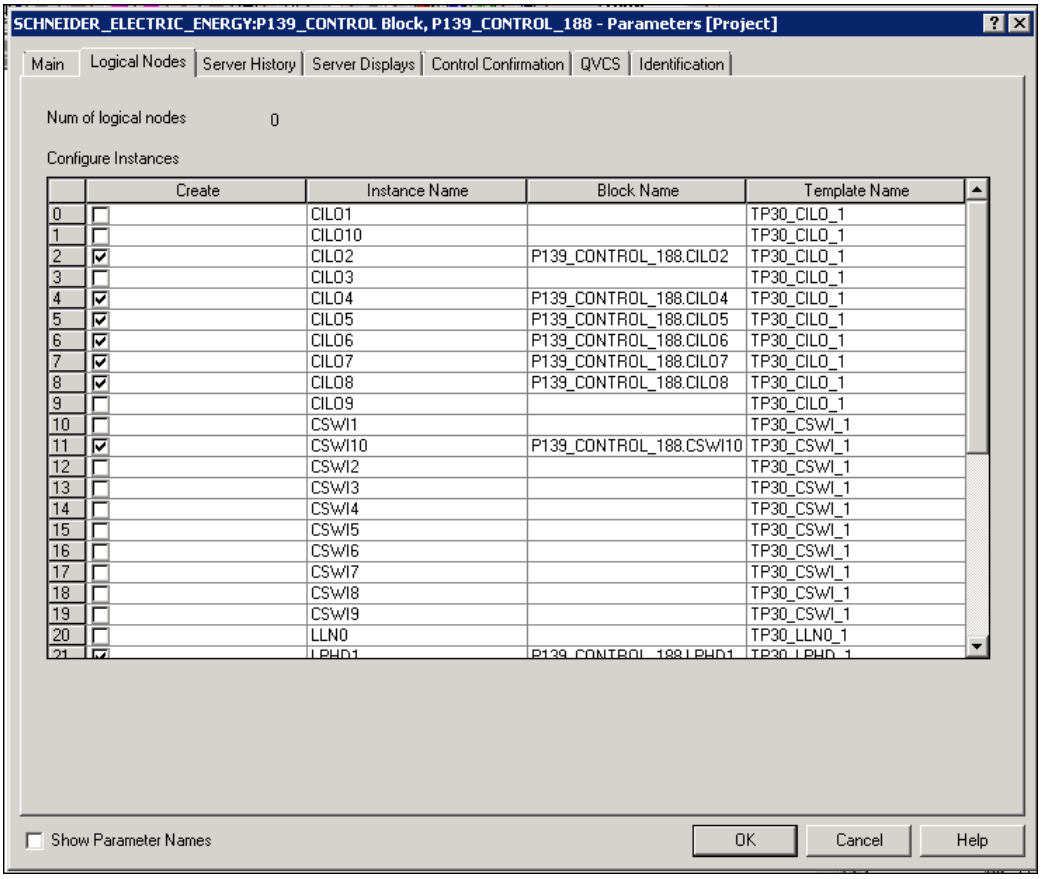


Figure 22: List of logical nodes in the Logical Nodes tab

3 Click **OK**.
The selected logical node instances are listed under the logical device instance in the **Project** tree.

6.1.9 Checking IED configuration

Considerations

- While the IED is assigned to an IEC61850LINK, it is the offline configuration of a matching physical device that must be connected to this IEC61850LINK.
- Each device on the link must have a unique physical device tag (PD_TAG) that the IEC 61850 system relates to a node address. The physical device tag, node address, and the manufacturer device identifier (DEV_ID) are used to match a configured device to a physical device.
- In the Experion system, each independent component in the control strategy must have a unique tag name (NAME). This is automatically enforced through the Control Builder application. The unique name that was assigned to the device when it was created in **Project** is also assigned as the device's physical device tag. This is done to assure that the names are unique within the system. This means a change in NAME results in an automatic change in PD_TAG to keep them the same. However, a change in PD_TAG does not result in an automatic change in the assigned NAME.
- While checking the IED configuration, you can only edit the **Tag Name**, **Item Name** and **Key Description** fields.

Prerequisites

You have assigned the IED to an IEC61850LINK in the **Project** tree.

To check IED configuration

1. Double-click the IED icon in the **Project** tree.
   The **Parameter Configuration** form appears with **Tag Name** highlighted.
2. Accept the assigned name or enter new name, which is unique within the system.
3. In the **Item Name** text box and enter the name of the entity that this object is associated with in the Enterprise Model Builder hierarchy.
4. In the **Key Description** text box and enter the required description for the device.
5. Refer to the *Control Building User's Guide* and/or the online help to complete configuration data on the **Server History, Server Display, Control Confirmation and Identification** tabs. Refer to the “Viewing 850M operation status in Control Builder” on page 114 for information on **Statistics** and **Memory** tabs.
6. When you complete entering configuration data, click **OK** to close the **Parameter Configuration** dialog box.

6.2 Configure control strategies

This section describes tasks to create a control strategy to control IED parameters through a C300 Controller.

The Project Engineer builds a library of the IED blocks in Control Builder. The Project Engineer then creates control strategies that use the instances of the IED blocks. The control strategies and the IED are used to control the IED after they are loaded to the C300 Controller and IEC61850M.

You can also configure parameters using the Series C Universal I/O module. For information about configuring strategies using the Series C Universal I/O module, refer to the *Control Building User's Guide*.

Considerations

- The navigation from the hyperlinked parameter is available to a parameter connector, which is for an Input/ Output parameter of a block.
- You can navigate to a parameter in other charts that belong to a different controller. Therefore, this navigation improvement can be used to traverse between peer-to-peer connections across controllers.
- In the Project mode, double-click on the parameter to edit the parameter name in the parameter connector. An edit box appears which allows you to change the parameter name.
- If the parameter belongs to a tagged block or a function block within a tagged block that does not exist, you cannot navigate to the source parameter and hence the hyperlink for such parameters does not exist.
- You can write a parameter to an IED only through a PUSH block or SCM block.
- There are no function blocks that can be configured specifically for the IEC61850M. Use the **Param Connector** option to configure any IED device parameter.
- To configure Control Strategy which writes parameters to IED, refer to the *Control Building User's Guide*.

Prerequisites

- Control Builder is running and the tree windows are open.
- You have created and loaded a physical device on a C300 Controller. The physical device has associated logical devices and it's and logical nodes.
- You have created a Control Module to associate the physical device to. Refer to the *C300 Controller User's Guide* to create a Control Module.
- You have identified the data type of IED data attributes that you want to connect to a Experion block that support the data type.

To configure Control Strategy which reads parameters from IED using the parameter connector

1 Click the parameter connector  button.

The pointer turns into a cross-hair.

2 Click on the desired input block pin.

3 Double-click outside the block at the required parameter connector location.

The parameter connector appears.

Tip

Clicking in different places outside the block symbol results in the parameter connector being placed in different locations. Click once to establish a path to a desired location before double-clicking. Press the ESC key to cancel the operation and start over if required.

4 Use one of the following methods to specify the name of the block connection.

Option	Procedure
Option 1	Enter the full name of the desired block connection, including Control Module, Block Name (Tag), Parameter and then press the ENTER key.

Option	Procedure
Option 2	1. Click on the button with the dot leader icon (three dots) to access the Point Selection dialog. 2. Find the desired point name and parameter and then click on **Select** to insert the specified parameter into the parameter connection field. 3. Click **Close** on the top right-hand corner of the Point Selection dialog box to close the dialog and return to the control drawing.

After you create a parameter connector, the parameter appears as hyperlink. When you click on the hyperlinked parameter with the Control key pressed, the chart/configuration form appears for the tagged block

Attention

850M supports IEC 61850 edition 1 data types. You can read/write parameters from the Project to the IEC 61850 edition 1 data types only. Parameters that have enumeration value beyond 64 have negative values. Perform the following workaround while reading and writing such parameters.

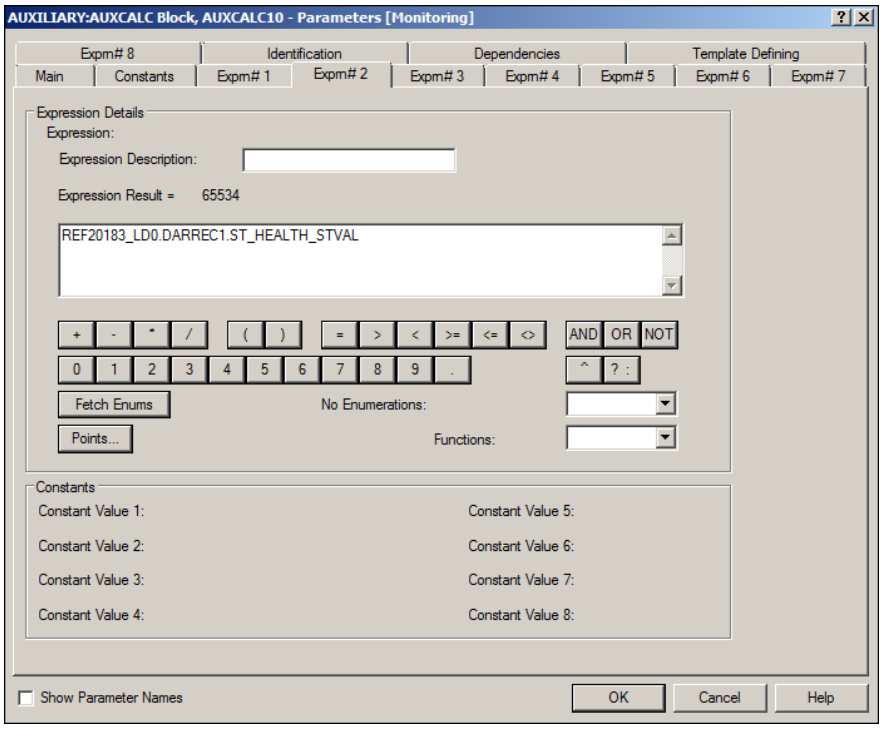
Reading negative enumerations

1. Read the value as a large positive value from ERDB.
2. Calculate the negative value.
3. Use the negative integer value in CM.

Example

- IED value = – 2
- Block in CM = AUXCALC block

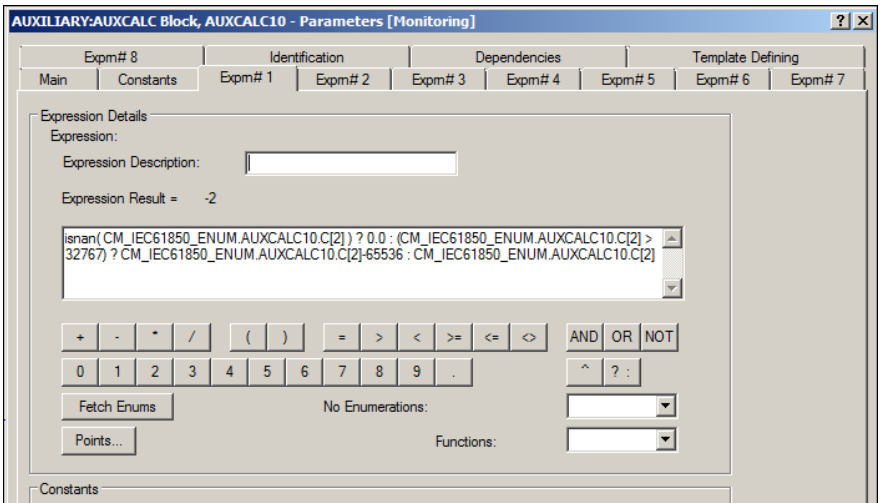
1. Read the IED value as a large positive: 65534 (65536-2)



2. Calculate the negative value using the AUXCALC block, as shown below.

```
isnan( CM_IEC61850_ENUM.AUXCALC10.C[2] )
        ? 0.0
            : (CM_IEC61850_ENUM.AUXCALC10.C[2] > 32767)
                ? CM_IEC61850_ENUM.AUXCALC10.C[2]-65536
                    : CM_IEC61850_ENUM.AUXCALC10.C[2]
```

The expression appears as follows, in the Control Builder



6.2.1 Control writes

850M supports the control model states defined in the *IEC 61850 Specification Part 7.2 (edition 1)* to operate on IED data with data attribute having the functional constraint FC. 850M supports direct control with normal security (direct-operate) control model. Control Builder supports configuration of control strategies in C300 Controller to write data to IED controllable status and analog data attributes of common data class specifications defined in the *IEC 61850 Specification Part 7.2 (edition 1)*.

You can write control data structures that send the control structure format and its data. Any logical node which contains data object with data attribute Oper requires a control write.

Considerations

- Experion currently supports direct control with normal security (direct-operate) control model only.
- When a control write is performed, the timestamp is stored/recorded.
- The sequence number increments and is reset/rolls over to 0 when the value crosses 255.
- It is recommended to specify the name of the 850M instance in the Modoper_origin_orident field.
- The Modoper_origin_orident is displayed as an ASCII value, but it is an *octet string* parameter type.

Prerequisites

- Control Builder is running and the tree windows are open.
- You have created and loaded an IED on an 850M. The IED has associated logical devices and it's and logical nodes.
- You have created a Control Module to associate the IED to. (Refer to the *C300 Controller User's Guide* to create a Control Module).
- Do not write the control value from the functional constraint FC tab of the logical node (associated with an IED). When IED control parameters are configured to write from control strategies, it might result in write failures. Special considerations are required to write to IED data attributes that has negative enumerations. Refer the negative enumeration workaround
- Configure IED with a control model from the supported control models and ctlModel. Use 3rd IED configuration or IED front panel display to set the control model.

To perform a control write

1. Project side configuration of logical node.
   a. Double-click the required logical node instance
      The Parameters form appears.
   b. Configure the mandatory data attributes of the classes having the functional constraint FC of the IED with a control model in Control Builder and load the IED to 850M.
      - Mod_oper_origin_orcat: accept the default value or change the value
      - Modoper_origin_orident: accept the default value or change the value
      - Mod_oper_test: applicable only test status to test the control model
      - Mod_oper_check: synchrocheck/ interlock-check-Applicable for DPC (double-point control) class only
   c. Click **OK**.
2. Writing a control value
   a. Configure control strategies in C300 Controller to write to IED controllable data attributes of the common data classes to PUSH blocks. for example, CtlVal).
   b. Configure control strategies in C300 Controller to write to IED controllable data attributes of the common data classes to SCM blocks.
      The Oper control parameter attributes of the logical device are updated.

Attention

The attributes that were set up while configuring the logical node in the Project side are not written to the IED until the CtlVal parameters are written.

3 This results in a change in the output status of an IED connected device, such as a relay or a switch.

Attention

If write is not successful due to invalid control model configuration for which IED reject the write, 850M report appropriate error message to C300 Controller. See trouble shooting section

6.3 Converting non-redundant 850M to redundant 850M

This section includes information and tasks associated with converting a non-redundant 850M to a redundant 850M.

Considerations

- The 850M redundant pair must have odd/odd+1 device index number combination, which means the primary or non-redundant 850M must have an odd address to support an odd+1 address for the secondary 850M. For example, if you set the Device Index to 15 for the primary 850M, the Device Index for the secondary 850M is 16.
- You can make the conversion to 850M redundancy while the process is online.
- The partner 850M to be added is at the same firmware revision level as the existing primary 850M.

Prerequisites

- The non-redundant 850M to be converted has an odd number device index.
- You have logged on with sufficient security level to make changes in a control strategy in Control Builder.

To convert to redundant 850M

1 In the **Project** tab, double-click a non-redundant IEC61850M icon.
The **IEC61850M Block Parameters** form appears.

2 Select the **Module is redundant** check box.
The **Secondary Tag Name** field shows the tag name of the redundant IEC61850M.

3 Click **OK**.
The IEC61850M icon is now redundant and the icon for the secondary IEC61850M appears in the Project tree.

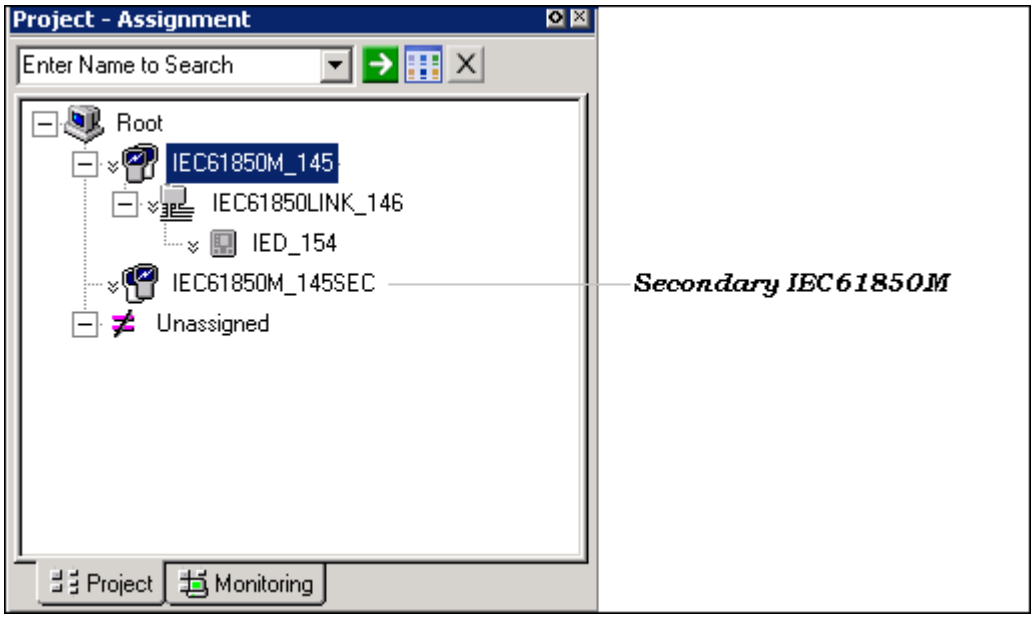


Figure 23: Secondary IEC61850M block under Root node

4 Load the primary IEC61850M block.

a Right-click the Primary IEC61850M icon and choose **Load** from the list.

b Click **Continue** to acknowledge the Warning prompt, if applicable.

c Confirm that only the IEC61850M block is selected for download.

d Click **OK** to load the block.

5 Right-click the Secondary IEC61850M icon and choose **Load** from the list. Click **Continue** to acknowledge the warning, if applicable; and click **OK** to load the block.

6 If both the IEC61850Ms are installed and auto synchronization is enabled, the modules synchronize when power is applied.

6.4 Converting redundant 850M to non-redundant 850M

This section includes information and tasks associated with converting a redundant 850M to a non-redundant 850M.

Considerations

- Only the 850M with odd+1 device index number, can be removed from the system.
- If you try to delete a secondary 850M from the **Monitoring** tab while the redundant 850M pair is synchronized, the command is rejected.
- If the secondary 850M is still installed when the primary/non-redundant 850M is loaded, an alarm signals the presence of a partner that is not configured.

Prerequisites

- The primary 850M has an odd number for its device index.
- The secondary 850M has an odd+1 number for its device index.
- You have logged on with sufficient security level to make changes in a control strategy in Control Builder.

To convert to non-redundant 850M

1. In the **Monitoring** tab, double-click the primary IEC61850M block icon.
   The **IEC61850M Block Parameters** form appears.
2. On the **Main** tab, confirm that block **Redundancy Role** is primary and **Device Index** is an odd number.
3. If the 850M with the odd device index number is not the primary, click the **Redundancy** tab and click **Initiate Switchover** to issue a switchover command.
4. On the **Redundancy** tab, click **Disable Synchronization** to disable auto synchronization. Click **Yes** to confirm the action.
5. Click **OK** to close the form.
6. Delete secondary from monitoring side for online conversion.
7. Loosen the three screws in the secondary 850M and remove it from the lower module slot on the redundant IOTA. Remove FTE cable connections, as applicable.
8. In the **Project** mode, clear the **Module is Redundant** check box.
   a. Right-click the primary/non-redundant IEC61850M icon and choose **Load** from the list.
   b. Click **Continue** to acknowledge the Warning prompt, if applicable.
   c. Confirm that only the 850M block is selected for download.
   d. Click **OK** to load the block.

7 Loading Series C 850M

Related topics

7.1 About load operations

The Experion system provides the ability to build control strategies offline, without being connected to the actual field components. The process of transferring the control strategy to the "live" working components in the field is called the load operation.

The load operation functionally copies configuration data from the control strategy that is stored in the Engineering Repository Database (ERDB) to the assigned field component in the system architecture. It indirectly assures that the planned system matches the actual one. The communication addresses and physical location assignments specified for components through Control Builder configuration must match the actual addresses and locations of components in the system.

7.1.1 Loaded versus project database versions

The master control strategy, stored in the Engineering Repository Database (ERDB), is configured and edited through the Project tab. Once the contents of the control strategy are loaded from Project to the applicable components, a loaded version of the Project or master database is created. The loaded version of the database can be viewed only through the Monitoring tab and supports only minimal editing of the control strategy configuration data.

The following commands are included in the Control Builder Controller menu to synchronize data in the loaded database with the data in the Project/master database.

- Update to Project (from Monitor)
- Update with Contents (to Project)

In addition, the *Upload* command allows you upload data for selected objects from the 850M to the Monitoring database. Thus, the monitoring database reflects the same data which is loaded in the 850M. For more information, see “Upload to the Monitoring database”.

7.1.2 Load initiation and load dialog box

You can initiate a load operation for selected components from either the Project tab or Monitoring tab using one of the following commands in the Control Builder.

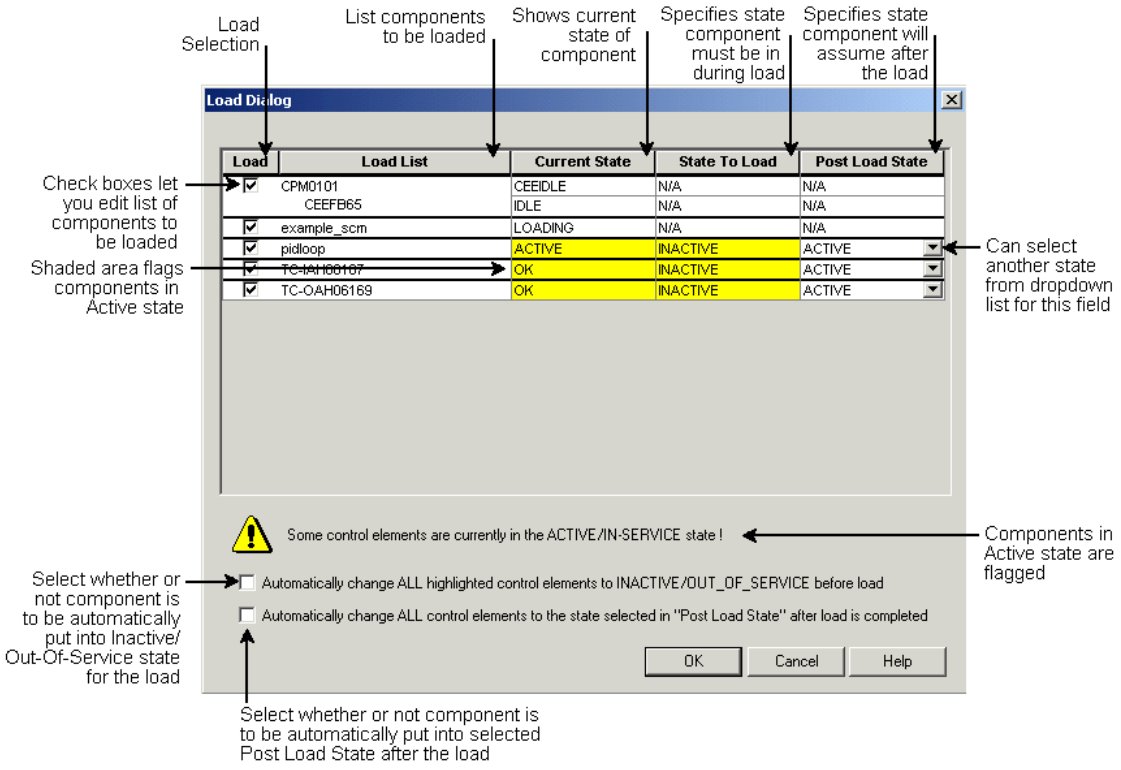
- Load
- Load with Contents

Either command invokes the **Load** dialog box. The following figure shows a sample The **Load** dialog box invoked for a load with contents operation for an 850M. It provides a brief description of the dialog box features for quick reference. The appearance of the dialog box varies depending on the current load circumstances such as whether this is an initial load or a re-load operation.

CAUTION

The load operation is inherently an offline function. The Load dialog box provides the ability to automatically inactivate a component during a load and then return the component to its active state. Do **not** use this automatic inactivate/activate function if your process cannot tolerate the load disruption and consequent delay in activation. In this case, you must manually toggle the component state through the Monitoring tab in Control Builder.

Table 1: Sample load dialog box



7.1.3 Load action with compare parameters function

The capability of the load action is expanded when the *Use Compare Parameters* function is enabled through the **System Preferences** dialog box. For more information, refer to the *Using Compare Parameters* section in the *Control Building User's Guide*.

7.1.4 Load options for server history and server displays configuration

You can enable or disable the loading of history, trend, or group configuration data for a block to Server through the **System Preferences** dialog box.

For more information, refer to the *Setting system preferences* section in the *Control Building User's Guide*.

7.2 Initial load order guidelines

Perform the initial load of control strategy components from the Project view in the following order to minimize possible load interaction generated error messages.

Table 2: Initial load order guidelines

Order	Component
1	IEC61850M
2	IEC61850LINK
3	IED
4	Logical device
5	Logical Node
5	CM or SCM*
* Refer to the *Control Building User's Guide* for information about loading these components.	

7.3 Loading 850M

Prerequisites

- Control Builder is running.
- 850M is installed and communicating with the Experion server.

To load an 850M instance

1 Right-click the required 850M and choose **Load**.
The **Load Operation** dialog box appears. The 850M and its link block are listed.

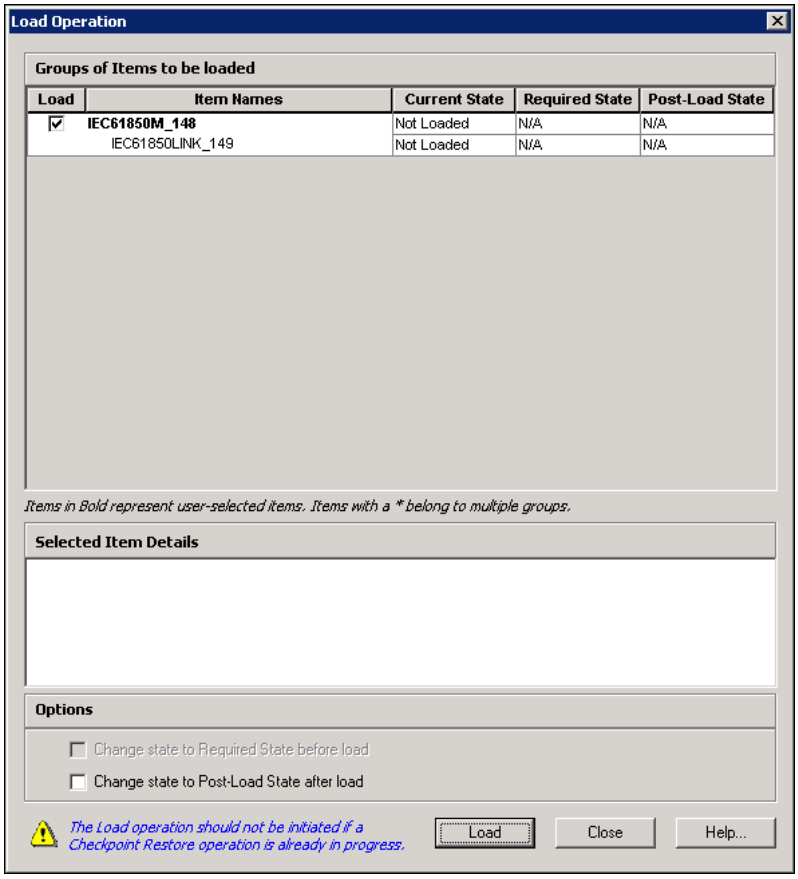


Figure 24: Load dialog box for 850M

2 Click **OK**.
The 850M loading to the monitoring side begins.

3 After successful load, the 850M instance is shown in active state.

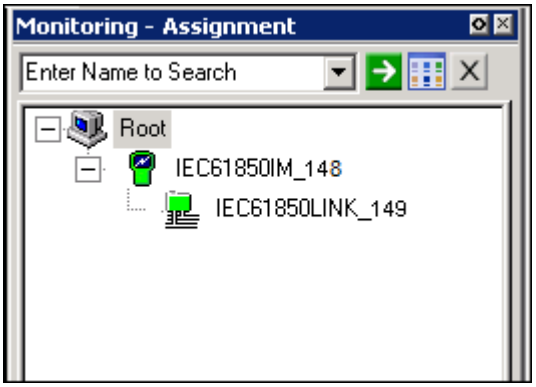


Figure 25: Loaded instance of 850M in Monitor tab

7.3.1 Loading 850M components

Related topics

“Loading 850M” on page 73
“Loading IED instance” on page 75

7.3.1.1 Loading 850M

Prerequisites

- Control Builder is running.
- 850M is installed and communicating with the Experion server.

To load an 850M instance

1 Right-click the required 850M and choose **Load**.
The **Load Operation** dialog box appears. The 850M and its link block are listed.

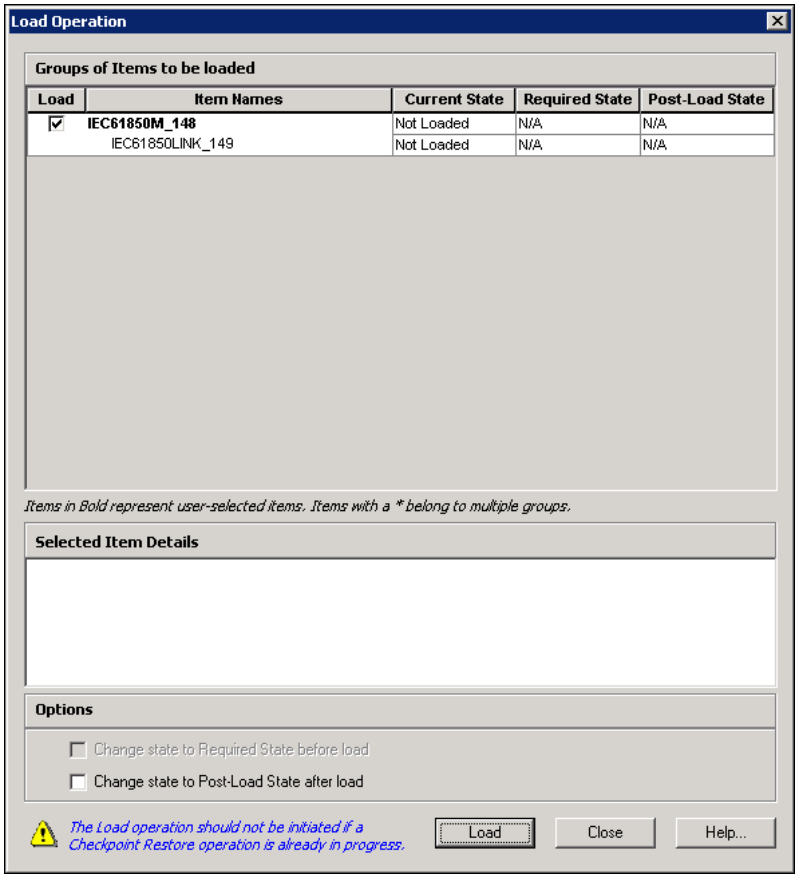


Figure 26: Load dialog box for 850M

2 Click **OK**.
The 850M loading to the monitoring side begins.

3 After successful load, the 850M instance is shown in active state.

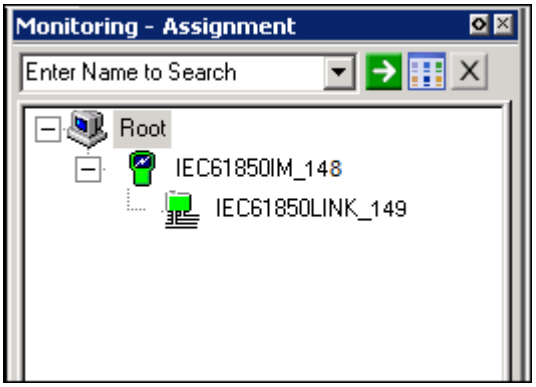


Figure 27: Loaded instance of 850M in Monitor tab

7.3.1.2 Loading IED instance

Prerequisites

- Control Builder is running.
- The 850M block and it's IEC61850LINK is loaded.

To load an IED

1 Right-click the required IED and choose **Load**.
The **Load Operation** dialog box appears. The IEC61850LINK is listed.

2 Click **OK**.
The IED loading to the monitoring side begins.

3 After successful load, the IED instance is shown in active state.

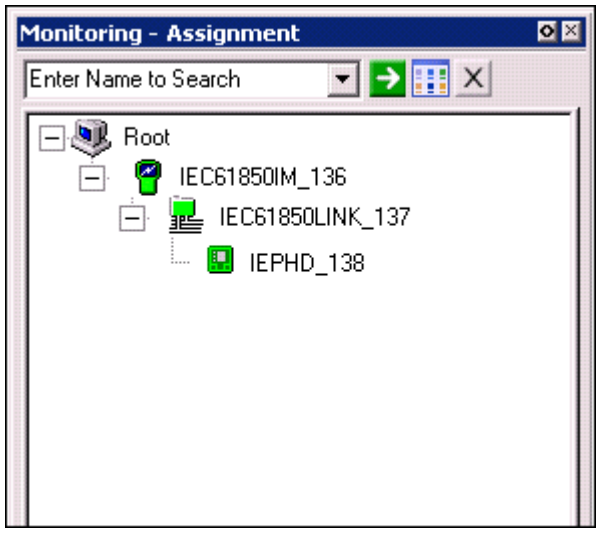


Figure 28: Loaded instance of IED in Monitor tab

7.4 Load With Contents command

The **Load with Contents** option shows the selected component and objects, (IEC61850LINKs, CMs, and so on) that are assigned to the selected component. For example, when an IEC61850LINK block is selected for loading, the **Load Dialog** lists all the objects assigned to (or contained by) that IEC61850LINK block in the dialog window. You can then select (or deselect) the objects that you want to load.

7.5 Reloading an 850M instance

Reloading component configuration is required when you make changes to the component or function block configuration, or after you replace a failed IED. You can use the applicable load procedure to reload data to components from the Project or Monitor tab. It is recommended to invoke the following commands through the Controller menu after a reload operation.

- “Upload to the Monitoring database” on page 79
- Update to Project

Before you begin reload, you must ensure that the 850M block on the Monitoring side is in IDLE State. If the block is not in IDLE state, the following error is shown

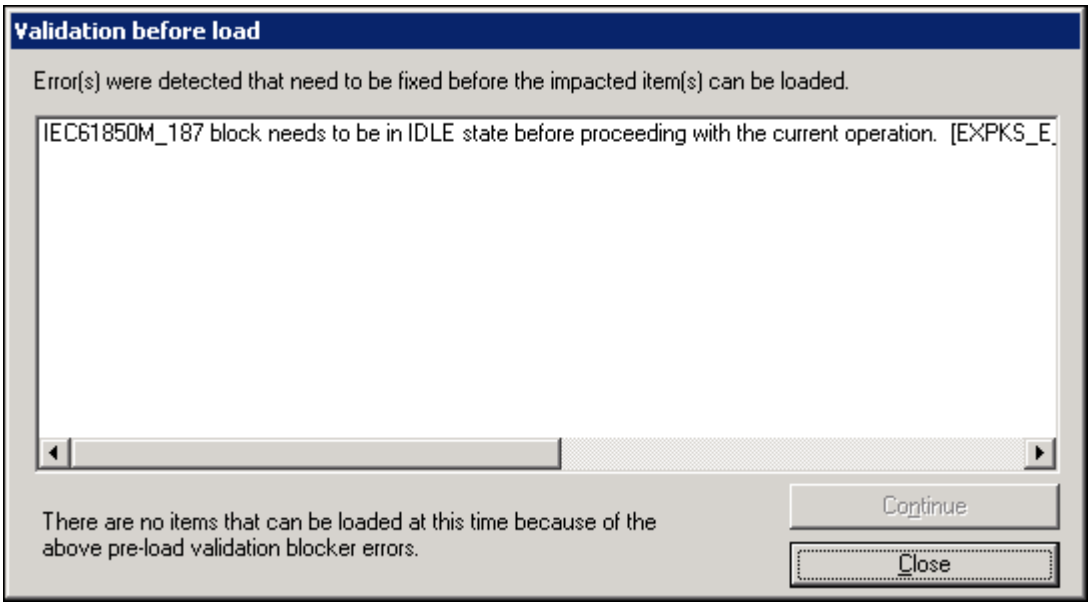


Figure 29: Error when the 850M is not in IDLE state

When the 850M block is in IDLE state, the **Load Dialog** appears. In the dialog box, both the 850M block and its IEC61850LINK blocks are listed. On clicking **OK**, the following warning appears. This warming appears only if the IEC61850LINK is reloaded along with the 850M block.

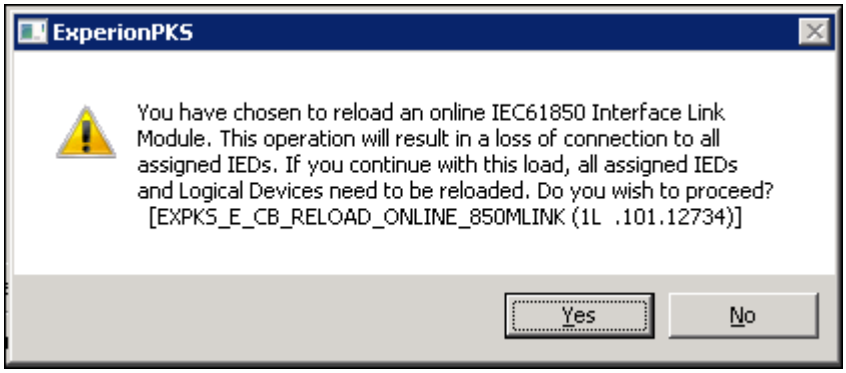


Figure 30: Warning when IEC61850LINK is reloaded along with the 850M

Click **Yes** to proceed with reload.

7.6 Upload to the Monitoring database

The upload operation uploads data for the selected objects from the 850M to the Monitoring Engineering Repository Database (ERDB). Upload of data for the selected objects from the server to the ERDB also can be performed.

Ensure to update the data to Project after an upload to the database, so that both the Monitoring and the Project databases are in sync.

See Using Upload Command in the*Control Building User's Guide* for procedures to upload component data.

8 Series C 850M redundancy functionality

This section provides information about using a redundant Series C 850M pair.

Related topics

8.1 Redundancy overview

850M redundancy is achieved by FTE network and IEC 61850 network communication. The IEC 61850 network has 3 Ethernet ports. Two Ethernet ports are used for FTE and one Ethernet port is used for IEC 61850 communication. The 850M does not communicate native HSR/PRP. Redbox is the redundancy box which is an IEC 61850 switch that converts Ethernet communication into the HSR/PRP field network. High availability requires that there are no intermediate switches between the 850M and Redbox.

Considerations

- Though it is possible to share a Redbox network appliance between multiple 850Ms by using an IEC 61850 compliant switch, it is recommended to connect each primary/secondary 850M must be directly connected to its own Redbox network appliance with no intermediate networking appliances for high availability redundancy. A shared switch, cable, or Redbox can result in several single points of failure, reducing the high availability of the redundant 850M configuration.
- The time take for initial synchronization of the 850M should be less than 400 seconds when the maximum number of Physical Devices, Logical Devices, and Logical Nodes are within specification.

Redundancy topology

The following figure shows a typical hardware configuration for a redundant 850M pair that includes a C300 Controller. You do not need the C300 Controller to support 850M redundancy.

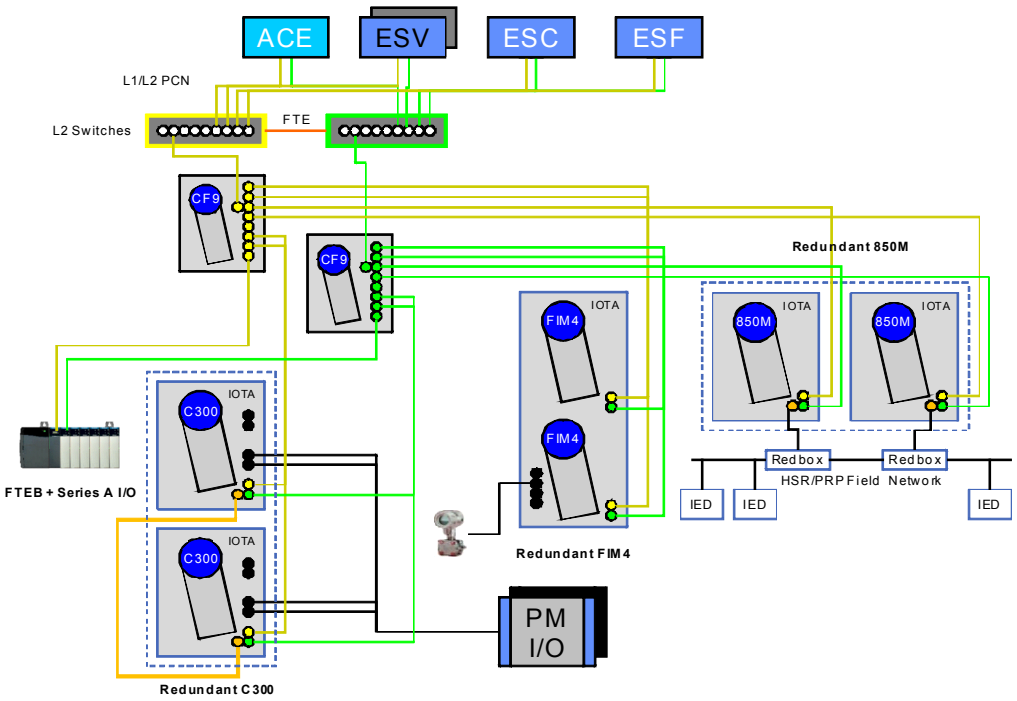


Figure 31: Redundancy topology

8.2 Redundancy configuration restrictions

This section describes the restrictions imposed to device configuration for the purpose of providing device redundancy.

Non-redundant device index

850M cannot be configured as non-redundant against the even device index.

Although the primary 850M configuration form accepts a numeric device index, the software verifies whether the device index is odd for the primary platform FB. The primary platform FB serves as the faceplate for the non-redundant and redundant primary 850M. Therefore, the software prohibits creation of a primary platform FB that targets the even device index.

Reloading the primary platform FB with MODISREDUN set false when the primary 850M has the even device index results in generation of a load error, **Cannot configure node at even Device Index as non-redundant EXPKS_E_CodeEvenDeviceIndexCannotBeNonRedun (6L .101.2351)**. Although the platform FB is loaded to the Control Builder monitor tree, it is not loaded to the 850M and the load error aborts load of any selected children blocks.

8.3 Partner compatibility

Controller redundancy is possible only when the primary controller has a compatible secondary partner. Once communication is established with the partner controller, the primary controller periodically sends a partner compatibility message that contains information necessary to perform the compatibility check, and the secondary responds with its own compatibility message. Each module compares local information against the supplied remote values to determine whether the partner module is compatible or incompatible. If all the compatibility criteria are satisfied, then the partner module is compatible. Otherwise, the partner module is incompatible and synchronization is not permitted. The following criteria are compared:

- Factory data, such as, vendor ID, product type, and product code must be identical to ensure same platform hardware.
- Firmware type must be identical to ensure same platform firmware. Some firmware personalities that differ in functionality share a common hardware platform (for example, the 5 ms and 50 ms C200 personalities). Synchronization cannot be allowed across different personalities.
- The partner module must have a properly configured device index. If this module has an odd device index N, the partner module has to have the even device index (N+1). Otherwise, if this module has an even device index M, the partner module has to have the odd device index (M-1).

Compatibility Results

RDNCMPT indicates whether redundant partner modules are compatible (from a controller redundancy perspective) and if not compatible, provides a reason why. The RDNCMPT parameter for the 850M platform indicates the following compatibility results (note that compatibility results that are obsolete or only supported on other platforms are not listed).

RDNCMPT	State	Description
– – –	Not applicable	Module is configured as non-redundant.
NOPARTNER	Not applicable	Initial/default state when no partner is responding to the partner compatibility query.
QUERYINPROG	Not applicable	Transient state while partner compatibility check is being performed.
COMPATIBLE	Compatible	Compatible indication for those platforms not sensitive to difference in firmware versions. This includes FIM2, FIM4, FIM8, FTEB, IOLIM, PGM, and 850M.
NodeNumber	Incompatible	Device Indexes of potential redundant partner modules are not properly configured as consecutive odd/even pair.
HardwareType	Incompatible	Mismatched factory data (i.e. different platform hardware).
FirmwareType	Incompatible	Mismatched compatibility types (i.e. different platform firmware).
PartnBootFmw	Incompatible	The partner module is executing from boot firmware (e.g. partner is in the Alive, Ready, or Fail State). To be compatible, both partners must be executing from application firmware.

8.4 Synchronization states

The RDNSYNCSTATE parameter indicates the controller's synchronization state. Given a redundant controller pair, synchronization is the act of transferring configuration and execution data from the primary controller to the secondary so that the secondary has the same information as the primary when it is needed to transition into the primary role. Synchronization is only possible for a compatible redundant controller pair; when a compatible partner is found, the controller transitions from the *No Partner State* to the *Partner Visible State*. **Initial-sync** is the act of performing first time transfer of synchronization data; during this time the controllers are in the Sync in *Progress State*. The redundant controller pair enters the *Synchronization Maintenance State* upon initial-sync completion. While in the *Synchronization Maintenance State*, the secondary is a viable replacement for the primary controller, and only that configuration data that is changed and the control data that changes as a consequence of primary controller execution is synchronized to the secondary controller.

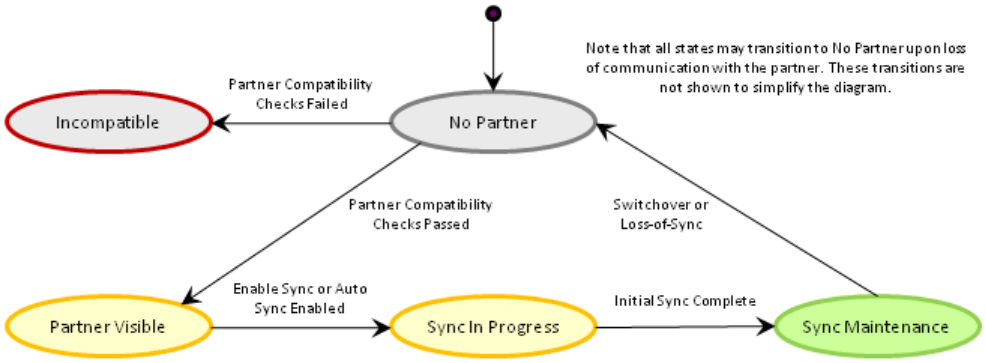


Figure 32: Synchronization states of 850M

8.5 Conditions that result in loss of synchronization

Starting with a synchronized or standby redundant controller pair, the following conditions result in loss of synchronization.

- Disable Sync command (from primary or secondary platform FB).
- Both FTE links to secondary controller are lost.
- The field network link to the secondary controller is lost.
- Field network faults that result in loss of communication between the primary and secondary 850M where either one of the following:
  - The primary 850M is not communicating with IEDs.
  - The primary 850M is actively communicating with at least one IED and the field network fault does not disrupt primary 850M communication with all IEDs.
- Shutdown command issued from the secondary platform function block.
- Loss of input power to secondary controller
- The secondary controller is reset (switch on IOTA).
- Secondary controller failure.
- Secondary controller firmware update.
- Removing the powered secondary controller module from its IOTA.
- The time taken for initial synchronization of the 850M(from Sync Start to Completion) should be less than 400 seconds.

8.6 Conditions that do not result in loss of synchronization

Starting with a synchronized or standby redundant controller pair, the following conditions do not result in loss of synchronization.

- Single FTE link to primary and/or secondary controller is lost.
- Field network faults that do not result in loss of communication between the primary and secondary 850M.

8.7 Switchover and secondary readiness

A switchover is a process where a synchronized secondary controller assumes the primary state. A switchover can be triggered immediately upon the detection of a fault in the primary or upon the receipt of an operator command. Depending on the switchover trigger, the original primary controller attempts to reboot into the secondary role, but this controller is not immediately able to participate in another switchover operation. After the new secondary reboots into the secondary role, it must first perform and complete initial-synchronization before another switchover is allowed.

The ability of a secondary 850M to take over the assigned control functions of the primary depends upon which one of the following readiness states reflects its current state.

If secondary 850M state is . . .	Then, the Secondary Series C 850M . . .
Not synchronized	Cannot assume the primary state. This is a state of non-readiness.
Synchronizing	Cannot assume the primary state. In this state, the secondary 850M is copying database information from the primary.
Synchronized	Can assume the primary state upon switchover. In this state, the database in the secondary is aligned with the database in the primary. The secondary closely tracks database changes to maintain its synchronization with the database of the primary. Otherwise, the secondary reverts to a not synchronized state.

8.7.1 Switchover conditions

The following conditions result in a switchover.

- Switchover command.
- Primary 850M failure results in a switchover.
- Secondary FTE reconnect when the primary has dual FTE disconnect results in initial-sync followed by immediate switchover.
- Secondary IEC 61850 reconnect when the primary has IEC 61850 disconnect results in initial-sync followed by immediate switchover.
- IEC 61850 field network faults that result in loss of communication between the primary 850M and all IEDs when the primary 850M was previously communicating with at least one IED.

Attention

Controller redundancy protects against all single faults and some dual faults. The Primary 850M IED communication fault switchover trigger is a dual fault that cannot be detected until after some control has been back-initialized with failsafe data. Although this dual fault affects control, switchover may provide automatic recovery that does not require the operator to diagnose how to deal with a primary that has complete loss of IED view.

8.7.2 Network switchover considerations

The redundant 850M operation accounts for the following key considerations associated with initiating a network switchover.

For this switchover consideration	850M redundancy operation
Device index number	The device indexes are fixed physical hardware identifiers and does not transition from primary 850M to the secondary 850M based on redundancy role.

For this switchover consideration	850M redundancy operation
IP address	The 850M uses floating IP address for its FTE IP address such that the lower (odd) IP address is used on the primary 850M and the higher (even) IP address is used on the secondary 850M. With floating IP address on the FTE network, the redundancy-role-based IP address cannot be used prior/during initial role determination. However, the 850M can generate ARPs to determine whether the primary & secondary IP address are in use or available for use on the FTE network. The 850M uses fixed IP on the IEC 61850 network such that the lower (odd) IP address is used on the 850M with odd device index and the higher (even) IP address is used on the 850M with even device index. With fixed IP address on the IEC 61850 network, the static IP address can be used for status message passing prior to any role determination when the IEC 61850 network IP address was previously configured and retained (on both primary and secondary 850M).

8.7.3 Switchover due to IEC 61850 network failure

The following table identifies IEC 61850 network failure conditions that result in a switchover and those that do not.

Failure conditions that result in a switchover	Failure conditions that do not result in a switchover
IEC 61850 link to primary controller are lost.	IEC 61850 link to secondary controller are lost.
IEC 61850 Network loss from IEC 61850 switch side.	IEC 61850 network fails with secondary.
	IEC 61850 SCADA server with dual home topology does not switchover when IEC 61850 network fails.

8.7.4 Switchover events

Switchover results in several Experion system events and alarms. All of them are system information or diagnostics type. No process alarms are generated due to switchover.

Typical events generated during switchover include the following:

- Connection failure to secondary module alarm
- Switchover event
- Unsynchronized alarm

Each of these events appears for 850Ms where switchover occurred.

9 Series C 850M operation

This section includes tasks associated with operating and monitoring the 850M.

Related topics

9.1 Series C 850M startup

The following table summarizes the stages the Series C 850M goes through after power is applied to its IOTA during startup. The Series C850M repeats these stages every time power is cycled Off/On.

Stage	Description
1	Power Light Emitting Diode (LED) Lights.
2	Executes firmware installed in FLASH memory. The initial firmware boot code is installed at the factory.
3	The Status LED briefly displays all of its colors: RED, GREEN, AMBER. Then, remains solid RED until the power-on self test (POST) completes.
4	Initiates a series of horizontal and vertical bars, as well as several brightness levels for evaluating the condition of the 4-character, alphanumeric display. At the end, the Link Status LEDs are blinked in turn.
5	Executes power-on self test to verify that all subsystems are working as intended. Cycles test number codes in the 4-character display to show progress of the test. (Initialization halts on the first test that finds an invalid or faulty piece of hardware. The Series C850M displays the test number code associated with the detected device failure until it is reset.)
6	Upon successful completion of the power-on self test, displays information about the application image currently stored through its 4-character display. The status LED should now reflect the true state of its associated hardware.
7	The 4-character display shows -bp- ((BOOTP) until it obtains its IP Address. The display then shows -ts- (Time Server) until time has been obtained from the NTP Server. Once its IP Address is known, it negotiates its redundancy role, either Primary or Secondary, with its partner module, if present. Verifies that the correct Device Index is displayed (#nnn) and that no addressing errors are detected. The primary module will have the odd IP address while the secondary module will have the odd + 1 IP address. The odd IP address follows the primary module during a switchover. The Device Index does not change during a switchover or any other role change. Once a device has obtained its IP Address and NTP Server IP Address(es), it retains them until its Device Index is changed or firmware is reloaded. (The Series C850M determines if any other module is using the same IP address. If it does find another module with the same Device Index, it does not join the network. Instead, it transitions to no address state waiting for new address assignment. If it finds another node with the same IP Address, it does not join the network. Instead, it transitions to dup address state; it must be reset to recover.)
8	The 4-character display cycles this information: Device Index setting, Link status, followed by Redundancy status. See the Display and LED Descriptions section for more information about the display and LED indications.

9.1.1 Series C 850M states in boot mode

850M state	Description
ALIVE	The 850M determined that no application image exists or an invalid application image is loaded. An upgrade can be performed in this state.
READY	The 850M received a command to remain in the boot mode to allow an upgrade.
FAIL	The controller detected a failure during startup. Use the CTools utility to retrieve problem report logs from the controller for failure diagnosis.

Tip
For information about upgrading the 850M, refer to the *C300 Controller User's Guide*.

9.1.2 Series C 850M states in application mode

850M state	Description
NODB	The 850M is configured as redundant or non-redundant and has not retained its database from operation prior to startup. The 850M moves to the NOTLOADED state.
IDLE	• The 850M is configured as non-redundant, or as redundant and has assumed the primary redundancy role. • The 850M has retained a valid database from operations prior to startup, • The 850M is configured to do a *Cold Start*. The 850Mmoves to the IDLE state.
OK	• The 850M is configured as non-redundant, or as redundant and has assumed the primary redundancy role. • The 850M has retained a valid database from previous operations prior to startup. • The 850M is configured to do a *Warm Start*. The 850Mmoves to the RUN state.
BKUP	The 850M is configured as redundant and has assumed the secondary redundancy role. The 850M moves to the BACKUP state.

9.2 850M faceplate displays

The faceplate of the 850M contains four LEDs and a four-character alphanumeric display as shown in the figure below. The labels on the LEDs are: Power, Status, FTE A and B.

The Status LED uses a 3-color scheme of red, green and orange. Generally, green indicates OK, red indicates power up tests, a fault or failure, and orange indicates backup mode. Blinking LEDs indicate a soft or hard failure and help to point to a problem. Soft failures also are indicated in other displays throughout the system. The four-character display provides additional 850M status information, see Faceplate display information. Directly below the display are two LEDs that indicate FTE activity.

Power and status LEDs

LED indication	Status/description	
Power LED		
GREEN Steady	Indicates the presence of 24Vdc to the 850M module.	
Status LED		
GREEN Steady	Non-redundant 850M OK Primary 850M OK (primary and backup 850Ms may or may not be synchronized)	
GREEN Blink off once per second (i.e. 1 sec. ON, 1 sec. OFF)	Primary OK with Soft Failure No database loaded (NODB)	
ORANGE Steady	Backup OK (850Ms synchronized)	
ORANGE Blink off once per second	Backup OK with Soft Failure (or 850Ms are not synchronized)	
RED steady	Selftest (POST) in progress, or Selftest has failed, Fault (hardware or software diagnostic failed), or Hardware Watchdog Timer expired	
RED Blink off once per second	Operating in BOOT mode: Alive state - (ALIV on faceplate display) Operating in Boot firmware, IP address assigned, primary address in use. No application image loaded, or manually put in Alive state for loading. Ready state - (RDY on faceplate display) Operating in Boot firmware, IP address assigned, primary address in use. Valid application image loaded.	
	AND faceplate display is blank.	Hardware Watchdog Timer expired.
	AND faceplate display is frozen.	Indicates unrecoverable fault.
	AND display is - frozen or blank	Unknown fault.
RED Blink off once per 1/4 second (i.e. 1/4 sec ON, 1/4 sec. OFF)	AND faceplate display shows: LOAD or PROG	Indicates: Firmware download in progress.
	AND faceplate display is blank.	Indicates: Hardware Watchdog Timer expired or other major fault.
OFF (a blank or frozen display)	AND faceplate display is frozen or blank.	Indicates: Fault (Hardware watchdog timeout or hardware failure)

Faceplate display information

The four-character display on the 850M faceplate shows a variety of information depending upon the 850M state and status:

- During 850M power-up, the display indicates the 850M's Power-On Self Test execution and software version.
- The 850M's operating state the display shows in a rotating display the FTE Device Index, and soft failures (such as redundancy, communications, or diagnostic faults).
- The 850M's redundancy role and synchronization status.
- Fault codes when the 850M ceases normal operation due to a major fault.

The following table includes a listing and descriptions of the various indications of the 850M display.

Table 3: 850M faceplate display indications

850M faceplate display	Indicates...	850M state shown on Station and Control Builder displays
(####) See Note 1	Communication Failure - No effect on 850M state, shown on Control Builder forms and Station displays	OFFNET
Tnnn	POST test number - Transient state, No CDA.	N/A
-BP-	850M in BOOTP mode waiting for IP address from BOOTP server - Transient state, No CDA.	BOOTING
-TS-	850M is attempting connection to configured time source, or time server is not available - Transient state, No CDA.	BOOTING
COMM See Note 2	850M not able to communicate with other nodes.	OFFNET
TEST	Factory Test mode - Non product state, No CDA.	TESTING
FAIL See Note 3	Failure in Module - No CDA	FAILED
ALIV	Boot mode with no valid application image - No CDA	ALIVE
RDY	Boot mode with application image - No CDA	PIREADY
LOAD	Firmware load in progress - No CDA	LOADING
PROG	Firmware flash in progress - No CDA	LOADING
NODB	Application mode with no database - CDA present	NOTLOADED
BKUP	Application mode with database loaded, all EEs good, module is secondary - CDA present	BACKUP
SF See Note 4	One or more soft fail conditions are present in the 850M. This state is independent on Redundancy role.	SOFTFAIL

Note 1: (####) - This symbol does *not* appear on the 850M faceplate display. It appears on Control Builder and operator (Station) displays representing the 850M to indicate that the 850M is OFFNET and this data is not available at this time. 850M continues to display the existing or changing faceplate display indication per the current 850M state. As a result of communication failure, CDA returns OFFNET as 850M Module State.

Note 2: The 850M is ‘lonely’ (cables disconnected or network related problem). Startup halts until 850M can obtain an IP address or validate an internally retained IP address.

Note 3: When a non-redundant 850M reboots into the FAIL state, it assumes the backup IP Address.

Note 4: SF indicates an on-line diagnostic soft failure, such as Battery status, and so on.

FTE activity LEDs

Each FTE port on the 850M has one status LED. The bi-color FTE A and B LEDs indicate connectivity (link present) and communication activity (transmit and/or receive). Table 4 describes the indications of the FTE Status LEDs.

Table 4: FTE activity LED indications

FTE A and B LEDs	Indicates...
RED	Link integrity check failed - No Ethernet signal detected, or cable is not connected.
OFF	Link integrity is OK - Ethernet signal is present, but no activity on link. Typically, every FTE node should show some activity. If the LED is observed for several seconds, some activity should be seen.
Blinking GREEN	Link integrity signal is present, with activity on link. During normal operation the FTE A and B LEDs should be blinking at a variable rate indicating normal network activity. Moderate to high network traffic conditions may cause the LEDs to appear as steady green.

9.3 850M faceplate display indications

850M display during normal operation

The 850M faceplate display rotates through the following fields during normal operation, executing the loaded application firmware:

<Device Index> -> <Redundancy Status>

For example, the display for a non-redundant or primary redundant 850M shows:

#003 -> RUN -> sync

The following table lists the possible display indications for 850Ms operating normally in application mode.

Table 5: Display indications when 850M is in application mode

Display Indications for…	Primary 850M	Secondary 850M	Description
Device Index	#nnn	#nnn	FTE Device Index, where nnn can be 001 to 255. Does not change with redundancy role.
850M State	NOEE / NODB / IDLE / RUN / OK	BKUP	Implies redundancy role.
Redundancy Status	-np-	-np-	No secondary/primary partner.
	!cpt	!cpt	Non-compatible partner visible
	!syn	!syn	Partner 850M visible, but not synchronized and initial sync not in progress.
	xxx	xxx	Initial sync is in progress, where xxx can be 000 to 100 to indicate percentage complete.
	sync	sync	Redundant 850M pair is synchronized.
	stby	stby	Backup 850M in Standby Secondary state (with retained database but normal synchronization disabled).
	nrdn	(n/a)	Indication that primary 850M is configured as non-redundant.
Soft Fail State See Note 1	SF	SF	Indicates a soft failure condition.

Attention
If a soft failure is detected, the soft failure indication alternates with the redundancy status indication.

850M display in BOOT mode

The 850M faceplate display rotates through the following fields when 850M is executing boot firmware:

<Device Index> -> <850M State>-> <Redundancy Role>

For example: **#003 -> ALIV -> PRI**

Table 6: Display indications when 850M is in boot mode

Display Indications for…	Primary 850M	Secondary 850M	Description
Device Index	#nnn	#nnn	FTE Device Index, where nnn can be 001 to 255. Does not change with redundancy role.

Display Indications for…	Primary 850M	Secondary 850M	Description
850M State	ALIV/ LOAD/RDY/ FAIL	ALIV/ LOAD/RDY/ FAIL	Does not imply redundancy role.
Fail Code	nnnn	nnnn	Indicated only when in FAIL, where nnnn = four digit failure code. Otherwise 850M State is displayed.
Redundancy Role	PRI or nrdn	SEC	Indicates redundancy role. See note.

Note: When the secondary 850M is in Boot mode, the 850M does not display BKUP because the 850M does not support redundancy in that 850M State. Similarly, when the secondary 850M is in Application mode, the 850M does not display SEC because the BKUP 850M State implies a redundant secondary.

9.4 Control Builder block icon descriptions

Adding an 850M block (non-redundant or redundant) to the Control Builder Project tab results in the appearance of an icon that represents a single 850M or redundant controller pair. Once the 850M block is loaded, the 850M icon appears in the Monitoring tab.

When a single 850M is defined, the icon appears as a single icon. When a redundant 850M is defined, two icons appear, one representing the primary 850M on the left and the icon representing the secondary 850M on the right. The appearance of either icon on top in a redundant controller pair indicates the active controller.

The following table shows the various appearances that the 850M block icon assumes based on the current 850M state and status.

Table 7: 850M icon indications in Control Builder

Icon	Represents . . .	850M state
Project Tab		
 (gray)	850M configured for non-redundant operation.	N/A
 (gray & white)	850M Primary configured for redundant operation.	N/A
 (white & gray)	850M Secondary configured for redundant operation.	N/A
Monitor Tab		
 (red)	850M is non-redundant and not communicating	No Communication (Offnet)
 (red & white)	Primary 850M is not communicating.	No Communication (Offnet)
 (white & red)	Secondary 850M is not communicating.	No Communication (Offnet)
 (yellow)	850M is non-redundant	No Database
 (yellow & yellow)	Primary 850M is not synchronized and partner 850M is visible	No Database
 (yellow & shadow)	Primary 850M is not synchronized and partner 850M is absent or incompatible	No Database

Icon	Represents . . .	850M state
 (green)	850M is non-redundant	Run or OK
 (green & white)	Primary 850M is synchronized	Run or OK
 (green & white, pause)	Primary 850M, standby synchronization	Run or OK
 (green & yellow)	Primary 850M is not synchronized and partner 850M is visible	Run or OK
 (green & shadow)	Primary 850M is not synchronized and partner 850M is absent or incompatible	Run or OK
 (white & green)	Secondary 850M is synchronized	Backup
 (white & green, pause)	Secondary 850M, standby synchronization	Backup
 (yellow & yellow)	Secondary 850M is not synchronized and partner 850M is visible	Backup
 (shadow & yellow)	Secondary 850M is not synchronized and partner 850M is absent or incompatible.	Backup
 (green)	850M is non-redundant	Run Soft Fail or OK Soft Fail
 (green & white)	Primary 850M is synchronized	Run Soft Fail or OK Soft Fail
 (green & white, pause)	Primary 850M, standby synchronization	Run Soft Fail or OK Soft Fail
 (green & yellow)	Primary 850M is not synchronized and partner 850M is visible	Run Soft Fail or OK Soft Fail

Icon	Represents . . .	850M state
 (green & shadow)	Primary 850M is not synchronized and partner 850M is absent or incompatible	Run Soft Fail or OK Soft Fail
 (white & green)	Secondary 850M is synchronized	Backup Soft Fail
 (white & green, pause)	Secondary 850M, standby synchronization	Backup Soft Fail
 (yellow & yellow)	Secondary 850M is not synchronized and partner 850M is visible partner present.	Backup Soft Fail
 (shadow & yellow)	Secondary 850M is not synchronized and partner 850M is absent or incompatible	Backup Soft Fail

9.5 Initiating 850M shutdown

The following procedure describes steps to initiate a shutdown command to the 850M, which results in the 850M rebooting to its RDY state or boot firmware.

Attention
Shutting down the 850M interrupts the transfer of data to the Experion system. Ensure that your system can tolerate the loss of live data, while the 850M is in its RDY state.

To shut down 850M

1. On the **Monitoring** tab, double-click the 850M icon.
   The **850M Block configuration** form appears.
2. Ensure the 850M is in IDLE state before initiating a shut down.
3. On the **Main** tab, click **Controller Command** box and then select **Shutdown** from the list.
4. Click **Yes** to confirm the action.
5. Wait for the 850M to reboot to its RDY state.

9.6 Initiating synchronization command

The following procedure provides steps to manually initiate synchronization to a redundant 850M pair.

Prerequisites

- You can view active redundant 850M pair on the **Monitoring** tab in Control Builder.

To initiate synchronization

1. In the **Monitoring** tab, double-click the primary IEC61850M icon.
   The **Parameters configuration** form appears.
2. In the **Redundancy** tab, click the **Enable Synchronization** button.
3. Click **Yes** to confirm the action and issue the synchronize command.
   The **Auto Synchronization** state is set as **ENABLED**.
4. Click **OK** to close the **Parameters** form.

9.7 Disabling synchronization command

The following procedure contains steps to manually disable synchronization to a redundant 850M pair.

Prerequisites

- You can view active redundant 850M pair in the **Monitoring** tab in Control Builder.
- The primary and secondary 850M are in one of the following states.
  - synchronizing state
  - synchronized state
  - standby state

To disable synchronization

1. In the **Monitoring** tab, double-click the primary IEC61850M icon.
   The **Parameters configuration** form appears.
2. In the **Redundancy** tab, click **Disable Synchronization**.
3. Click **Yes** to confirm disabling synchronization and issue the *Disable Synchronization* command.
   The **Auto Synchronization State** is **DISABLED**.
4. Click **OK** to close the **Parameters** form.

9.8 Initiating Become Primary command

The following procedure describes steps to manually cause an unsynchronized secondary controller to transition into a primary role in the absence of a partner controller.

Prerequisites

- You can view active redundant 850M pair on the **Monitoring** tab in Control Builder.
- The unsynchronized secondary controller has no view to a partner controller across the redundancy cable and the primary IP address is currently not occupied.

To command become primary

1 In the **Monitoring** tab, double-click the primary IEC61850M icon.
The **Parameters configuration** form appears.

2 In the Redundancy tab, click the **Become Primary** button.

3 Click **Yes** to confirm the action and issue the *Become Primary* command.
The secondaryIEC61850M assumes the primary role.

4 Click **OK** to close the **Parameters** form.

9.9 Initiating switchover command

The following procedure provides steps to manually initiate a switchover command to a redundant 850M pair.

Prerequisites

- You can view active redundant 850M pair in the **Monitoring** tab in Control Builder.
- The primary and secondary 850M are synchronized.

To command a switchover

1. In the **Monitoring** tab, double-click the primary IEC61850M icon.
   The **Parameters configuration** form appears.
2. In the **Redundancy** tab, click the **Initiate Switchover** button.
3. Click **Yes** to confirm the action and issue the switchover command.
   The secondary IEC61850M assumes the primary role. The old primary controller should boot up in the backup role.
4. Click **OK** to close the **Parameters** form.

9.10 Using station displays

850M Point Detail displays

The Experion Station application includes configured detail displays for the IEDs and logical devices in an 850M. These displays are the default entries for the Point Detail Display parameter on the **Server Displays** tab of the configuration form.

Once you establish communications with an 850M, you can begin monitoring the status of any component that has been loaded as part of a control strategy to an 850M with points registered in the Experion server. The dDetail displays let you quickly view the component's current state, fault status and pertinent configuration data.

System status displays

The System Status Display is part of the Alarm Management Displays in Station.

The 850M is represented in the System Status Display using the same icon set as is used in the “Control Builder block icon descriptions” on page 99.

Event and Alarm summary displays

The ExperionStation also provides Event and Alarm Summary displays that support 850M notifications and events. These displays are integrated with Experion component data. Use the Event Summary to get a quick view of recent actions that have taken place within the system.

Group detail displays

There are several group detail displays that can be configured. Some of them are as follows:

- The logical device and it's associated physical devices.

  The 850M and it's associated IEDs.

Custom displays

There are several controls available on the custom display for creating, executing, and monitoring activities. For more details, refer to the *Server and Client Configuration Guide*.

9.11 850M operating behaviors

This section describes some of the 850M's features and operating behaviors related to event and alarm reporting.

Related topics

“Time management in IEC 61850” on page 108
“Hardware watchdog timer” on page 110
“Critical task monitor” on page 110

9.11.1 Time management in IEC 61850

9.11.1.1 About time protocols

Simple Network Time Protocol (SNTP) is a proper subset of Network Time Protocol (NTP), which uses the same packet format. As a subset, SNTP gets time from an NTP server, but does not run complex filtering and control algorithms to extract the best time from multiple sources and precisely set the local clock increment rate. SNTP only measures round-trip-delay and sets the local clock when it drifts beyond internal limits.

Time protocols and Microsoft Windows

All supported Microsoft Windows operating systems use NTP. Each domain controller in a Windows Server 2003 or 2008 domain, by default, is an NTP server. The Active Directory provides a hierarchical time infrastructure. Each system added into the Active Directory/domain synchronizes time with a time source in the domains hierarchy.

About setting up time synchronization in your Experion PKS control system

Because the default Windows NTP implementation is not set up for the tolerances needed for control systems, Honeywell recommends that you use the *NTPConfig* tool to configure time synchronization on your Windows nodes. The *NTPConfig* tool corrects the tolerance deficiencies and converts the Active Directory default settings to be compatible with control system requirements. To overcome the tolerances, parameters are updated to maintain more stringent time synchronization.

If your control system is integrated with a Windows domain, it is recommended that you use the domain controller as the time source for *all the clients within the domain* (this is the default setting). As domain controllers are typically not on a network that is accessible to the control system itself, the controllers within the process control should be configured to get their time from an Experion server that has been set up as an NTP server acting as a secondary NTP server, which gets its time from the domain controller.

Time protocols and time servers for Experion PKS controllers

The C300 uses SNTP or PTP to attain the time, but includes its own proprietary ability to adjust the clock increment rate to that of the time source so that fewer actual adjustments (bumps) are necessary (similar to the functionality of NTP).

When plant-wide correlation of C300 DI-SOE is required,PTP must be provided.

As a client, Safety Manager supports the NTP protocol but also supports the PTP time protocol, which is used for synchronization over its own SafeNet network.

Precision time protocol (PTP)

The IEEE-1588 Precision Time Protocol provides high-precision time with low overhead. Unlike NTP, it is only a Local Area Network protocol, requiring a local time server, known as an IEEE-1588 Grandmaster. PTP supports multiple Grandmasters for availability. Typically, Grandmasters get their reference time from GPS, but can also get time from other GPS devices using one of the standard coaxial cable protocol connections. Multiple

units from the same manufacturer may even share a GPS antenna. PTP is a UDP Multicast protocol, so it adds some network traffic.

Time source hierarchy

The Series C controllers and interfaces have a time source hierarchy. When the better time source becomes unavailable, they degrade to a less-accurate source. From highest to lowest precision:

- PTP (if enabled)
- SNTP
- CDA Server Protocol

Time source configuration

SNTP is used when the IP addresses of one or two NTP servers are configured in Control Builder System Preferences. SNTP Server 1 is tried first. If unavailable, SNTP Server 2 is tried. PTP is used when individual devices are configured in Control Builder to use it. Once enabled, PTP is self-configuring.

PTP Grandmaster configuration notes

PTP defines synchronization profiles for various applications. We use the default profile. The basic settings are synchronization every two seconds, and using multicast for round-trip-time determination.

9.11.1.2 Maintaining time synchronization in an 850M

The 850M supports clock synchronization using version 2 of the Precision Time Protocol (IEEE Std 1588-2008). A dedicated Precision Time Protocol (PTP) time source is the preferred time source if the module is configured to use PTP. However, if the module is not configured to use PTP, SNTP time source is preferred.

When PTP is enabled, the module listens for PTP Master Clocks on the FTE network and synchronizes to the PTP Master Clock selected using the Best Master Clock algorithm as defined by the IEEE specification.

To support clock synchronization using version 2 of the PTP, a new parameter Enable Precision Time Protocol is introduced in the System Time tab of the 850M module properties.

The Experion FTE network is separate from the IEC 61850 network connection. Hence, the time source is connected separately to each network to provide the time to 850M to Experion network and IEDs using IEC 61850 network. Refer the following figure for details.

The IED receives time from the NTP master clock or the PTP master clock through the IEC 61850 switch as shown in the figure below.

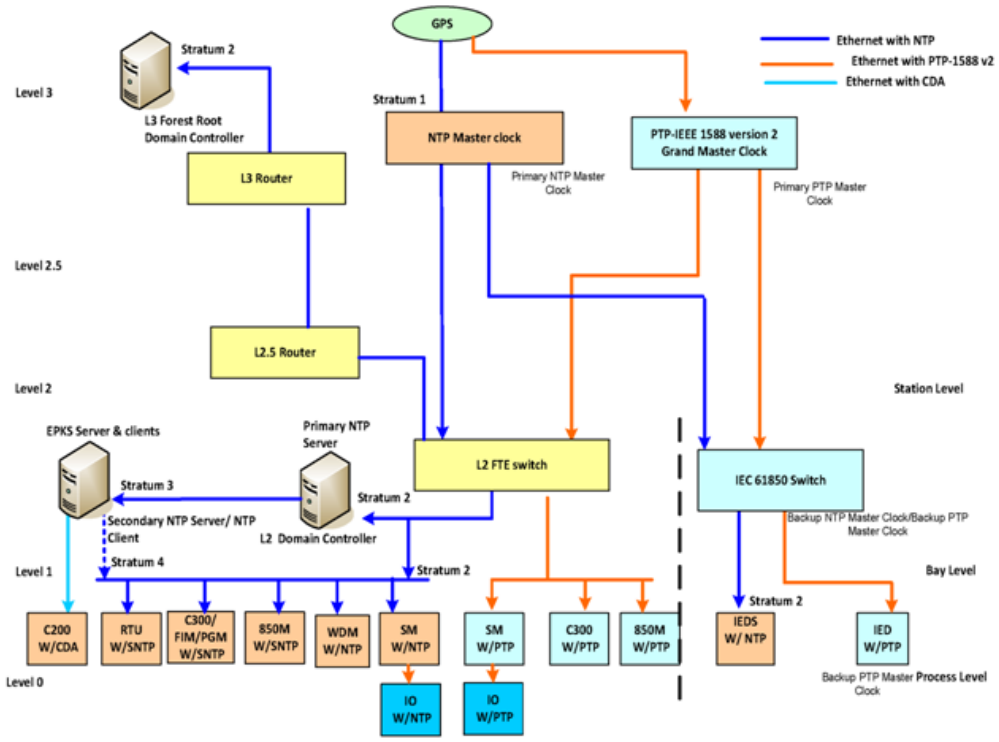


Figure 33: Time distribution topology in 850M network

Refer to the *Setting up time synchronization* section in the *Supplementary Installation Tasks Guide* for setting up a system time server.

9.11.2 Hardware watchdog timer

A Hardware Watchdog Timer is employed in conjunction with the Health Monitor and the internal Memory Management Unit to ensure that a catastrophic failure which disrupts the 850M's internal instruction execution or timing results in the 850M achieving a fail-safe state. The timer is refreshed periodically during normal 850M operation. If a refresh does not occur within the required time interval, the 850M suspends control execution and is placed into a safe state. A hardware watchdog timeout may cause the 850M faceplate display to become blank and the Status LED blinks red in 1/4 second intervals. The 850M attempts to re-boot into the FAIL state.

A refresh of the watchdog timer later than expected in normal operation, but not late enough to cause a timeout produces the soft failure condition: **WDT Software Warning**.

9.11.3 Critical task monitor

The Critical Task Monitor detects conditions for tasks executing within the 850M which are critical to proper control and view. Alarms and soft failures are generated when any of these tasks execute less frequently than expected.

Tasks critical to control

When a timeout occurs in the Critical Task Monitor for a task critical to performing control, the 850M asserts a hard failure, suspends normal operation and reboots into the FAIL state. If the 850M is redundant and

synchronized with the secondary 850M prior to the failure on the primary, a switchover occurs to allow the secondary to assume control. If the 850M is non-redundant or the 850M is redundant but was not synchronized with its secondary, the failed 850M is placed into a fail safe state. If capable, the 850M reboots into the FAIL state. When a timeout of a control-critical task occurs, the 850M generates the appropriate alarms (Diagnostic Alarm - Critical Task Watchdog Warning), but no other action is taken by the 850M.

There is an exception to this behavior where a timeout occurs when the 850M CPU is heavily loaded and the CPUFREE parameter indicates less than 5 percentage. The 850M does not take any action and does not re- boot into a FAIL state.

Tasks critical to view

Tasks executing in the 850M, which are critical to view, such as communication with I/O, display or peer devices, may not execute as required due to excessive loading of the CPU. The CPU overloading due to tasks other than executing control and result in a sustained level of CPU Free at 0 percentage (CPU usage is 100 percentage) may cause a loss of view of the 850M.

When a timeout of a view-critical task occurs, the 850M generates the appropriate alarms (Diagnostic Alarm - Critical Task Watchdog Warning), but no other action is taken by the 850M.

9.12 850M overload

850M overload processing behavior

When the 850M experiences processing overload the time to read data from or write data to an IEC 61850 IED (the latency in MMS request/response transactions) will lengthen and CPUFREE shows a value significantly below 20%. If this happens, the user should review the configuration of the 850M to determine how CPU usage may be reduced.

Causes of overloading

Processing overload can be caused by a combination of any of the following factors such that available processing power ('CPU') is exceeded.

- Exceeding the specified maximum number of function blocks
- Exceeding specified peer communication resource limits
- Exceeding specified display communication resource limits
- Exceeding specified PUSH block resource limits
- FTE network overload
- Call up of displays that collect data from the 850M

How to avoid overloading

To avoid processing overload, you should perform the following:

- Pay attention to and not exceed specified resource limits listed above.
- Maintain CPUFREE at 20% or more. Pay attention to the CPUFREE statistic as the 850M is loaded and operated.
- During operation, acknowledge warning alarms associated with low values of CPUFREE. Take appropriate steps to reduce CPU usage when such alarms occur on a frequent basis.
  - Decrease the number of IED parameters accessed and/or the frequency of IED parameter accesses
  - Decrease loading associated with other factors listed above under *Causes of overloading*

The 850M block supports the following diagnostic alarms related to CPUFREE.

- CPUFREE Low
  - Threshold defaults to 20% and can be configured.
  - Alarm is generated when CPUFREE is less than the threshold.
- CPUFREE Low Low
  - Threshold is fixed at 10% and cannot be configured.
  - Alarm is generated when CPUFREE is less than 10%.

9.13 Using bulk configuration tools

The **Bulk Configuration Tools** is used to do bulk build and bulk edit operations for process control strategies in Control Builder or in a local folder. This tool eliminates repetitive manual tasks, reduces system configuration cost, and enables the Project Engineers to deliver the project in a shorter time.

Bulk Configuration Tools is integrated in Control Builder as an add-in feature and can be invoked from the **Tools** menu. The data manipulation can be done in both online and offline.

For information about using the Bulk Configuration Tools, refer to the *Control Building User's Guide*.

Tip
If you are creating IEDs in bulk, then ensure to specify the IED name parameter along with ICD/CID file path.

9.14 Viewing 850M operation status in Control Builder

The **Monitoring** tab in Control Builder can be used to view the operation and status of any of the various 850M components represented as icons in the **Monitoring** tree.

Statistics tab – IEC61850M block

The **Statistics** tab shows messages details exchanged between the C300 Controller and the 850M. It contains statistical parameters used for maintaining and monitoring 850M performance. Information includes CPU utilization, hardware temperature and communications subsystem (CDA) statistics. The following table summarizes the parameter data you can monitor on the **Statistics** tab of the configuration form for the selected 850M block.

Plain Text	Parameter Name	User Configurable	Notes
Reset All Statistics	STATSRESET	No	Button to initiate reset of statistics in **Monitoring** mode.
CPU Statistics			
CPU Free	CPUFREEAVG	No	Current CPU Free value, in percent.
Minimum CPU Free	CPUFREEMIN	No	Minimum CPU Free value, in percent. Value represents minimum recorded since module power up or last statistics reset.
Time Since Powerup	UPTIME	No	Indicates time that has elapsed since the last powerup of the 850M CPU.
Hardware Temperature			
Current Temperature (degC)	CTEMP	No	Current operating temperature, in degrees C.
Maximum Temperature (degC)	CMAXTEMP	No	Maximum recorded operating temperature, in degrees C.
Minimum Temperature (degC)	CMINTEMP	No	Minimum recorded operating temperature, in degrees C.
Notification and Network Message Statistics			
Notifications Rate	TNUMNTFRQUAVG	No	Shows the total number of notification requests per second average.
Maximum Notifications Rate	TNUMNTFRQUMAX	No	Shows the total number of notification requests per second maximum.
Responder Input Rate	TRNUMINMSGAVGPS	No	
Max Responder Input Rate	TRNUMINMSGMAXPS	No	
Responder Output Rate	TRNUMOUTMSGAVGPS	No	
Max Responder Output Rate	TRNUMOUTMSGMAXPS	No	

Statistics tab – IEC61850LINK block

The **Statistics** tab shows messages details exchanged between the 850M and the IED. It contains CDA and Common Component Library (CCL) statistics used for maintenance and performance monitoring. The following table summarizes the parameter data you can monitor and/or configure on the **Statistics** tab of the configuration form for the selected IEC61850LINK block.

Plain Text	Parameter Name	User Configurable	Notes
Statistics			
Reset All Statistics	STATSRESET	No	Button to initiate reset in **Monitoring** mode.
Notification Statistics			
Notifications Rate	NUMNTFRQUAVG	No	The number of Notification Requests per second average.
Maximum Notifications Rate	NUMNTFRQUMAX	No	The number of Notification Requests per second maximum.
Responder Statistics			
Total Responder Rate	NUMPARRSPAVG	No	The average number of parameter get/store responses per second.
Maximum Total Responder Rate	NUMPARRSPMAX	No	The maximum number of parameter get/store responses per second.
Peer Responder Rate	CPEERAVGPPS [ ]	No	The average number of peer parameters per second processed by the IEC61850LINK.
Maximum Peer Responder Rate	CPEERMAXPPS [ ]	No	The maximum number of peer parameters per second processed by the IEC61850LINK.
Display Responder Rate	CDISPAVGPPS [ ]	No	The average number of display peer parameters per second processed by the IEC61850LINK.
Maximum Display Responder Rate	CDISPMAXPPS [ ]	No	The maximum number of display peer parameters per second processed by the IEC61850LINK.
IEC 61850 Network			
Total IEDs	NUMIEDS	No	The number of IEDs configured in an IEC 61850 network per second.
MMS Request Rate	MMSRPS	No	The number of data sets read operations between IEC61850M and IED per second.
MMS Store Rate	MMSSTORERPS	No	The number of read operations between IEC61850M and IED per second.

Memory tab – IEC61850LINK block

The Memory tab contains data on general memory usage in the 850M. It also shows memory usage parameters in terms of internal memory units: descriptors and blocks. The following table summarizes the parameter data you can monitor on the **Memory** tab of the configuration form for the selected IEC61850LINK block.

Plain Text	Parameter Name	User Configurable	Notes
Memory Usage in KBytes			
Total User Memory(kb)	TOTALMEMINK	No	Shows the total size of user memory pool, in kilobytes.

Plain Text	Parameter Name	User Configurable	Notes
Currently Used Memory(kb)	USEDMEMINK	No	The total amount of used memory in user memory pool, in kilobytes.
Currently Free Memory(kb)	FREEMEMINK	No	Amount of free memory in user memory pool, in kilobytes.
Largest Free Memory Block Size(kb)	MAXFREEINK	No	The size of largest contiguous memory block in user memory pool, in kilobytes.
Memory Usage in Bytes			
Total User Memory(b)	TOTALMEM	No	Total size of user memory pool, in bytes.
Currently Used Memory(b)	USEDMEM	No	Total amount of used memory in user memory pool, in bytes.
Currently Free Memory(b)	FREEMEM	No	Current amount of free memory in user memory pool, in bytes.
Largest Free Memory Block Size(b)	MAXFREEBLKSZ	No	Shows size of largest contiguous memory block in user memory pool, in bytes.
Memory Descriptors			
Total Memory Descriptors	NTOTMEMDESC	No	Total number of memory descriptors available.
Free Memory Descriptors	NUMFREEDESC	No	Number of free (available) memory descriptors.
Registered Memory Descriptors	NUMREGDESC	No	Number of registered memory descriptors.
Used Memory Descriptors	NUMUSEDDESC	No	Number of used memory descriptors.
Memory Blocks			
Used Memory Blocks	NUMUSEDBLKS	No	Number of used memory blocks.
Free Memory Blocks	NUMFREEBLKS	No	Number of free (available) memory blocks.
External Memory Blocks	NUMEXTBLKS	No	Number of external memory blocks.
Driver Memory Usage			
Reserved (kb)	DRVMEMRESERVED	No	The amount of reserved memory in kilobytes for 850M hardware.
Reserve Used (kb)	DRVMEMUSED	No	The amount of memory in kilobytes used by the 850M hardware.
Reserve Free (kb)	DRVMEMFREE	No	The amount of memory in kilobytes available for 850M hardware. (The value is calculated by Memory pools free + DRVMEMRESERVED – Pools RAM used).

Statistics tab – IED block

The **Statistics** tab shows the response details of an IED during its interaction with 850M.

Plain Text	Parameter Name	User Configurable	Notes
Statistics			
Reset All Statistics	STATSRESET	No	Button to initiate reset in **Monitoring** mode.
IEC 61850 Comm Performance			
Average Response Time (ms)	RESPTIMEAVG	No	The average response time of an IED to a request sent from an IEC61850M.
Fastest Response Time	RESPTIMEMIN	No	The number of data sets read operations between IEC61850M and IED per second.
Slowest Response Time	RESPTIMEMAX	No	The number of read operations between IEC61850M and IED per second.

10 IEC 61850 SCADA server acting as alarm and events server

The IEC 61850 SCADA server supports configuration of events and alarms. For information about configuring events and alarms, refer to the *IEC 61850 SCADA Configuration Reference* document in the Experion PDF Collection.

11 850M maintenance

This section includes information about maintaining the 850M including replacement of the 850M module and associated IOTA.

Related topics

“Periodic checks” on page 122
“Recommended spare parts” on page 123
“Replacing an 850M module and IOTA” on page 124

11.1 Periodic checks

Check . . .	Possible Corrective Action . . .
That all segments of the 4-character display and the light emitting diodes (LED) on 850M are working.	If segment or LED is not lit or has dimmed, you must replace the 850M, since front-panel indicators and LEDs are not field replaceable.
That all connections are secure.	Secure connections, as needed.
That cable insulation is not worn or cracked.	Replace cables, as required.
That IOTA is secure.	Tighten mounting screws.

11.2 Recommended spare parts

The following table provides a list of parts that you may want to keep on hand for backup.

Attention

Since aging occurs, even if the batteries have been regularly recharged throughout their lifetime, the 24 Volt Battery, Honeywell part number should be replaced after every two years of operation.

Part Name	Description	Quantity per 10/100
850M	850M	1/5
850M IOTA	C850M Input Output Terminal Assembly	1/2
Fuse	800 mA, quick-acting fuse on Input Output Terminal Assembly	4/25
RAM Charger Assembly	Module, RAM Charger 2 Connections	2/10
RAM Charger Assembly	Module, RAM Charger 4 Connections	2/10
24 Volt Battery Backup Kit	Battery Kit Main (3 batteries and interconnecting cables)	1/5
* Supersedes RAM Charger Assembly <part number>.		

11.3 Replacing an 850M module and IOTA

For replacing a non-redundant 850M module

CAUTION

This procedure can only be performed while off process.

- We recommend that you proceed with **extreme caution** whenever replacing any component in a control system. Be sure the system is offline or in a safe operating mode.
- Component replacements may also require corresponding changes in the control strategy configuration through Control Builder, as well as downloading appropriate data to the replaced component.
- Do not disconnect the redundancy cable while you disconnect the FTE cables from a primary 850M as this may cause unusable dual-primary condition.
- If you remove the redundancy cable then reboot the 850M after connecting the redundancy cable prior to reconnecting the network cables.

- Loosen screws at each side of the module cover that secures the 850M module to the IOTA board.
- Loosen the plastic screw on the front of the 850M module cover. Be careful not to strip the plastic screw head.

For replacing a redundant or secondary 850M module

CAUTION

This procedure can be performed while on-process *only* if the module to be replaced is in the secondary role.

We recommend that you proceed with **extreme caution** whenever replacing any component in a control system. Be sure the system is offline or in a safe operating mode.

Component replacements may also require corresponding changes in the control strategy configuration through Control Builder, as well as downloading appropriate data to the replaced component.

For replacing a non-redundant 850M IOTA board

CAUTION

This procedure can only be performed while off process.

We recommend that you proceed with **extreme caution** whenever replacing any component in a control system. Be sure the system is offline or in a safe operating mode.

Component replacements may also require corresponding changes in the control strategy configuration through Control Builder, as well as downloading appropriate data to the replaced component.

To replace a non-redundant 850M module

1. Carefully remove the 850M module from the IOTA board and connector.
2. Insert the new 850M module onto IOTA board making sure that the 850M circuit board mates properly with the IOTA board connector.

   Note that all modules are keyed.
3. Secure the 850M module to the IOTA board with two screws located at each side of the plastic cover.
4. Using a #2 Phillips screwdriver, hand tighten the plastic screw on the front of the module cover. Be careful not to strip the plastic screw head.
5. The new 850M boots up to ALIVE or NODB state.
6. Load firmware which is the same version as was running in the old 850M.
7. In **Control Builder**, perform a '**Load with Contents**' to the 850M.

To replace a redundant or secondary 850M module

1. In **Control Builder**, open the primary 850M FB and select the **Redundancy tab**. Click the **Disable Synchronization** button to the auto-sync parameter to "Disabled."

2 Perform steps 1 through 5 of the procedure .

3 Load firmware which is the same version as was running in the old 850M.

4 The new backup 850M will boot to ALIVE or BKUP. If the application image does not match the primary 850M, it will be unsynchronized.

5 From either the primary or secondary 850M FB **Redundancy tab**, click the **Enable Synchronization** button to initiate synchronization and allow auto-synchronization.

6 The 850M will now display a synchronized redundancy state.

To replace a non-redundant 850M IOTA board

1 On the defective IOTA, loosen screws at each side of the module cover that secures the 850M module to the IOTA board.

Loosen the plastic screw on the front of the 850M module cover. Be careful not to strip the plastic screw head.

2 Carefully remove the 850M module from the IOTA board and connector.

3 Label and disconnect all cables from the IOTA board connectors, (yellow and green FTE cables, gray cables, and Battery cable).

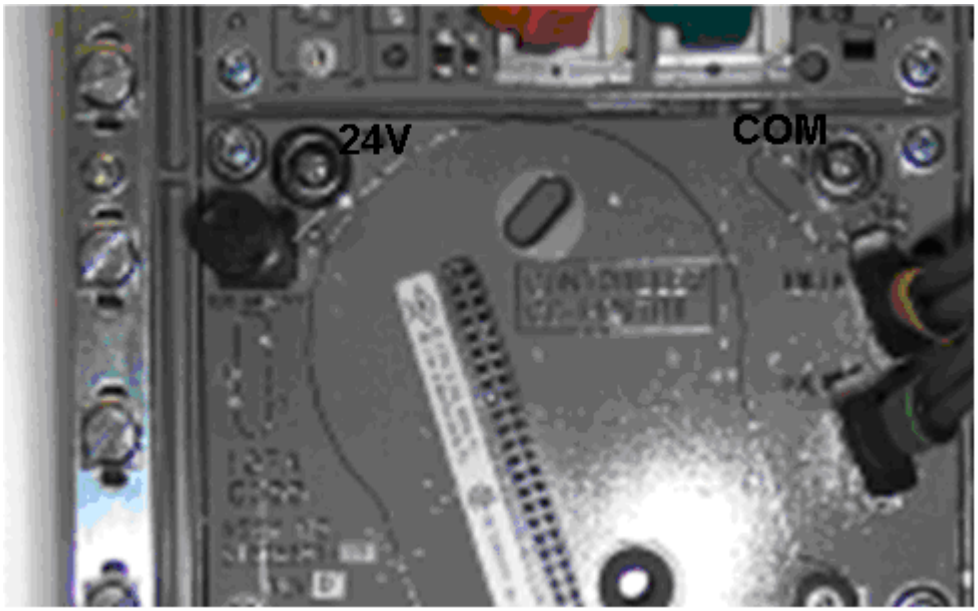
CAUTION

Do **not** fully tighten the IOTA mounting screws before installing and tightening the power and ground screws (**24V** and **COM** terminals) which can bind during installation or removal. Follow instructions carefully.

4 Loosen the four mounting screws only **half-way** that secure the IOTA board to the channel.

5 Remove 24V power to the IOTA board. See figure below.

- Remove the screw from the left side of the IOTA board that connects to the **24 Vdc** bus bar.
- Remove the screw from the right side of the IOTA board that connects to the **COM** bus bar.



6 Remove completely the four mounting screws securing the IOTA board to the channel and remove the IOTA.

7 Place screws, washers and spacers aside for reassembly.

8 Assemble screws, washers and spacers on the new IOTA board.

Mount new 850M IOTA board on the channel at the same position as the old IOTA board.

9 Insert and thread the four mounting screws only **half-way** to attach the IOTA board to the channel. Do **not** tighten.

10 Refer to the figure above.

11 Tighten the four mounting screws securing the IOTA board to the channel.

- Insert and tighten the screw to the left side of the IOTA board that connects to the **24 Vdc** bus bar.
- Insert and tighten the screw to the right side of the IOTA board that connects to the **COM** bus bar.

12 Set the Device Index address to the same address as the old IOTA using the three rotory **FTE DEVICE INDEX** switches.

13 Connect FTE-A and FTE-B Ethernet link cables to the RJ-45 connectors on 850M IOTA board.

- The **yellow** Cat5 cable connects to the "**FTEA**" connector on the IOTA.
- The **green** Cat5 cable connects to the "**FTEB**" connector on the IOTA.

14 Install the two-wire twisted pair Battery cable onto the **MEMORY HOLD-UP** connector on the left side of the IOTA board.

15 Insert the 850M module onto IOTA board making sure that the 850M circuit board mates properly with the IOTA board connector.

Secure the 850M module to the IOTA board with two screws located at each side of the plastic cover.

16 Using a #2 Phillips screwdriver, hand tighten the plastic screw on the front of the module cover. Be careful not to strip the plastic screw head.

17 The 850M will boot-up into an ALIVE state or a NODB operating state.

18 In **Control Builder**, perform a '**Load with Contents**' to the 850M.

To replace a redundant or secondary 850M IOTA

1 In **Control Builder** open either the primary or secondary 850M FB and select the **Redundancy tab**. Click the **Disable Synchronization** button to set the Auto-Synchronization State parameter to "DISABLED."

2 Perform steps 1 through 17 of the procedure

Note that there is additional orange REDUNDANCY cable connected to the IOTA.

3 The 850M will boot-up into an unsynchronized secondary redundancy state with BKUP operating state.

4 From either the primary or secondary 850M FB form **Redundancy tab**, click the **Enable Synchronization** to initiate synchronization and allow auto-synchronization.

5 The 850M will now display a synchronized redundancy state.

12 Series C 850M troubleshooting

This section provides guidance and background information about the causes and remedies for failures which may occur in the 850M.

Related topics

“What to do when faults occur” on page 128
“Fault classifications” on page 129
“Initial checks” on page 132
“Fixing common problems” on page 134
“Soft failures” on page 140
“Online diagnostics” on page 144
“Communications and system time faults during startup” on page 131
“Communication failures in 850M” on page 152
“Gathering information for reporting problems to Honeywell” on page 154
“Guidelines for requesting support” on page 155

12.1 What to do when faults occur

If an 850M fails, it does not fail into a state that should cause unsafe process conditions. When a fault occurs, you must gather information related to the event, such as: the status of the 850M, the conditions or sequence of events that occurred before the fault. See “Initial checks” for a list of information. This information can be gathered from various sources in the system. See “Initial checks” for guidance in obtaining information from displays, diagnostic tools and log files within the Experion system. Read the topics in this section that includes troubleshooting procedures to clear faults. Refer to other troubleshooting sources.

12.2 Fault classifications

Faults have been classified based on the severity of the failure. The 850M behavior when a failure is detected is determined by type of fault and whether the 850M is non-redundant, or is one of a redundant 850M pair. The following table identifies these fault classifications and describes 850M behavior in response to the fault type.

This section also includes more detailed descriptions of these fault classifications, how these faults are indicated both on the 850M faceplate and through other system displays and corrective actions to clear the faults.

Table 8: 850M fault classifications and possible causes

Fault classification	Description
Hard Failure	Hardware detected failure. Operation cannot continue. If software is running, the affected 850M is rebooted into the FAIL State. • Hard failure on a synchronized primary 850M triggers a switchover to the backup 850M. • Hard failure on a backup 850M causes a loss-of-synchronization (and reduced availability until fault is corrected). • Hard failure on a non-redundant 850M causes a loss-of-control and loss-of-view.
Severe Failure	Software detected failure. Operation cannot continue. The affected 850M is rebooted into the FAIL State. • Severe failure on a synchronized primary 850M triggers a switchover to the backup 850M. • Severe failure on a backup 850M causes a loss-of-synchronization (and reduced availability until fault is corrected). • Severe failure on a non-redundant 850M causes a loss-of-control and loss-of-view.
Partial Failure	Software detected failure. Non-redundant 850M could continue to operate. • Partial failure on a non-redundant 850M results in some or all loss-of-view and/or loss-of-control. However, the 850M does not reboot into FAIL State but continues to provide whatever services it can.
Soft Failure	Software detected failure. 850M continues to operate with full control and full view. Soft failures are alarmed to the operator. FTE is monitored by the FTE System Management Tool. • Soft failure on the synchronized primary 850M does *not* trigger a switchover to the backup 850M. • Soft failure on the backup 850M does *not* result in a loss-of-synchronization. • Soft failure on a non-redundant 850M does *not* result in loss-of-control or loss-of-view.
Installation/Startup Failure	Software detected failure. 850M may not become operational. • Installation/Startup failure on a non-redundant 850M results in the inability to commence control or view the 850M on the network. • Installation/Startup failure on the backup 850M results in the inability to complete initial synchronization or view the 850M on the network. • Installation/Startup failure does not apply to the synchronized primary 850M, because installation & startup must be successful to reach a synchronized primary state.

12.2.1 Hard/severe failures

When a hard failure is detected, the following 850M events occur depending on its redundancy status:

- Hard/severe failure on a synchronized primary 850M triggers a switchover to the backup 850M. If capable, the failed 850M reboots into the FAIL state and captures diagnostic data which may contain internal state events that occurred prior to a failure. The CTools utility can be used to retrieve the diagnostic data.

- Hard/Severe failure on a backup 850M causes a loss-of-synchronization. The Primary 850M continues operation, but enters the ‘Not synchronized’ state. If the redundant 850M pair was not synchronized when the fault occurred, then the failed 850M reboots into the FAIL state, if capable. No further synchronization will occur and no switchover will occur.
- Hard/Severe failure on a non-redundant 850M causes a loss-of-control and loss-of-view. The I/O modules associated with the 850M force their outputs to safe values. If capable, the failed 850M reboots into the FAIL state and captures diagnostic data which may contain internal state events that occurred prior to a failure. The CTools utility can be used to retrieve the diagnostic data.

Alarm display and function block detail display

Usually a hard or severe failure results in a communication failure. Calling up the Alarm Detail Display in Experion Station or the 850M Block Detail Display will show this failure.

Control Builder indications and error log

Using Control Builder, you can view the current state of 850Ms in the system. In the Control Builder monitor tab, a hard failure in the 850M is denoted by a red 850M icon indicating no communication. See “Control Builder block icon descriptions” on page 99 for a complete listing of the 850M icons that may appear in Control Builder.

The Errlog_n.txt log provides a running list of Control Builder detected errors in chronological order. The n represents any number that is assigned to the most recent log.

To check the log, navigate to this file location on the server: *<Drive>:\Documents and Settings\All Users \Application Data\Honeywell\Experion\Errlog_n.txt*.

12.2.2 Soft Failures

Soft Failures are detected also through execution of the 850M's “Online diagnostics” on page 144. Soft failures do not cause change in the state of the 850M's execution environments. There is no loss of control or loss of view when an 850M detects a soft failure.

In a redundant 850M pair, a soft failure in a synchronized primary 850M does not cause a switchover to the backup 850M. A soft failure in the backup 850M does not result in a loss of synchronization, if the redundant 850M pair is synchronized.

Alarm displays and Control Builder forms

Soft failures are reported in the Alarm Summary and the 850M Function Block Detail displays in Station. In Control Builder, soft failure status is indicated on:

- The Main tab of the configuration form for the associated 850M block (Soft Failures Present).
- The “Soft failures” on page 140 includes a list of the possible soft failure conditions.

  The Control Builder monitor tab, soft failure in the 850M is denoted by a 850M icon with a small red circle with an **x** inside the circle.

Soft Failure alarm return to normal

The alarm returns to normal once the on-line diagnostics detect that the soft failure condition has been corrected. Note that on-line diagnostics run on a cycle and hence it may take a period of time for the 850M to perform the subsequent diagnostic check for the condition, notice the change and then record it.

In some cases, online diagnostics may continue to assert the soft failure condition even when it appears to have been corrected. This may happen when one occurrence of the soft failure is considered sufficient to require action that requires replacement of hardware. When the 850M hardware is replaced, the alarm returns to normal once the 850M function block is deleted and reloaded.

12.2.3 Installation startup failures

A fault that is detected during the 850M's startup may prevent the 850M from entering an operational state. The 850M executes a boot program automatically when power is applied to the 850M. These tests, verify the presence and integrity of the 850M. See “Communications and system time faults during startup” for details on abnormal startup conditions and corrective actions to clear them.

12.2.4 Communications Failure

The System Management Display software application provides the means to configure and monitor FTE nodes in Experion. The FTE Status Server and FTE Auxiliary display includes detailed information on FTE links monitored by the FTE Provider. See the *Fault Tolerant Ethernet Status Display User's Guide* for more details.

12.2.5 Communications and system time faults during startup

The tables in this section help to provide guidance for determining the cause of abnormal startup conditions in the 850M. These conditions may occur when the 850M:

- Cannot establish normal communication on the FTE network
- Cannot obtain its network address from the system's BootP server
- Cannot obtain system time from the time source configured for the domain in which it resides,
- Finds that CDA services are not available.

Various indications on the 850M's faceplate display or the state of the Control Builder icon that represents the 850M (if the 850M had been loaded previously) are described that point to a abnormal condition.

The following tables detail the abnormal conditions for both redundant and non-redundant 850M configurations and whether or not the 850M memory has been retained via battery backup.

Corrective actions for resolving these conditions are found below the tables, (see Secondary 850M with Memory Retention).

12.3 Initial checks

This section offers some checks that you can make to help isolate the problem. The checks are arranged in no particular order.

Checking Control Builder error code reference

An indication of a problem may be in the form of an error dialog that includes an error message and possibly an error code in Control Builder.

The syntax for a typical Control Builder error message is as follows:

Connection to device is not open EPKS_E_CL_NOCONN(6L.101.3326)

In this syntax, the error code is the last four digits in the message or **3326**.

Please refer to the *Control Builder Error Codes Reference* book for applicable error code information.

Checking faceplate display and LEDs

Check the 850M's 4-character display and 850M/IOTA LED indications and compare results with data. For more details on these fault classifications and possible causes of these faults see the “Fault classifications” on page 129.

Fault Classifications	Module display	LEDs
“Hard/severe failures” on page 129	**FAIL** alternating with a four-digit error code **03A7** = Hardware failure Any other four digit code = possible software fault A blank display indicates a Watchdog Timer timeout.	Status LED = RED
“Soft failures” on page 140	**-SF-** alternating with the following module information: <DeviceIndex> <Rdn State> <DeviceIndex> -SF -	Primary module - Status LED = GREEN blinking off once per second Backup module - Status LED = ORANGE blinking off once per second
“Installation startup failures” on page 131	**Tnnn** indicating the test number that the module was performing when a fault was detected. **-bp-** BootP service not available **-TS-** Time source not available.	Status LED = solid RED
“Communications Failure” on page 131	**COMM** indicating no communications with other nodes.	FTE LEDs = RED

Using CTools to capture diagnostic data

You can use the CTools utility to capture diagnostic data used to examine the operating conditions within the module. This data also can be analyzed to determine the cause of an error or fault. The following data can be captured using CTools.

- Trace Log
- Registers
- SSP

- Call Stack
- Instructions

See Series C Firmware Load Tool (CTools) for Series C Components in the *Control Hardware Troubleshooting and Maintenance Guide* for the procedure to capture diagnostic data.

Viewing flash log

The Flash.txt log provides a list of firmware updates that have been initiated.

To view the log, navigate to this file location on the server:

C:\Program Files\Honeywell\Experion\Engineering Tools\system\bin\Flash.txt.

Viewing release information log

The ReleaseInfo.txt log provides a list of Experion software releases that have been installed on the computer.

To view the log, navigate to this file location on the server:

C:\Program Files\Honeywell\Experion\Engineering Tools\system\bin\ReleaseInfo.txt.

Checking server point build log

The SvrPtBld_servername.txt log provides list of process (CB) points built in the server database.

To check the log, navigate to this file location on the server: *C:\Program Files\Honeywell\Experion PKS \Engineering Tools\temp\SvrPtBld_servername.txt*.

Checking server point build error log

The svrptblderr_servername.txt log provides list of any errors associated with process (CB) points built in the server database

To check the log, navigate to this file location on the server: *C:\Program Files\Honeywell\Experion PKS \Engineering Tools\temp\svrptblderr_servername.txt*.

Checking error log

The Errlog_n.txt log provides a running list of Control Builder detected errors in chronological order. The n represents any number that is assigned to the most recent log.

To check the log, navigate to this file location on the server: *C:\ProgramData\Honeywell\Experion PKS \ErrLog_n.txt*.

12.4 Fixing common problems

Loss of power

The power supply has failed or the main power source has shut down or is experiencing a brownout or blackout condition.

Diagnostic Check	• The 4-character display on the 850M and LEDs on the module and the IOTA are off. • In the **Monitoring** tab, the 850M icon turns red.
Cause 1	Main power source is disconnected or shut down either manually or temporarily by *brownout* or *blackout* condition.
Solution	Re-connect the main power source or turn it On or wait for temporary *brownout* or *blackout* condition to pass.
Cause 2	The 24 Vdc power supply failed or power cable is disconnected or failed.
Solution	Replace the 24 Vdc power supply or re-connect/replace the power cable.
Cause 3	Power fuse opens on IOTA.
Solution	Replace power fuse.

Module display shows -bp- or -ts-

After the 850M completes POST, the module was unable to contact the BootP server to obtain an IP address. Note that if BootP service is available, but no time service is available, the module display shows -ts-.

Diagnostic Check	Display shows -bp-
Cause	BootP service is not available.
Solution	If the display shows -bp- • Check FTE cable connections to FTE A and FTE B connectors on the module IOTA. • Verify FTE network connections between the module IOTA and the associated server. • Verify that the bootP service is running on the associated server. Restart BootP service if not running. • In Control Builder, check System Preferences for valid network IP address settings. Verify correct configuration of System Time server. If the display shows -ts- • Verify that the NTP source is available on the network and NTP time source is properly configured in the control builder system preference.

Diagnostic Check	Display shows -ts-
Cause	BootP service is available, but time source is not available. Time Server may not be configured or server may not be running the latest release time service.
Solution	Verify that the system time source is configured. Check that the Server Windows Time Service (w32time) is running on the server.

Module display shows -SF- alternating with OK/BKUP

A Soft Failure condition is detected during execution of background diagnostics.

Diagnostic Check	Display shows -SF- alternating with OK/BKUP
Cause	Soft Failure condition detected by module.

Solution	• View Soft Failures tab of 850M block configuration form to identify fault. • Use 850M Detail Display in Station to identify fault. • Refer to 850M Soft Failures table for description and corrective actions.

One or both FTE LEDs are RED

The 850M has detected a fault in the FTE cables or the IOTA.

Diagnostic Check	One or both FTE LEDs on the module faceplate are RED.
Cause 1	No connection.
Solution	Check cable connections on module IOTA (FTEA and FTEB connectors) and at CF9 IOTAs.
Cause 2	Bad cables
Solution	Swap known good cable with suspect cable. Replace bad cable.
Cause 3	Bad switch port.
Solution	Swap cables with known good port to identify defective port. Replace assembly that contains defective port.
Cause 4	Bad IOTA.
Solution	Replace IOTA

FTE receives fault diagnostics

The 850M has detected an open receive signal line between either of its two Ethernet interface devices and the processor handling incoming communication.

Diagnostic Check	• The Status LED on the front panel of the 850M turns RED • The LAN_A or LAN_B indicator for the faulted port turns RED. The indicators are found on the FTE Tab of the 850M Block configuration form. • An alarm is generated by the 850M that indicates **FTE Port A Receive Fault** or **FTE Port B Receive Fault**.
Cause	The following conditions may result in a false indication of an FTE Receive Diagnostic fault. These conditions are external to the 850M that allow a carrier to be detected by the 850M's Port A or Port B Ethernet interface but eliminate FTE traffic on that port. • Disconnecting the uplink cable of a CF9 when only one device is connected to any of the downlink ports on the CF9. When the uplink cable is disconnected, there are no incoming messages to the device. Since the downlink cable from the CF9 to the 850M remains attached, the 850M has a 'good' Link Status on the port. The combination of a good Link Status and no incoming messages results in the spurious indication of an FTE Receive Fault. • Removal and re-insertion of a CF9 module or power cycling a CF9, when the associated 850M is not power cycled. In this case, when the CF9 is powered up, Link Status transitions to the ‘good’ state before the CF9 completes its power on self tests (POST) and starts passing FTE Diagnostic messages again. This interval is long enough that the 850M's FTE Receive Fault Diagnostic indicates a spurious fault. • Throttling of Ethernet traffic during of an abnormal amount of communication traffic on one or both of the 850M's Ethernet ports. During a ‘storm’ on the FTE network, the 850M initiates limiting of incoming Ethernet traffic on its FTE ports. As a result of this limiting, a sufficient number of incoming messages may be lost so that while one or both ports see ‘good’ Link Status signals it sees no traffic over the sample interval of this diagnostic. In this case, the 850M's FTE Receive Fault Diagnostic indicates a spurious fault. The spurious alarm generated by the FTE Receive Fault Diagnostic is a relatively minor side effect, in the case of a network storm. A network storm is signaled by other alarms in the system.

Solution	Unless you suspect that one of the causes described previously exists and is resulting in a spurious indication, replace the 850M Module exhibiting this diagnostic at your earliest convenience. When this fault exists, network redundancy for this node no longer is working. See “Replacing an 850M module and IOTA” on page 124.

Module does not synchronize with backup

Diagnostic Check	Primary module cannot synchronize with backup. In the Monitoring tab, double-click the primary 850M icon to call up its Parameters configuration form. Click the Redundancy tab to display it. Troubleshoot to correct condition for inhibiting sync.
Cause 1	Bad redundancy cable.
Solution	Replace redundancy cable. Check to see if modules synchronize.
Cause 2	Bad backup module
Solution	Replace module. See “Replacing an 850M module and IOTA” on page 124 for details. Check to see if modules synchronize.
Cause 3	Backup IOTA bad.
Solution	Replace the IOTA. Reinstall the original backup module on the new IOTA. See “Replacing an 850M module and IOTA” on page 124 for details. Check to see if modules synchronize.
Cause 4	Primary module bad.
Solution	Replace primary module. See “Replacing an 850M module and IOTA” on page 124 for details. Check to see if modules synchronize.
Cause 5	Primary IOTA bad.
Solution	Replace primary IOTA. Reinstall the original primary module on the new IOTA. See “Replacing an 850M module and IOTA” on page 124 for details. Check to see if modules synchronize.
Cause 6	Software problem.
Solution	Contact Honeywell SSC.

Module failure

The 850M software has detected a module failure condition that can be a multiple-bit error or excessive single-bit errors in the main Random Access Memory (RAM).

Diagnostic Check	• The 4-character display on the module shows FAIL or mMBE. • In the Monitoring tab, the 850M icon turns red.
Cause	The module software has detected a failure that does not allow operation to continue. There can be many causes for a failure including hardware. See the *Using CTools to capture diagnostic data* to capture diagnostic data for the device to determine the possible cause before proceeding. If the error occurs in the backup RAM, a fault is indicated. If the error occurs in main RAM, the module freezes with mMBE on the display.

Solution	Try shorting the reset pads on the IOTA to restart the module. If error persists, replace the module. See the “Replacing an 850M module and IOTA” on page 124 for details. Check the Trace log for breadcrumbs that occurred prior to the event. See *Using CTools to capture diagnostic data* for more information. Provide the results of the trace log to Honeywell Solutions Support Center (SSC) for analysis.

Display shows FAIL

The 850M detects failure during system integrity checks, such as Watch Dog Timer (WDT), error detection circuits, Field Programmable Gate Array (FPGA) readback, microprocessor static configuration registers, and Read Only Memory (ROM) checksum.

Diagnostic Check	• The 4-character display on the module displays FAIL. • In the Monitoring tab, the 850M icon turns red.
Cause	The module software has detected a background diagnostic failure that does not allow operation to continue.
Solution	Recycle power to the module. If error persists, replace the module. See “Replacing an 850M module and IOTA” on page 124 for details. Check the Trace log for breadcrumbs that occurred prior to the event. See *Using CTools to capture diagnostic data* for more information. Provide the results of the trace log to Honeywell Solutions Support Center (SSC) for analysis.

Isolated (lonely) Node

For a redundant 850M pair, Fault Tolerant Ethernet (FTE) communications with partner and FTE network are lost.

Diagnostic Check	The Primary module determines whether or not to initiate a switchover. If the Secondary was n a better condition than the Primary at the time of fault determination, then the Primary must fail so that a Secondary switchover is initiated. But, the new Secondary (old Primary) still cannot restore FTE communications. The Secondary module must reboot once, in an attempt to restore communications. The Primary module reports the problem in the Secondary. If the Secondary cannot restore FTE communications, it must synchronize again over the redundancy link and be a partially functional backup.
Cause 1	Secondary module is defective.
Solution	Replace the secondary module that initiated switchover when fault was detected. See “Replacing an 850M module and IOTA” on page 124 for details. If secondary module synchronizes after replacement, the removed module is defective. Otherwise, go to Cause 2.
Cause 2	Secondary IOTA is defective.
Solution	Replace the Secondary IOTA that initiated switchover when fault was detected. See “Replacing an 850M module and IOTA” on page 124 for details. If Secondary module synchronizes after replacement, the removed IOTA is defective. Otherwise, go to Cause 3.
Cause 3	Primary module is defective
Solution	Replace the Primary module. See “Replacing an 850M module and IOTA” on page 124 for details. If you can command synchronization after replacement, the removed 850M is defective. Otherwise, go to Cause 4.
Cause 4	Primary IOTA is defective

Solution	Replace the primary IOTA. See “Replacing an 850M module and IOTA” on page 124 for details. If the module pair synchronize after IOTA replacement, The removed IOTA is defective. Other wise, go to Cause 5.
Cause 5	There is a software problem.
Solution	Contact Honeywell Solution Support Center (SSC).

Duplicate Device Index setting

The FTE subsystem detects duplicate Device Index settings in separate nodes.

Diagnostic Check	All nodes stop tracking cable status for the detected duplicate Device Index value. Communications continue and does not impact system performance until there is a cable fault. This fault is detected by the FTE System Management Tool. A duplicate Device Index can cause a duplicate IP Address. In most cases, the duplicate IP Address would be detected first and prevent the FTE diagnostic messages from being sent.
Cause	Device Index switches on separate IOTA's are set to same value.
Solution	Change Device Index switches setting on one of the IOTA's to a unique value.

Device Index value is zero upon power up

The module's 4-character display shows a Device Index value of zero (#000).

Diagnostic Check	Be sure Device Index switches on the IOTA were not intentionally set to zero to initiate a Device Index/IP Address reset.
Cause 1	Device Index switches set to zero.
Solution	Change Device Index switches to correct setting.
Cause 2	The module is defective
Solution	Replace the module. See “Replacing an 850M module and IOTA” on page 124 for details. If Device Index switch setting matches Device Index number in 4-character display upon module power up, the removed module is defective. Otherwise, go to Cause 3.
Cause 3	The IOTA is defective.
Solution	Replace the IOTA. See “Replacing an 850M module and IOTA” on page 124 for details. If Device Index switch setting matches Device Index number in 4-character display upon module power up, the removed IOTA is defective.

IED template creation failure

The IED template creation fails.

Diagnostic Check	IED template creation fails.
Cause	Usage of incorrect Data types, usage of data types that are not according to IEC 61850 standards
Solution	Correct the data type in the ICD file or contact the IED manufacturer to get the corrected IED ICD file.

Invalid subnet mask address configuration of 850M

The 850M accepts invalid subnet mask address values.

Diagnostic Check	The 850M accepts invalid subnet mask address values. For example, 164.145.96.191/164.145.96.192. The subnet mask must consist of all 1's followed by all 0's, with at least two 0's in the lower bits.
Cause	Usage of incorrect values.
Solution	1. Delete the 850M platform function blocks from the Monitor tree. 2. Edit the primary platform function block on the Project tree. 3. Change the 850M mask to a valid mask (for example, 255.255.255.0). 4. Reload the primary and secondary platform function blocks.

12.5 Soft failures

The **Soft Failures** tab provides indications of various soft failure conditions for the 850M hardware. The following table describes these soft failure conditions detected by the 850M during background diagnostic checks, when indicator is lit.

Plain Text	Parameter Name	Notes	Condition when indicator is lit	Corrective Action
Battery State Warning	BATTERYNOTOKSFTAB	Indicates the status of CPM battery. Status is also shown on **Main** tab of 850M block. The *Battery State Warning* soft failure condition is indicated when the 850M does not have a battery backup and the **Disable Battery Alarm and Soft Fail** field in the **Main** tab is not checked.	Indicates that battery voltage for module RAM retention is not within specified limits. Module state may not be maintained through a power down. This would prevent warm start and may require the user to reload control strategies when power is restored.	On the 850M block **Main** tab. • If Battery Status = UNDERVOLTAGE, then replace battery. • If Battery Status = OVERVOLTAGE, ensure that the battery type used is specified by Honeywell.
Device Index Switches Changed	BCDSWSTS	Online diagnostic warning: Switches broken or deliberately changed.	The Device Index switch changed while the 850M was operating. This condition would place the module at a different and unexpected IP address following a subsequent module restart.	Verify if the Device Index switch setting is correct, reset if necessary. If failure still persists, the IOTA may be defective. Replace the IOTA. **CHECK** Reset/reboot will cause module to assume new/incorrect address. If visibly correct, rotate each of them 360 degrees. If this corrects problem, replace IOTA. Otherwise replace module then IOTA.
Factory Data Error	FACTDATAERR	Online diagnostic error reading factory data.	The Factory Data block is corrupt which may cause failure of Boot Image download or Application Image download during a subsequent module restart.	Replace the module and return faulty module to the factory.
ROM Application Image Checksum Failure	ROMAPPIMGCHKSMFAIL	Online diagnostic error: ROM application image may be corrupted.	The module Application Image is corrupted which may cause a failure on a subsequent module restart.	Reload the 850M Application image. See “Upgrading 850M firmware” on page 30 for procedure. If failure still persists, replace the module and return faulty module to the factory.

Plain Text	Parameter Name	Notes	Condition when indicator is lit	Corrective Action
ROM Boot Image Checksum Failure	ROMBOOTIMGCHKSMFAI L	Online diagnostic error: ROM boot image may be corrupted.	The 850M Boot Image is corrupted which may cause a failure on a subsequent module restart.	For redundant modules: • If primary, command a switchover. • If backup, reboot, reset or remove and reinsert module. If module does not fail POST, continue normal operation. Re-load the 850M Boot image. See “Upgrading 850M firmware” on page 30 for procedure. If failure still persists, replace the module and return faulty module to the factory.
WDT Hardware Error	WDTHWFAIL	Online diagnostic error: Fault detected in the Watchdog Timer hardware circuit.	The watchdog timer hardware circuit is faulty.	Replace the module and return faulty module to the factory.
WDT Refresh Warning	WDTSWFAIL	Online diagnostic warning: Watchdog Timer is being refreshed late and close to the timeout limit.	The watchdog timer is being refreshed at a rate which is outside acceptable limits. Or The watchdog timer is being refreshed late, but not late enough for it to expire.	Contact Honeywell SSC. You may be asked to #8230. • Further describe operating conditions • Gather module logs • Capture and provide the control strategy running in the module • Replace the module
Critical Task Watchdog Warning	TASKHLTHMON	A key task within the module is executing less frequently than normal.	Indicates that one of a number of key tasks within the module is executing less frequently than expected. See “Critical Task Monitor” on page 179 for more information.	Contact Honeywell SSC. Note that an alarm associated with this soft failure appears immediately after detection of a timeout on one of these internal tasks. The timeout will place the module in a FAIL state with a fail code of 0123.
Uncorrectable Internal RAM Sweep Error	RAMSWEEPERR	Uncorrectable single-bit errors in Main RAM.	Test of the RAM location where the module's Application Image executes has detected an uncorrectable bit error. Possible hardware failure which may affect module operation.	Replace the module and return faulty module to the factory.

Plain Text	Parameter Name	Notes	Condition when indicator is lit	Corrective Action
Corrected Internal RAM Sweep Error	RAMSCRUBERRS	Corrected single-bit errors in Main RAM.	Test of the RAM location where the module's Application Image executes has detected (and corrected) a number of bit errors which have exceeded the acceptable threshold. Possible hardware failure which may affect module operation.	Replace the module and return faulty module to the factory.
Uncorrectable User RAM Sweep Error	BACKUPRAMSWEEPERR	Uncorrectable single-bit errors in Application RAM.	Test of the RAM location where the module's control strategies and states are maintained has detected an uncorrectable bit error. Possible hardware failure which may affect module operation.	Replace the module and return faulty module to the factory.
Corrected User RAM Sweep Error	BACKUPRAMSCRUBERRS	Corrected single-bit errors in Application RAM.	Test of the RAM location where the module's control strategies and states are maintained has detected (and corrected) a number of bit errors which have exceeded the acceptable threshold. Possible hardware failure which may affect module operation.	Replace the module and return faulty module to the factory.
Debug Flag Enabled	DEBUGFLAGSET	Warning: Engineering internal debug flag is set.	Indicates that engineering debug firmware is running in the module. Non-standard behavior and/or performance may occur.	If not running a special image under the direction of HoneywellSSC, reload the module with the 850M firmware for the Experion system release that is currently running on the system.
Minimum HW Revision	MINHWREVSF		Indicates that the module hardware is useable (POST passes) but it must be upgraded for proper operation.	Replace module with a module that meets current hardware specifications.
Partner Not Visible On FTE	PARTNERNOTVISFTE	Indicates redundant module partner is not visible on FTE.	Indicates that the Fault Tolerant Ethernet (FTE) communications with redundant module partner and FTE network are lost.	See *Isolated (lonely) Node*.
Dup IP - IEC 61850 Network	DUPIPIECNETWORK		Indicates that there is another node on the network with this IP address.	Either change the IP address or remove the other node from the network.
IEC 61850 FTE Network Subnet Conflict	FTEIECSUBNETCONF		Due to routing issues, the FTE network and the 850M-network are not allowed to be in the same IP address range.	Check the FTE's IP address and network mask against the IEC 61850's IP address and mask. Both IP address ranges must be on different networks.

Plain Text	Parameter Name	Notes	Condition when indicator is lit	Corrective Action
IEC 61850 Link Inactive	IECLINKINACTIVE		Indicates that the IEC 61850 network fails.	Check the network cable between the 850M and the network switch. If that does not resolve the issue, then check the network switch's port settings on the port connected to the IEC 61850 uplink.

The following soft failures appear in the Redundancy tab (of an 850M).

Plain Text	Parameter Name	Notes	Condition when indicator is lit	Corrective Action
No Partner Communication on FTE network	RDNCOMMFAILFTE	The 850M establishes redundancy communication on both the FTE and IEC 61850 networks. This parameter reflects the redundancy communication status on the FTE network.	850M is not able to see it's partner on the FTE network.	Check the FTE cable connections.
No partner communication on IEC 61850 network	RDNCOMMFAILRDN	The 850M establishes redundancy communication on both the FTE and IEC 61850 networks. This parameter reflects the redundancy communication status on the IEC 61850 network.	850M is not able to see it's partner on the IEC 61850 network.	Verify IEC 61850 switch port speed setting, Flow control and port mirror. Also, check the cable connections.

12.6 Online diagnostics

Hardware diagnostics are executed within the 850M during normal operations. Some diagnostics execute frequently, but all diagnostics are designed to complete within eight hours (the Diagnostic Test Interval).

When a fault is detected by the 850M, it identifies and reports the fault to the system and acts to maintain control and view through a switchover, if required (in the case of synchronized redundant 850M pairs). Various actions are taken by the 850M depending upon the severity or type of fault (Fault classification). Even though some of these detected faults do not cause a failure or an action (such as a switchover) by the 850M, the faults are reported to alert operators of a potential failure in the future if not corrected.

12.7 Communications and system time faults during startup

The tables in this section help to provide guidance for determining the cause of abnormal startup conditions in the 850M. These conditions may occur when the 850M:

- Cannot establish normal communication on the FTE network
- Cannot obtain its network address from the system's BootP server
- Cannot obtain system time from the time source configured for the domain in which it resides,
- Finds that CDA services are not available.

Various indications on the 850M's faceplate display or the state of the Control Builder icon that represents the 850M (if the 850M had been loaded previously) are described that point to a abnormal condition.

The following tables detail the abnormal conditions for both redundant and non-redundant 850M configurations and whether or not the 850M memory has been retained via battery backup.

Corrective actions for resolving these conditions are found below the tables, (see Secondary 850M with Memory Retention).

12.7.1 Conditions for redundant and non-redundant 850M configurations

12.7.1.1 Non-redundant 850M with memory retention

850M Faceplate		Problem	850M block time source	Station alarm
Status LED	Blinking Red -> Green	No communication on FTE network.	Internal	850M OFFNET
FTE LEDs	Off			
Display	BP for 2 min. TS for 3 min. then IDLE			
CB icon	Red			
Status LED	Blinking Red -> Green	Communication on FTE network. • No communication via CDA • Unable to establish connection to system time source	Internal	CDA Comm Lost Connection
FTE LEDs	Blinking Green			
Display	TS for 3 min. then -> IDLE			
CB icon	Grey			
Status LED	Blinking Red -> Green	Communication on FTE network • Communication via CDA • Unable to establish connection to system time source	CDA	Not Using Configured Timesource
FTE LEDs	Blinking Green			
Display	TS for 1 min. then -> IDLE			
CB icon	Red -> Blue			

850M Faceplate		Problem	850M block time source	Station alarm
Status LED	Green	Communication on FTE network • No communication via CDA • Established connection to system time source	SNTP	CDA Comm Lost Connection
FTE LEDs	Blinking Green			
Display	IDLE			
CB icon	Grey			
Status LED	Green	None. Normal operation for non-redundant 850M with battery backup following a power cycle.	SNTP	None
FTE LEDs	Blinking Green			
Display	IDLE			
CB icon	Blue			

12.7.1.2 Non-redundant 850M with no memory retention

850M faceplate		Problem	850M block time source	Station alarm
Status LED	Blinking Red	No communication on FTE network 850M does not complete startup.	Internal	850M OFFNET
FTE LEDs	Off			
Display	COMM			
CB icon	Red			
Status LED	Blinking Red -> Blinking Green	Communication on FTE network • No Communication via CDA • Unable to establish connection to system time source	Internal	CDA comm Lost Connection
FTE LEDs	Blinking Green			
Display	TS for 3 min. then -> NODB			
CB icon	Grey			
Status LED	Blinking Red -> Blinking Green	Communication on FTE network • Communication via CDA • Unable to establish connection to system time source	CDA	850M Not Synchronized
FTE LEDs	Blinking Green			
Display	TS for 1 min. then -> NODB			
CB icon	Red			
Status LED	Blinking Green	Communication on FTE network • No communication via CDA • Established connection to system time source 850M appears to startup normally but Control Builder cannot communicate with the 850M …so attempts to load or reload 850M fail. If 850M was loaded	SNTP	CDA comm Lost Connection
FTE LEDs	Blinking Green			
Display	NODB			

850M faceplate		Problem	850M block time source	Station alarm
CB icon	Grey	before a power cycle, its associated icons in the Monitor tab is Red.		
Status LED	Blinking Green	None. Normal operation for non-redundant 850M with no battery backup following a power cycle.	SNTP	850M Not Synchronized
FTE LEDs	Blinking Green			
Display	NODB			
CB icon	Yellow			

12.7.1.3 Redundant Primary 850M with memory retention

850M faceplate		Problem	850M block time source	Station alarm
Status LED	Blinking Red	No communication on FTE network.	None	850M OFFNET
FTE LEDs	Off			
Display	BP for 2 min. COMM for 1 min. TS for 3 min. then IDLE			
CB icon	Red			
Status LED	Blinking Orange	Communication on FTE network. • No communication via CDA • Unable to establish connection to system time source 850M transitions to secondary redundancy role assuming its partner has CDA available.	None	CDA Comm Lost Connection
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Grey			
Status LED	Blinking Red -> Green	Communication on FTE network • Communication via CDA • Unable to establish connection to system time source	CDA	Not Using Configured Timesource
FTE LEDs	Blinking Green			
Display	TS for 1 min. then -> IDLE			
CB icon	Red			
Status LED	Blinking Orange -> Orange	Communication on FTE network • No communication via CDA • Established connection to system time source 850M transitions to secondary redundancy role assuming its partner has CDA available.	SNTP	CDA Comm Lost Connection
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Grey			
Status LED	Green	None. Normal operation for redundant 850M with battery backup following a power cycle.	SNTP	None

850M faceplate		Problem	850M block time source	Station alarm
FTE LEDs	Blinking Green			
Display	IDLE			
CB icon	Blue			

12.7.1.4 Redundant Primary 850M with no memory retention

850M Faceplate		Problem	850M Block Time Source	Station Alarm
Status LED	Blinking Red	No communication on FTE network 850M does not complete startup.	None	• 850M OFFNET When FTE and CDA communication is established: • 850M Not Synchronized • Battery Undervoltage
FTE LEDs	Off			
Display	COMM			
CB icon	Red			
Status LED	Blinking Red -> Blinking Green	Communication on FTE network • No Communication via CDA • Unable to establish connection to system time source	None	850M OFFNET When FTE and CDA communication is established: • 850M Not Synchronized • Battery Undervoltage
FTE LEDs	Blinking Green			
Display	TS for 3 min. then -> NODB			
CB icon	Grey			
Status LED	Blinking Red -> Blinking Green	Communication on FTE network • Communication via CDA • Unable to establish connection to system time source	CDA	850M Not Synchronized
FTE LEDs	Blinking Green			
Display	TS for 1 min. then -> NODB			
CB icon	Red			
Status LED	Blinking Green	Communication on FTE network • No communication via CDA • Established connection to system time source 850M appears to startup normally but Control Builder cannot communicate with the 850M …so attempts to load or reload 850M fail. If 850M was loaded before a power cycle, its associated icons in the Monitor tab will be Red.	SNTP	CDA comm Lost Connection 850M Not Synchronized
FTE LEDs	Blinking Green			
Display	NODB			
CB icon	Grey			
Status LED	Blinking Green	None. Normal operation for redundant primary 850M with no battery backup following a power cycle.	SNTP	850M Not Synchronized

850M Faceplate		Problem	850M Block Time Source	Station Alarm
FTE LEDs	Blinking Green			
Display	NODB			
CB icon	Yellow			

12.7.1.5 Secondary 850M with memory retention

850M faceplate		Problem	850M block time source	Station alarm
Status LED	Blinking Red	No communication on FTE network. 850M does not complete startup.	None	None
FTE LEDs	Off			
Display	COMM			
CB icon	Red			
Status LED	Blinking Red	Communication on FTE network. • No communication via CDA • Unable to establish connection to system time source 850M transitions to primary redundancy role on command of its partner with the possibility that it has a CDA connection.	None	None
FTE LEDs	Blinking Green			
Display	TS -> IDLE			
CB icon	Grey			
Status LED	Blinking Orange -> Orange	Communication on FTE network • Communication via CDA • Unable to establish connection to system time source 850M assumes secondary redundancy role.	CDA	None
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Yellow			
Status LED	Green	Communication on FTE network • No communication via CDA • Established connection to system time source 850M transitions to primary redundancy role on command of its partner with the possibility that it has a CDA connection.	SNTP	• CDA comm Lost Connection
FTE LEDs	Blinking Green			
Display	IDLE			
CB icon	Grey			
Status LED	Blinking Orange -> Orange	None. Normal operation for redundant secondary 850M with battery backup following a power cycle. 850M assumes secondary redundancy role.	SNTP	None
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Yellow			

NOTES

Note 1: Perform the following quick checks: Are the FTE cables properly connected to the 850M's IOTA and the associated CF-9 switches? • Are the FTE cables intact? • Are the connected CF-9 switches powered? • Is the CF-9 switch firmware up-to-date? • Are the CF-9 switches properly configured? If the problem is not identified with these checks, please consult FTE Troubleshooting information and/or contact Honeywell TAC.
Note 2: Perform the following quick checks: • Was **-BP-** displayed for a prolonged period of time during startup? If so, check to make sure that … – The server node on which the Honeywell BootP server is installed, is powered and running. – The Honeywell BootP server is running on the node on which it is installed. • Are the server nodes turned on and properly connected to the network on which the 850M resides? • Are CDA and system services running on the designated nodes?
Note 3: Perform the following quick checks: • Is the timeserver node powered and running? • Is the time service running on the node on which it is installed? • Is the "SNTP Server IP Address" properly configured? – Check the value configured in Control Builder **=> System Preferences => FTE** – Compare this to the value found on the 850M FB Form à System Time Tab when opened from the Monitor Tab in Control Builder or the System Time Tab of the 850M FB Detail Display. • Re-run ntpsetup.exe to ensure that the NTP time source is properly configured.
Note 4: Perform the following quick checks: • Is the Experion node running CDA Server powered and running? • Is the CDA service running on the node on which it is installed

12.7.1.6 Secondary 850M with no memory retention

850M faceplate		Problem	850M block time source	Station alarm
Status LED	Blinking Red	No communication on FTE network.	None	None
FTE LEDs	Off			
Display	COMM			
CB icon	Red			
Status LED	Blinking Orange	Communication on FTE network. • No communication via CDA • Unable to establish connection to system time source	None	None
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Grey			
Status LED	Blinking Orange	Communication on FTE network • Communication via CDA	CDA	C300 Not Synchronized

850M faceplate		Problem	850M block time source	Station alarm
FTE LEDs	Blinking Green	• Unable to establish connection to system time source		
Display	BKUP			
CB icon	Red -> Blue			
Status LED	Blinking Orange	Communication on FTE network • No communication via CDA • Established connection to system time source	SNTP	• CDA comm Lost Connection • C300 Not Synchronized
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Grey			
Status LED	Blinking Orange	None. Normal operation for redundant secondary 850M with no battery backup following a power cycle.	SNTP	850M Not Synchronized
FTE LEDs	Blinking Green			
Display	BKUP			
CB icon	Yellow			

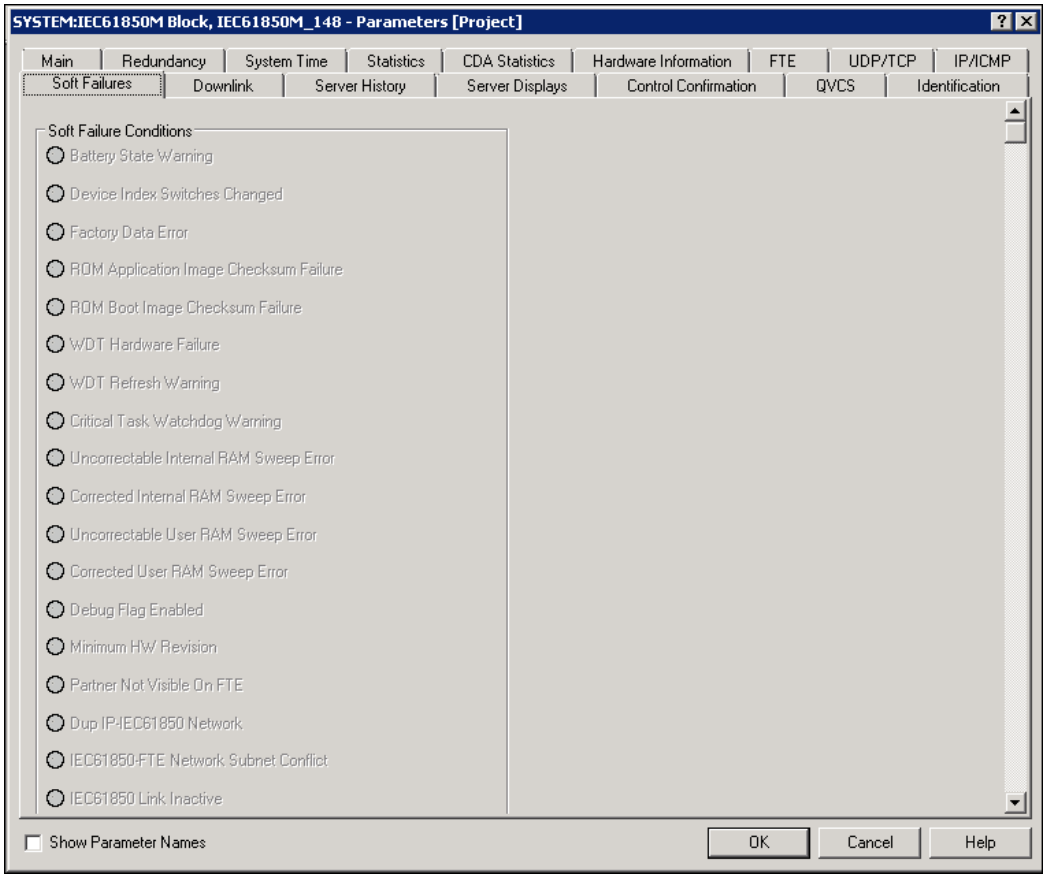
12.8 Communication failures in 850M

This section provides guidance and remedies which may occur during 850M communication.

850M cannot communicate with any other IED

1. In the **Monitoring** tree, double-click the IEC61850M.

   The **Parameters Form** appears.
2. In the *Main* tab, check the values specified for the following fields.
   - **IEC 61850 Network IP Address** : ensure it has the correct IP address.
   - **IEC 61850 Network Mask**: ensure it is correct and in range of the IEDs.
3. Check for the following soft failures on the *Soft Failures* tab.

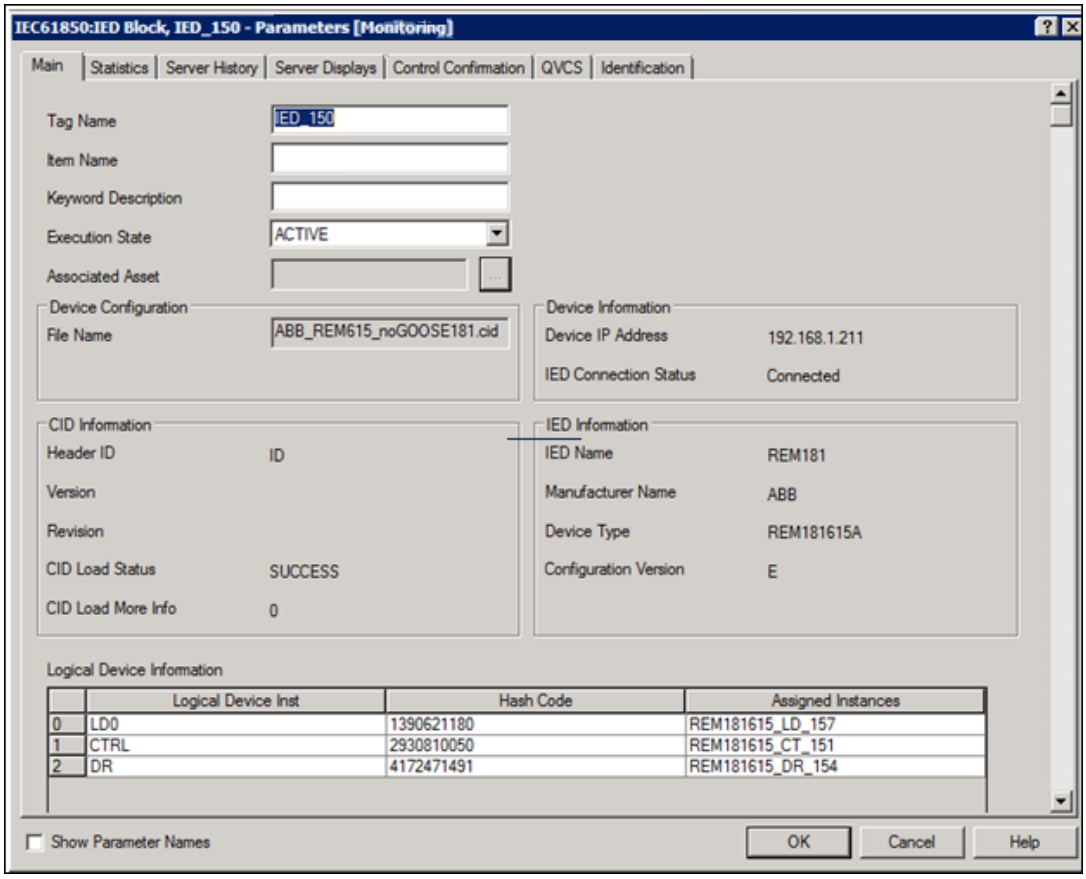


   - **Dup IP-IEC61850 Network**: There is another node on the network with this IP address. Either change the IP address or remove the other node from the network
   - **IEC 61850 – FTE Network Subnet Conflict**: Due to routing issues, the FTE network and the 850M-network are not allowed to be in the same IP address range. Check the FTEs IP address and network mask against the IEC 61850's IP address and mask. Both IP ranges must be on different networks.
   - **IEC 61850 Link Inactive**: Check the network cable between the IEC61850M and the network switch. If that doesn't resolve the issue, then check the network switch's port settings on the port connected to the IEC 61850 uplink.

850M cannot communicate with a single IED

1. In the **Monitoring** tree, double-click the IED icon in the Project tree.

   The **Parameter Configuration** form appears.



2. In the **Main** tab, verify the following fields:
   - In the Device Information section, verify that the **Device IP Address** IP address listed is the same as the IP address of the physical IED.
   - In the IED Information section, verify that the IED information is correct and matches the physical IED.
   - In the CID Information section, verify that the CID load status is SUCCESS. The **CID load More Info** displays an error number if the load of the CID file failed. In a success case this should display **0**. Inform the DEE know if any other value is displayed here.
   - Verify the number of devices making MMS connections to an IED. If MMS connections are limited, it is possible the IED cannot accept another connection.

How to determine the number of IEDs loaded on the 850M

1. In the **Monitoring** tree, double-click the required IEC61850LINK.

   The **IEC61850LINK Block Parameters** form appears.
2. In the **Statistics** tab, in the *IEC 61850 Network* section, the **Total IEDs** field indicates the number of IEDs loaded on the 850M.

Read and write failures (850M to IED)

1. Collect the error code reported in control strategy.
2. Collect 850M and IED communication statistics from Control Builder and from IED local display/ configuration tool.
3. For write failures, ensure that the control model is properly configured in the physical device that match with the Control Builder configuration.

12.9 Gathering information for reporting problems to Honeywell

When an 850M failure occurs, gather information about the 850M and the conditions under which it failed. This information can help the Honeywell Solution Support Center (SSC) in diagnosing and correcting the fault and/or replacing the 850M hardware.

Use this list to obtain information from the 850M and the system so that when you contact Honeywell SSC, a complete description of the problem can be made.

- Use the CTools utility to retrieve internal 850M state information to aid technical personnel in diagnosing the failure. Refer to section, *Using CTools to capture diagnostic data* for the steps to retrieve problem report data for a failed 850M.
- Note the four-digit fail code shown on the 850M's faceplate display.
- Remove and replace the failed 850M. See “Replacing an 850M module and IOTA” on page 124 for details.
- Install the failed 850M in a safe off-process location and start it up.

Obtain the following:

- Hardware revision number of the 850M
- Firmware revision, both the Boot image and Application image
- The Experion System release number in which the 850M was operating

Additional information regarding the operating conditions of the 850M and sequence of events.

- Was the 850M operating in a redundant or non-redundant hardware configuration?
- What was the redundancy state of the 850M at the time of the failure, if redundant?
- Any other status or fail indications on the 850M's faceplate observed at the time of the failure or following the event?
- What were the Control Builder Monitor view indications at the time of the failure or following the event?
- What did the Alarm Status summary show for the time interval around the event?
- Provide a detailed summary of the sequence of events leading up to the failure.
- What operations preceded the event, such as: load, activate, change parameter, delete, synchronization, switchover, and so on.

12.10 Guidelines for requesting support

If you cannot resolve a problem by using this guide, you can request support from your Honeywell Solutions Support Center. When requesting support, please supply as many relevant details about the problem by referring to “Gathering information for reporting problems to Honeywell” to obtain the problem-related information.