GuardLink EtherNet/IP Interface

Catalog Number 432ES-IG3

Allen-Bradley
by ROCKWELL AUTOMATION

Guardmaster®

User Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.

Identifies information that is useful and can help to make a process easier to do or easier to understand.

Table of Contents

Certifications and Directives

Appendix B

Safety Statements

Appendix C

Uninstall the Logix Designer Application Module Profile

Appendix D

Configure Automatic Diagnostics

Appendix E

Notes:

About This Publication

This manual is a reference guide for the 432ES-IG3 EtherNet/IP™ Communications Module for the 432ES-IG3 GuardLink® Network Interface Module.

This publication describes the procedures to install, wire, configure, and troubleshoot the 432ES-IG3 GuardLink network interface module. You must be familiar with the following:

- Use of a safety controller in a Logix 5000® control system.
- Use of safety systems.
- Use of the Studio 5000® Logix and View Designer application environment.
- Knowledge of applicable regulatory standards.

ATTENTION: Personnel who are responsible for the design, application, and maintenance of safety-related programmable electronic systems (PES) must be aware of the safety requirements in the application of the system. Personnel must also be trained in the use of the system.

Who Should Use this Manual

Use this manual to design, install, program, or troubleshoot systems that use the 432ES-IG3 GuardLink EtherNet/IP network interface module.

You are required to have a basic understanding of electrical circuitry and familiarity with safety-related control systems. If you do not, obtain the proper training before using this product.

IMPORTANT	Read and thoroughly understand the manual before installing or operating a system that contains this device.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Updated Guard Locking section.	18

Definitions

The Industrial Automation Glossary (publication AG-7.1) contains terms and abbreviations that Rockwell Automation uses to describe industrial automation systems. The following table lists specific terms and abbreviations that are used in this manual.

Table 1 - Terms and Abbreviations

Term	Description
AOP	Add-on Profile - A Logix Designer application file that facilitates the implementation of the 432ES. This term is also known as the module profile.
CIP	Common Industrial Protocol - An industrial communication protocol that Logix 5000-based automation systems use on Ethernet, ControlNet®, and DeviceNet® communication networks.
CIP Safety™	Safety certified version of CIP™.
CIP Security™	Helps CIP connected device protect itself from malicious CIP communications.
CIP Sync™	Synchronizes the timing of events.
Client	The client is a GuardLink-enabled device that connects into one of the GuardLink circuit channels of the 432ES-IG3 network interface module. Each client is a node.
DHCP	Dynamic Host Configuration Protocol - A network management protocol that Internet Protocol networks use to assign an IP address and other network configuration parameters to each device on a network dynamically.
FW	Firmware revision level.
GuardLink circuit	Includes all hardware that connects to one channel of the 432ES. This hardware includes the cables, taps, safety devices, and the terminator.
HI	The on-state of the output of a logic block, or the state of an input to a logic block, or a voltage level that is above the turn-on threshold. HI is equal to a Boolean value of 1.
HMI	Human Machine Interface - A Rockwell Automation® product in the PanelView™ family.
Host	The host is the 432ES-IG3 network interface module.
HW	Hardware revision level.
LO	Logic off-state or a voltage level below the turn-off threshold. LO is equivalent to a Boolean value of 0.
MAC ID	Media Access Control Identification Number - An Ethernet device on a network is assigned a unique physical (hardware) number. This number must associate with the IP address that is assigned to the device for proper communication.
NC	No connection.
Node	A GuardLink-enabled device that is installed in a GuardLink circuit. Up to 32 nodes can connect to a circuit. The nodes are numbered from 0 to 31.
Operational state	All nodes on the GuardLink channel are safety valid, and the safety Status tag for the channel is set to a value of 1.
OSSD	Output Signal Switching Device - Typically, OSSD is a pair of solid-state signals that are connected to a DC source supply. The signals are tested for short circuits to the DC power supply, to the DC common, and between the two signals. The 432ES-IG3 network interface module does not have OSSD outputs because the safety status is transmitted over the Ethernet network. In the controller input tags, the SIL 3 rated signal for the safety output on each channel is called Status.
PFHd (PFH)	The probability of failure to danger per hour. When IEC 61508 is applied, the acronym PFH implies the probability of failure to danger.
PLC (PAC)	A programmable logic controller or a programmable automation controller.
Reaction time	The input reaction time is the time from when the signal changes on an input terminal to when safety data is sent to the GuardLogix® controller.
Response time	Describes the time between the initial demand that is placed on a safety device/system, to the time when its output changes to a safe state.
Safe state	One or more nodes on the GuardLink channel are not safety valid, and the safety Status tag for the channel is set to a value of 0.
Safety valid	The safety circuit receives input signals that satisfy its requirements to allow transition to an operational state.
Tap	A tap connects a safety device to the GuardLink circuit. GuardLink-enabled taps are nodes on the GuardLink circuit. Passive taps are not GuardLink-enabled and therefore must connect to a GuardLink-enabled device to be considered as a node on the GuardLink circuit. A tap is not considered as a node when the tap is a passive or passive power tap with a shorting plug.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
ControlLogix System Selection Guide, publication 1756-SG001	Provides information to help you select a ControlLogix® system.
ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information to help you design a system, operate a ControlLogix or GuardLogix-based controller system, and develop applications.
Guardmaster DG Safety Relay and GuardLink System User Manual, publication 440R-UM015	Provides a detailed description of the GuardLink system when connected to the Guardmaster® DG safety relay.
GuardLink EtherNet/IP Network Interface Installation Instructions, publication 432ES-IN001	Describes how to install a 432ES-IG3 network interface module.
ControlFLASH Plus Quick Start Guide, publication CFP-QS001	Describes how to use the ControlFLASH Plus™ software to upgrade device firmware.
EtherNet/IP Network Devices User Manual, publication ENET-UM006	Describes how to configure and use EtherNet/IP devices to communicate on the EtherNet/IP network.
Ethernet Reference Manual, publication ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
Ethernet Media Specifications Technical Data, publication 1585-TD001	Provides technical specifications for Ethernet media cables and accessories.
System Security Design Guidelines Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.
Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley® industrial automation controls and assemblies.
Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at rok.auto/literature.

Notes:

Introduction

Overview

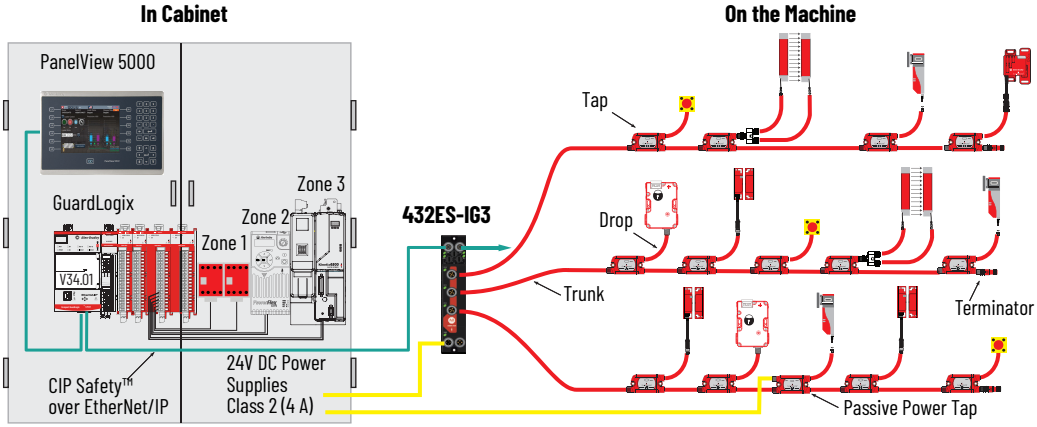
A GuardLink® system is a collection of components to simplify a series connection of safety devices while achieving the highest industrial safety rating. The system has these important features:

- Simplifies the connection of series connected safety devices.
- Facilitates the scalability of the safety series connections.
- Provides diagnostic information about each device in the system without having to run a separate status wire back to the machine control system.
- Allows the simultaneous or individual lock/unlock of guard locking interlocks in the series-connected system. No need for an additional wire from the machine control system to lock/unlock the safety gate.
- Helps ease communication to the machine control system over EtherNet/IP™. Communication includes the sending of non-safety commands to devices and the receiving of status information back from the safety devices.

The following image shows a typical safety system that uses the 432ES-IG3 network interface module. A typical system consists of an HMI, a GuardLogix® controller, the 432ES-IG3 GuardLink EtherNet/IP network interface module, and a series connection of safety devices, which connect to the interface through taps in a trunk and drop network configuration.

The GuardLogix controller and PanelView™ reside in an environmentally protected control cabinet. The 432ES network interface module and associated taps and devices are at various points on the machine.

Figure 1 - Typical 432ES-IG3 Network Interface Module Safety System



The 432ES-IG3 network interface module can control up to three safety zones, one zone for each GuardLink channel. With logic, the channels can combine to control only one or two zones.

Requirements

A GuardLogix controller must control the 432ES-IG3 network interface module. See the ControlLogix System Selection Guide, publication 1756-SG001. As of the time of release, you can use the following controllers:

- 1756 GuardLogix 5580 controllers
- 5069 Compact GuardLogix 5380 controllers

The controller must run Studio 5000® version 34.01 or later. You must use FactoryTalk® Linx 6.30 or later for communications. A PanelView 5000 HMI is required for automatic diagnostic reporting. PanelView Performance Plus can be used with FactoryTalk SE; setup is not automatic.

The 432ES-IG3 network interface module provides additional status information and the ability to upgrade the firmware in GuardLink-enabled devices. To achieve this functionality, the firmware in the taps and guard locking switch is upgraded to 2.00x. The 432ES-IG3 network interface module can operate with firmware 1.00x, but 2.00x is the preferred level. When multiple levels of protocol connect on a channel, the channel operates at the lowest level.

IMPORTANT
- Channels 0 and 1 can operate with GuardLink 1.0 or 2.0. If nodes are mixed, the channel operates at 1.0.
- Channel 2 can only operate with GuardLink 2.0 devices.

Automatic Diagnostics

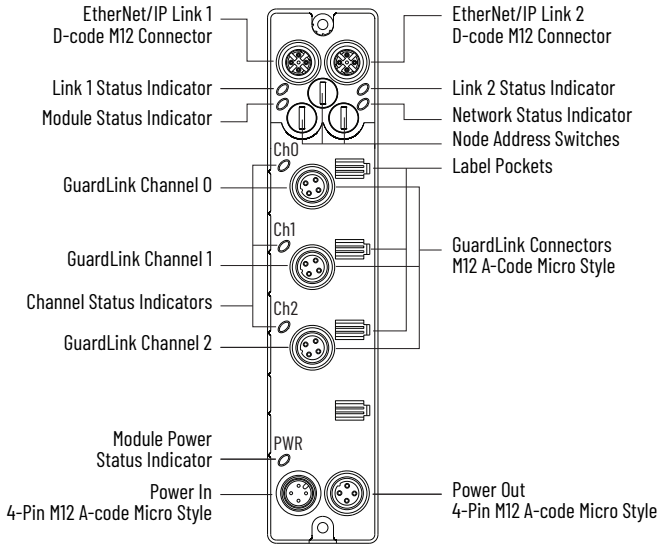
Automatic diagnostics is a system-level feature in devices that provides device diagnostics to HMIs and other clients, with zero programming. GuardLink 2.0 products come with the automatic diagnostics feature enabled by default, so diagnostics - including device description conditions and state events - are sent to an HMI device.

You can deactivate and activate the whole feature while online or offline from the Controller Properties dialog box. You can also deactivate automatic diagnostics for a specific device in the module properties. See Configure Automatic Diagnostics on page 87 for more information.

Physical Features

The following image identifies the key physical features of the 432ES-IG3 network interface module. Connections for the GuardLink channels, the Ethernet ports, and the power connections are all M12 quick disconnect cables to reduce installation and troubleshooting costs. Status indicators use color and blink rates to provide status and diagnostic information.

Figure 2 - 432ES Network Interface Module Key Features



Modes of Operation

The GuardLink system has four modes of operation for each channel:

- Start Up - Initializes the system when power is initially applied. The 432ES network interface module determines the number of channels in use, and the number and type of nodes on each channel.
- Operational - All safety devices on the GuardLink channel are safety-valid.
- Safe State - One or more of the devices on the GuardLink channel are not safety-valid.
- Firmware Update - The 432ES network interface module or one of its client devices is undergoing a firmware update. Updates can only occur when the system is in the safe state.

The 432ES network interface module has three independent channels. Any channel can be in the operational state, while the others can be in a safe state. The 432ES-IG3 network interface module has one safety-rated controller Status tag for each channel.

In the operational state, the 432ES network interface module transmits the channel Status = 1 to the safety controller, which indicates the channel is in an operating state. The machine must use the Status tag as part of the safety function to allow the machine to enter Run mode.

In the safe state, the 432ES network interface module transmits the channel Status = 0 to the safety controller, which indicates the channel is operating in a safe state; one or more safety devices are actuated (not valid).

System Design

GuardLink Components

Each GuardLink circuit accommodates up to 32 taps.

A typical GuardLink system consists of:

- One GuardLink interface
- One tap for each safety device
- One terminator for each GuardLink circuit
- Patchcords and cordsets

Taps

Taps create nodes in the GuardLink circuit. A safety device connects to each tap. The following types of taps are available:

- GuardLink-enabled taps that interface with devices that have voltage-free safety contacts
- GuardLink-enabled taps that interface with devices that have OSSD signals
- GuardLink-enabled 8-pin taps can be either Power to Release or Power to Lock
- Passive taps that interface with devices that are GuardLink-enabled
- Passive power taps that interface with devices that are GuardLink-enabled and add power to the link

GuardLink-enabled taps are available in an 8-pin and 5-pin device connection version. Passive style taps are only available in a 5-pin device connection version.

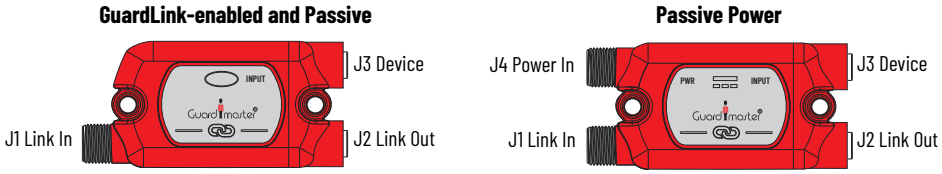
The taps are intended to mount on the machine, near the location of the device the tap monitors. You can mix and connect the different tap types and versions in any order.

Tap Type	Description
OSSD Tap	The OSSD tap is designed to specifically interface with safety products that generate OSSD outputs. The OSSD tap does not perform testing on the OSSD signals as the input device must perform the test. The OSSD tap verifies if the outputs of the connected device are energized or de-energized. If the outputs are de-energized, then the tap goes to a safe state, and the input status indicator is red. If the outputs of the device are energized, then the tap shows a solid or flashing green input status indicator. If the OSSD tap inputs are not the same state for 3 or more seconds, then the tap enters a recoverable fault state. Both inputs must go to LO and then back to HI to recover. The 8-pin OSSD taps are available in Power to Release and Power to Lock versions for guard locking switches.
EMSS Tap	The EMSS tap is designed to interface with two voltage-free contacts. The tap applies 24V to one side of the contact on both channels and looks for the 24V on the monitoring input. The tap pulse tests these contacts. The tap verifies if both contacts are closed or open. When the contacts open, the tap goes to a safe state, and the input status indicator is red. When the contacts close, the tap goes to an operational state, which turns the input status indicator either solid or flashing green. The EMSS tap has a 10 second simultaneity window. If one contact opens, the second contact must open within 10 seconds. Similarly, if one contact closes, the second contact must close within 10 seconds. If the simultaneity window requirement is not met, the tap goes to a recoverable fault state. To recover, both contacts must cycle open and then closed again within 10 seconds. The 8-pin EMSS taps are available in Power to Release and Power to Lock versions for guard locking switches.
Passive Tap	The passive tap is designed to interface with safety-rated devices that have built-in GuardLink technology. The passive tap simply passes the GuardLink signals to and from the device. The passive tap does not operate with safety devices that have OSSD or EMSS outputs.
Passive Power Tap	The passive power tap has two significant features: • The passive power tap acts as a passive tap by passing the GuardLink signals directly to devices with built-in GuardLink technology • The passive power tap allows additional power to be introduced into the GuardLink circuit to compensate for voltage drops resulting from long cable lengths and numerous devices in the circuit.

Tap Connections

The following image identifies the tap connections. Follow the instructions to modify the GuardLink circuit. The Link In (J1) connection supplies power to the tap.

Figure 3 - Tap Connections



Tap Cabling

The GuardLink system is designed to minimize wiring with quick-disconnect patchcords, while also allowing some manual wiring to terminals, when pinout incompatibilities exist.

The preferred cables are the Bulletin 889D hardware (red jacket, PVC, unshielded, with epoxy coat). Use any jacket color, however, the red is the preferred color to indicate a safety circuit. To minimize the voltage drop due to wire resistance, the preferred wiring gauge for the link cable is 18 AWG (0.823 mm^2).

Visit rockwellautomation.com/en-us/products/hardware/allen-bradley/connection-devices/cables-and-cordsets/dc-micro--m12-/dc-micro-cordsets-and-patchcords.html for other options, such as right-angle connectors, stainless-steel couplings, and shielded cables.

To maintain the integrity of the GuardLink signal, the wiring distance between GuardLink-enabled devices is important. There are two application cases:

- Case 1: Includes Guard Locking Devices on page 15
- Case 2: No Guard Locking Devices on page 15

For both cases, the wiring distance between the taps and the safety device is limited to 10 m (32.8 ft). Proper wiring requires at least 22 AWG (0.33 mm^2) wire size for 5-conductor cables and for 8-conductor cables.

Case 1: Includes Guard Locking Devices

When the GuardLink circuit includes one or more guard locking devices, the maximum distance between GuardLink-enabled devices is 30 m (98.4 ft). If the distance between devices is greater than 30 m (98.4 ft), you must insert a GuardLink-enabled tap at a maximum of every 30 m (98.4 ft). If a device is not needed at a particular location, use a shorting plug for the device connection.

The following image shows an example GuardLink circuit that includes at least one guard locking device.

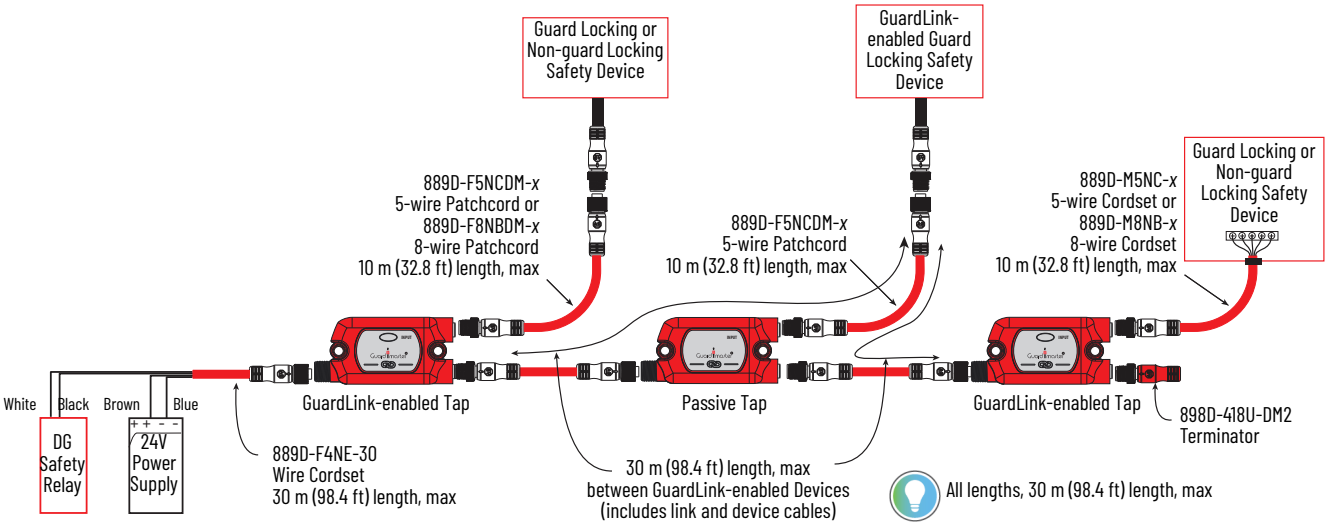
Tap 1 is a GuardLink-enabled tap that can be connected to a guard locking or a non-guard locking device.

Tap 2 is a passive tap, which is connected to a GuardLink-enabled device.

The following image also shows tap 3 as a safety device with terminal block connections. In this case, a cordset is used to connect the safety device to the tap. The safety device can be a guard locking or non-guard locking device.

Because the GuardLink circuit has at least one guard locking switch, the maximum distance between GuardLink-enabled devices is 30 m (98.4 ft). When a passive tap is used, the cable length includes both the length of the link cable and the length of the device cable.

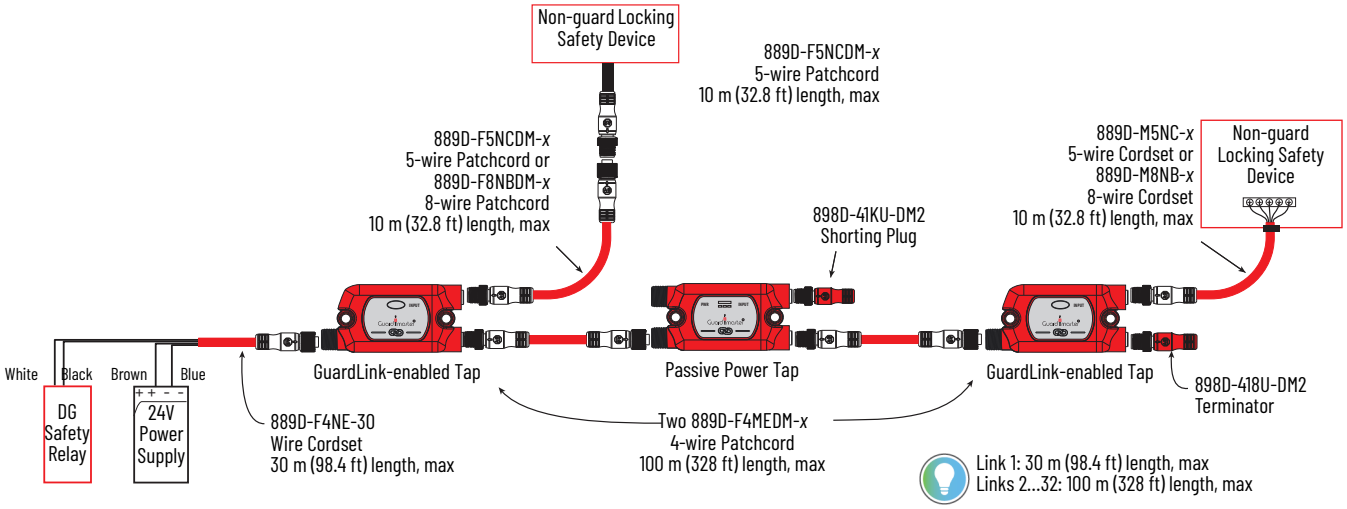
Figure 4 - Example Guard Locking Circuit



Case 2: No Guard Locking Devices

The following image shows an example of a GuardLink circuit with no guard locking devices. When the GuardLink circuit excludes any guard locking devices, the maximum distance between 2...32 GuardLink-enabled devices is 100 m (328.1 ft). The distance from the DG safety relay or the 432ES-IG3 network interface to the first tap is limited to 30 m (98.4 ft). If a passive power tap is used with a shorting plug, the total length between the two neighboring GuardLink-enabled taps is 100 m (328.1 ft).

Figure 5 - Example of a Non-guard Locking Circuit



Tap Replacement

You can replace a GuardLink tap with the same type of tap while the link is powered. When the connections are remade, the GuardLink circuit recovers automatically.

When a GuardLink tap is replaced with another type of tap that is removed or added to the circuit, cycle the power to the DG safety relay to relearn the number and types of connected taps. If you use the 440R-ENETR interface, cycle its power and update the Add-on Profile (AOP) of the interface.

For applications with the 432ES network interface, momentarily remove a link cable to cycle the power to the channel, or cycle the power to the 432ES network interface. The 432ES network interface AOP must also be updated.

Channel Order

Each channel acts independently. You can add the nodes to any channel in any order. For example, it is not necessary to add nodes to Channel 0 first. You can add to Channel 1 or Channel 2 first.

Each channel can accommodate up to 32 nodes, numbered 0...31. The nodes must be sequential with no skipping over numbers.

You can either add the hardware, then add the nodes into the Controller Organizer (software), or vice versa. We recommend that you add the hardware before you change the controller tree. This order allows the Discover Modules feature to add the nodes to the Controller Organizer quickly, in the correct order, with the correct part number, and compatible electronic keying.

- Channels 0 and 1 can accommodate protocols 2.0 and 1.0.
- When multiple levels of protocol connect on a channel, the channel operates at the lowest level. Protocol 1.0 provides basic on/off information, with limited diagnostics. Protocol 2.0 provides on/off, additional diagnostic information, and firmware updates.
- Channel 2 only operates with GuardLink 2.0 devices. If a GuardLink 1.0 device (Series A tap or Series A 440G-MZ) is installed on Channel 2, all nodes on Channel 2 show a fault condition with the message, "(Code 16#0312) Connection Request Error: Invalid link address."

Terminator

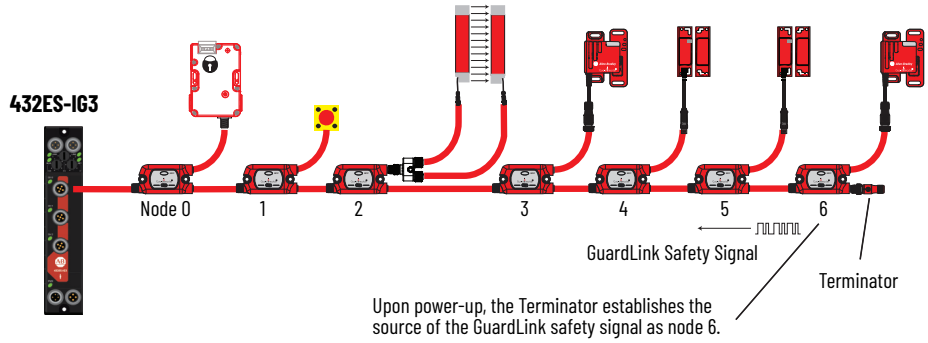
The terminator plays a key role in the GuardLink system. To understand the role of the terminator helps you to understand the modifications you can apply to the GuardLink circuit, such as how to change tap types, insert nodes, delete nodes, and append nodes.

The terminator must be installed on the J2 connector of the last tap to complete the link connection. The terminator contains internal electrical components specifically for a GuardLink system; other terminators cannot be used as substitutes.

Figure 6 - Terminator (Catalog Number 898D-418U-DM2)

The following image shows an example GuardLink circuit. When power is applied to the GuardLink circuit, components in the terminator set a specific reference voltage. The device, which connects to the terminator, reads this voltage and determines that it is the last device. The last device is the safety source, as it initiates the GuardLink safety signal. Upon initiation, the GuardLink safety signal determines the number of devices and the identity of the devices in the circuit. After initiation, the GuardLink signal monitors all devices for their safety status.

Figure 7 - Terminator Determines the Source of the GuardLink Safety Signal



The terminator affects the closest GuardLink-enabled device. As of the date of this publication, the device can be a Smart Tap or a 440G-MZ guard locking switch. Additional GuardLink-enabled devices will be available in the future.

After the initial power-up and establishment of the GuardLink circuit, the terminator plays no role. You can remove the GuardLink circuit with no effect on the system, though this action causes the next power cycle to result in a faulted state.

A new GuardLink configuration does not generate if you move the terminator without a power cycle. Modifications to the GuardLink circuit are only realized upon power-up with the terminator in place. For a simple power-up, break the link signal at any point in the circuit before the device that last had the terminator.

The terminator is also an important tool when you commission a new system, troubleshoot an existing system, or make topology changes.

To help troubleshoot a GuardLink system, reduce the number of taps in the GuardLink circuit by relocating the terminator. After relocation, cycle power to the DG safety relay to allow it to relearn how many taps are connected. If a 440R-ENETR interface is used, then you must cycle the power to it and update the AOP of the interface.

For applications with the 432ES network interface, momentarily remove a link cable to cycle the power to the channel, or cycle the power to the 432ES network interface. The 432ES network interface AOP must also be updated.

Commissioning Example

For example, the system requires 15 nodes. During commissioning, connect five nodes at a time, rather than connecting all 15 at once. After moving the terminator, cycle power to the tap or switch from where the terminator is removed. Reapply power to the channel after you install the terminator in its new location.

Guard Locking

The international standard ISO 14119, most recently updated in 2013, provides requirements for the application of interlock safety devices.

When guard locking devices are applied, the opening of the guards must be prevented until all hazards have reached a safe state. This configuration requires proper design of the Unlock function, which consists of two different types:

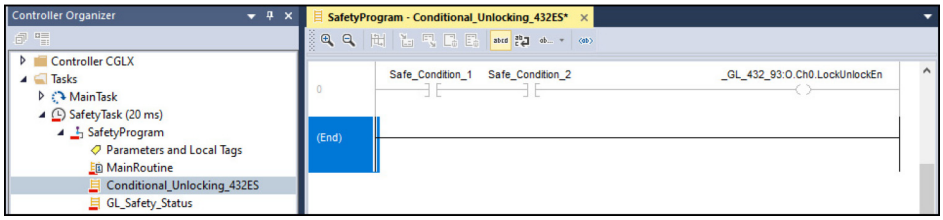
- Unconditional Unlocking - The Unlock command can be issued at any time, regardless of the state of the machine. In this scenario, the guard locking switch unlocks the safety gate and generates a stop command. The safety distance calculation timing begins immediately when the switch unlocks. The machine must be designed such that the operator cannot reach the hazard until it is in a safe state.
- Conditional Unlocking - The unlock command can only be issued after the hazard has reached a safe state. The conditions for unlocking can be based on the time when the stopping performance of the hazard is known and consistent, or other conditions may exist, like required tolerances of pressure, temperature, atmospheric conditions, speed, or other criteria. If there is variability in the hazard stopping performance, then monitoring for a safe state may be required before the unlock command can be issued.

In some applications, the risk assessment may determine that the safety rating of the guard unlocking function is lower than the safety rating of the guard monitoring function. For example, the guard monitoring function may require a SIL3/PLe rating, whereas the unlocking function may only require a SIL2/PLd rating. This is justified when the existing guards limit the operator's exposure to the hazard or increase the probability of avoiding the hazard.

Firmware 3.001 adds a safety-rated Lock/Unlock Enable controller tag. This tag is labeled LockUnlockEn. You can use logic to confirm safe conditions before enabling the lock and unlock commands to be sent to client devices. The conditions must be tested in the safety task.

The following image shows two (redundant) input conditions in the Safety Task are required to enable unlock and lock commands to be sent to clients on Channel 0. If either condition is not satisfied, lock and unlock commands cannot be sent to the client devices. Each channel has an enable output tag.

Figure 8 - Conditional Unlocking Example



When conditional locking/unlocking is required, the lock/unlock event requires two tags to be set:

- The LockUnlockEn in the safety task
- The Lock or Unlock tag for the client in the main task.

The sequence of setting the tags is interchangeable. You can first set the unlock or lock tags to the individual clients and then set the LockUnlockEn tag to execute the unlock or lock commands or vice versa. From a functional safety perspective, all guard locking devices connected to one of the three GuardLink channels must be considered as unlocked if one guard locking device is commanded to unlock. No individual guard locking/unlocking is achievable within one GuardLink channel from a functional safety perspective.

IMPORTANT	When the LockUnlockEn tag is set to 1, the channel immediately transitions to a safe state.

If only unconditional locking/unlocking is needed, then the safety rated Lock/UnlockEn tags can be hidden (not used) by setting the Output Data selection in the Module Definition to None. When None is selected, firmware 3.001 is backward compatible with firmware 2.001 and 1.001 regarding the locking function.

Notes:

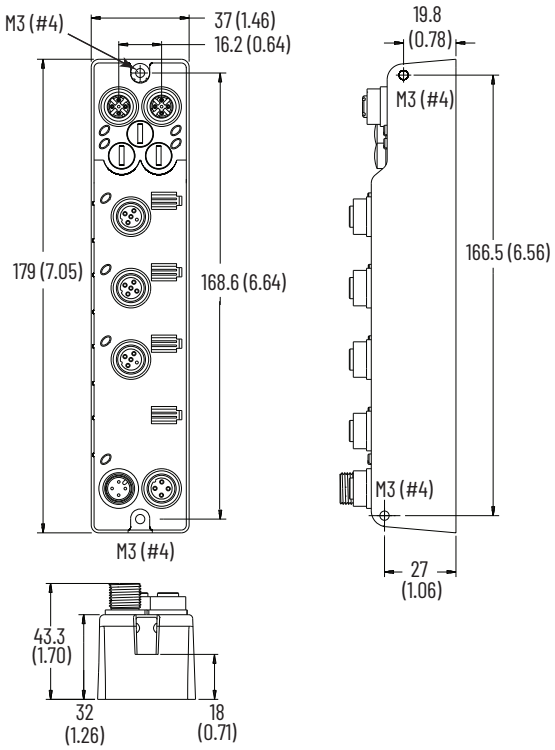
Mechanical Installation

Approximate Dimensions

The following image shows the body and mounting dimension of the 432ES network interface module. Two sets of mounting holes allow you to mount the module directly to a panel, or to the front or side of the machine.

Mounting holes accommodate M3 (#4) pan head screws. Torque to 0.68 N•m (6 lb•in).

Figure 9 - Approximate Dimensions [mm (in.)]

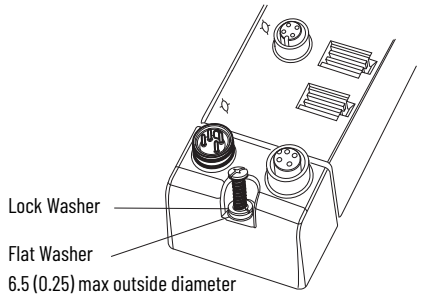


High Vibration Areas

The following image shows the recommended mounting if the module is in an area that is subject to shock or vibration.

Use a flat and lock washer; mount the flat washer underneath the lock washer. Torque the mounting screws to 0.68 N•m (6 lb•in).

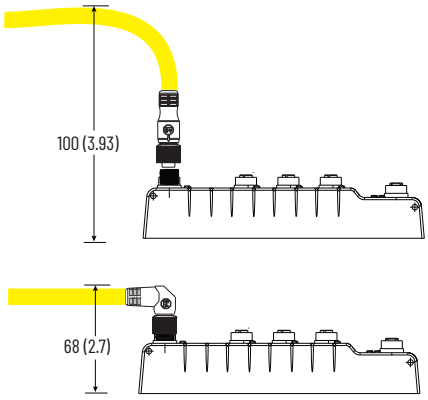
Figure 10 - High Vibration Mounting [mm (in.)]



Cable Clearance

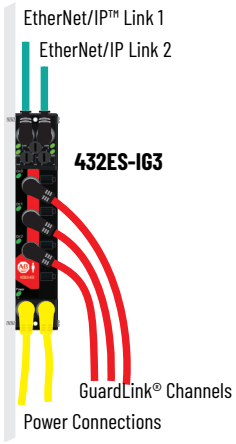
The 432ES-IG3 network interface module can accommodate both straight and right-angle connectors. The following image shows the typical vertical cable clearance for the straight and right-angle connectors.

Figure 11 - Cable Clearance [mm (in.)]



The following image shows an example of the 432ES-IG3 network interface module that is mounted against a side wall with all cables using right-angle quick-disconnect connectors.

Figure 12 - Side Mounting with Right-angle Connectors



Electrical Connections

Wiring

ATTENTION: Before you install and wire any device, disconnect power to the system. Calculate the maximum current in each power and common wire. Observe all electrical codes that dictate the maximum current allowable for each wire size. Current above the maximum ratings can cause wiring to overheat, which can cause damage.

Do not run signal or communications wiring and power wiring in the same conduit. Route wires with different signal characteristics by separate paths.

Separate wiring with signal type. Bundle wiring with similar electrical characteristics together.

Label wiring to all devices in the system. Use tape, shrink-tubing, or other means to label wires. Also use colored insulation to identify wires based on signal characteristics. For example, you can use blue for DC wiring and red for AC wiring.

IMPORTANT Fault exclusions for conductors and wiring must follow the requirements of EN ISO 13849-2, table D.3 and D.4. A fault exclusion can reduce the overall safety rating of the related safety function to a maximum of PLd per EN ISO 13849-1.

The following image identifies the connectors and the following tables list the connections for the pins.

Figure 13 - Pin Assignments

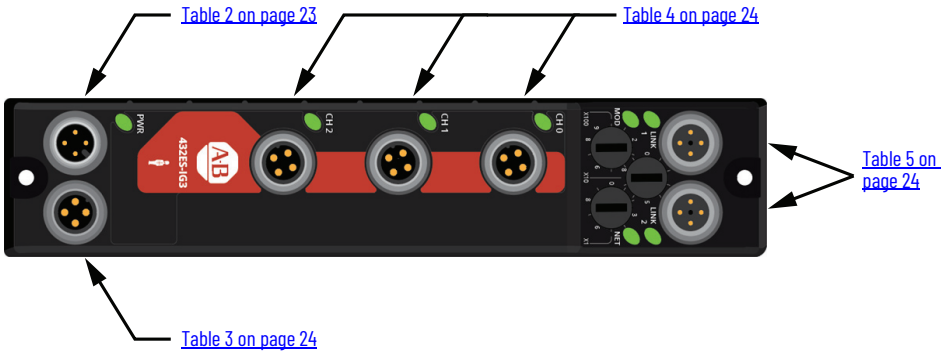


Table 2 - Power In

4-pin A-code Micro (M12) Convex	Pin	Description
	1	Output power +24V DC
	2	Module power +24V DC
	3	Module power 0V
	4	Output power 0V

Recommended cordset catalog numbers:
- 889D-F4AE-x (1) - Straight concave, no connector
- 889D-R4AE-x (1) - Right-angle concave, no connector

(1) x = 2 [2 m (6.6 ft)], 5 [5 m (16.4 ft)], 10 [10 m (32.8 ft)], 15 [15 m (49.21 ft)], 20 [20 m (65.62 ft)], or 30 [30 m (98.42 ft)] for standard cable lengths. For other cable lengths, contact your local Allen-Bradley distributor or Rockwell Automation sales office.

Table 3 - Power Out

4-pin A-code Micro (M12) Concave	Pin	Description
	1	Output power +24V DC
	2	Module power +24V DC
	3	Module power 0V
	4	Output power 0V

Recommended patchcords catalog numbers:
- 889D-F4AEDM-*x* (1) - Straight concave, straight convex connector
- 889D-R4AEDE-*x* (1) - Right-angle concave, right-angle convex connector

(1) *x* = 0M3, 0M6, 1 [1 m (3.28 ft)], 2 [2 m (6.6 ft)], 5 [5 m (16.4 ft)], 10 [10 m (32.8 ft)], 15 [15 m (49.21 ft)], 20 [20 m (65.62 ft)], or 30 [30 m (98.42 ft)] for standard cable lengths. For other cable lengths, contact your local Allen-Bradley distributor or Rockwell Automation sales office.

Table 4 - GuardLink Channels

4-pin A-code Micro (M12) Concave	Pin	Description
	1	24V DC
	2	GuardLink® safety signal
	3	0V
	4	CLU (control lock unlock)

Recommended patchcords catalog numbers:
- 889D-F4NEDM-*x* (1) - Straight concave, straight convex connector
- 889D-R4AEDE-*x* (1) - Right-angle concave, right-angle convex connector

(1) *x* = 0M3, 0M6, 1 [1 m (3.28 ft)], 2 [2 m (6.6 ft)], 5 [5 m (16.4 ft)], 10 [10 m (32.8 ft)], 15 [15 m (49.21 ft)], 20 [20 m (65.62 ft)], or 30 [30 m (98.42 ft)] for standard cable lengths. For other cable lengths, contact your local Allen-Bradley distributor or Rockwell Automation sales office.

Table 5 - EtherNet/IP Ports

4-pin D-code Micro Concave	Pin	Description
	1	Tx Data+
	2	Rx Data+
	3	Tx-
	4	Rx-

Recommended Ethernet cables catalog numbers:
- 1585D-M4UBJM-*x* (1) - Straight convex, RJ45 straight convex connector
- 1585D-E4UBJM-*x* (1) - Right-angle convex, RJ45 straight convex connector
- 1585D-E4UBDE-*x* (1) - Right-angle convex, M12 right-angle convex connector
- 1585D-M4UBDM-*x* (1) - Straight convex, M12, straight convex connector

(1) *x* = 0M15, 0M2, 0M3, 0M6, 1 [1 m (3.28 ft)], 2 [2 m (6.6 ft)], 2M5, 3 [3 m (9.84 ft)], 4 [4 m (13.12 ft)], 5 [5 m (16.4 ft)], 10 [10 m (32.8 ft)], 15 [15 m (49.21 ft)], 20 [20 m (65.62 ft)], 30 [30 m (98.42 ft)], or 40 [40 m (131.23 ft)] for standard cable lengths. For other cable lengths, contact your local Allen-Bradley distributor or Rockwell Automation sales office.

Power Supply

An external 24V DC power supply source provides power for the 432ES-IG3 network interface module block. To comply with the European Low Voltage Directive (LVD), power must come from a protected extra low voltage (PELV) DC source.

To comply with UL restrictions, power must come from DC sources that has double insulation or reinforced insulation to isolate the secondary circuits from the primary circuit. The DC power supply must satisfy the requirements for the National Electric Code (NEC) Class 2 and ground to protective earth.

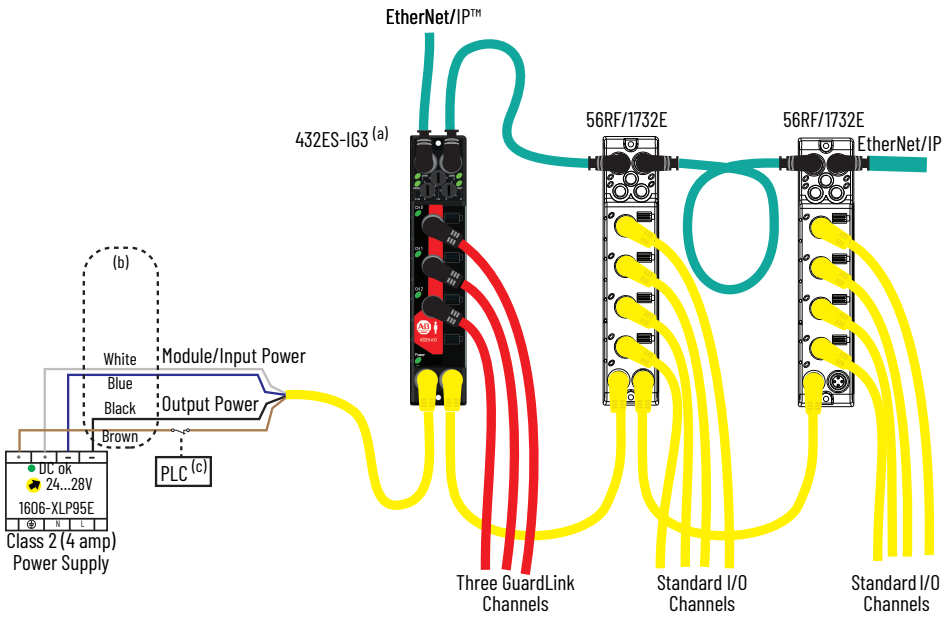
Many of our Bulletin 1606 power supplies are both PELV and NEC Class 2 compliant. The following is a list of compliant power supplies:

- Power supply 1606-XLP30E
- Power supply 1606-XLP50E
- Power supply 1606-XLP50EZ
- Power supply 1606-XLP72E
- Power supply 1606-XLP95E
- 1694 modular electronic circuit protector
- On-machine power supply 1607-XT100D1B

The 432ES-IG3 network interface module has isolated module and output power connections. Both power connections are daisy chained to similar blocks (for example, 56RF and 1732E). This feature allows you to turn output power off, while maintaining module/input power. You can turn output power off to commission and troubleshoot to help prevent inadvertent actuation of output devices.

The 432ES-IG3 network interface module does not use output power. The output power solely passes from the power-in to the power-out connector. The following image shows an example of how the connections work.

Figure 14 - Module/Output Power Daisy Chain



(a) Does not use output power.
(b) Typical Bulletin 889D DC micro cordset wire colors
(c) PLC can turn off output power while still being able to monitor input devices.

Multiple Power Supplies

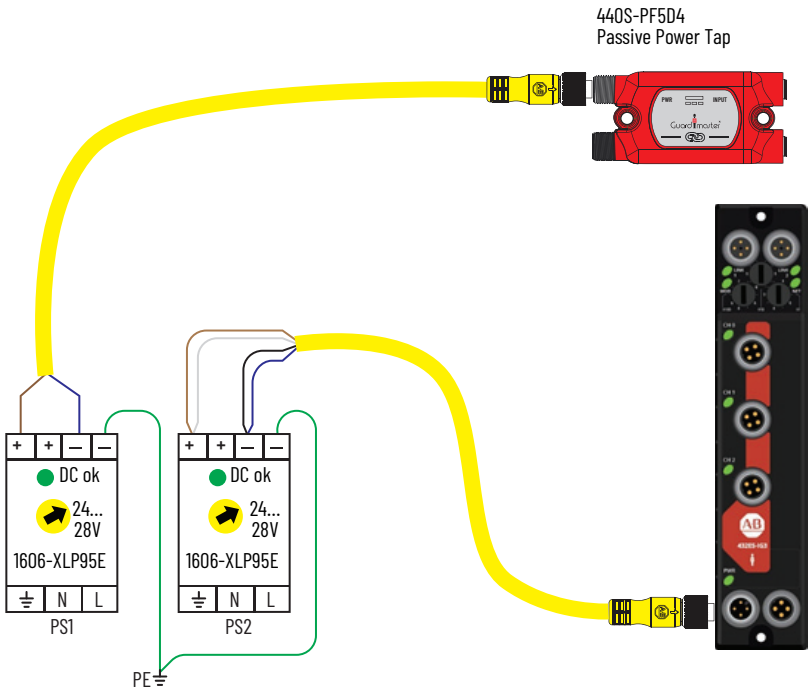
Depending on the number of devices and the cable lengths, the GuardLink circuit can require additional power to maintain the voltage at an appropriate value. Add power to a GuardLink channel with the 440S-PF5D4 passive power tap (seven taps max per channel).

When you use multiple power supplies, you can turn on the power supplies simultaneously, or turn on the power supplies sequentially. To turn on power supplies in sequential, begin with the 432ES-IG3 network interface module and end with the terminator.

The 24V common of all power supplies must connect together. In addition, the 24V common must connect to protective earth (PE) ground to be PELV-compliant. The 24V common connections must be at one joint location to avoid ground loop circuits.

You can use the 1607-XT100D1B on-machine power supply in GuardLink applications. The power supply has a 96...264 AC input and supplies a 24V DC supply, which meets NEC Class 2 with an earth grounded 0V terminal.

Figure 15 - Multiple Power Supplies



Add the Network Interface Module

To add the 432ES-IG3 network interface module in your GuardLink® system, follow the steps that are explained in this chapter.

1. Set the IP Address.
2. Download and install the firmware from rok.auto/pcdc.
3. Update Firmware on page 28.
4. Install the Profile on page 31.
5. Add the Network Interface Module to a Controller Project on page 32.
6. Append GuardLink Nodes on page 44.

Download the network interface module firmware and profile (AOP) files from rok.auto/pcdc.

Search 432 and select Downloads to access the network interface module profile.

Set the IP Address

Before you can connect to the controller through the Ethernet or USB port, configure the EtherNet/IP™ in Linx-based software on your workstation.

For more information on how to install communication drivers, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

When the network interface module is in the out-of-the-box state, the following apply regarding IP addresses:

- The network interface module ships without an IP address.
- The network interface module is DHCP-enabled. That is, the network interface module is configured to obtain an IP address via a DHCP server.

If there is no DHCP server or the DHCP server is not configured to set the IP address, you must set the IP address with the three IP address switches marked X1, X10, and X100. The IP address becomes 192.168.1.X1 X10 X100.

Requirements

To set the IP address, obtain the following:

- EtherNet/IP driver installed on the programming workstation
- MAC ID from the device, which is on the label on the side of the device
- Recommended IP address for the device

Alternative Methods to Set the IP Address

The network interface module supports the following methods to change the IP address:

- EtherNet/IP Address Commissioning Tool
- BOOTP/DHCP utility
- FactoryTalk® Linx 6.30 or later software
- Studio 5000 Logix Designer® application

For more information on how to use these methods, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

Update Firmware

Use ControlFLASH Plus™ software to update the firmware. For information on how to download, install, and use ControlFLASH Plus software, see the ControlFLASH Plus Quick Start Guide, publication CFP-QS001.

The network interface and GuardLink-enabled devices contain the latest firmware when shipped from the factory. Subsequent firmware revisions to address anomalies are released during the life of a product.

Verify that you have downloaded the firmware to your computer. Check rok.auto/pcdc to determine if later revisions of the controller firmware are available.

Before You Update

You can only upgrade the firmware of devices with GuardLink firmware 2.0 or later. In addition, all devices on the channel must have firmware 2.0 or later.

Firmware updates are occasional processes and must be planned according to when time is available. Updating a device at node 0 takes a few minutes. Updating the firmware on many devices on a large GuardLink system can be time consuming. Updating a device in node position 20 can take upwards of 20 minutes; node position 31 can take upwards of 45 minutes.

A helpful technique is to have a spare 4-conductor link cable to connect temporarily from one of the channels of the 432ES-IG3 network interface module directly to the device that requires updating. This technique places the device at node 0 for a quick update. After the update, reconnect the cables and move to the next device.

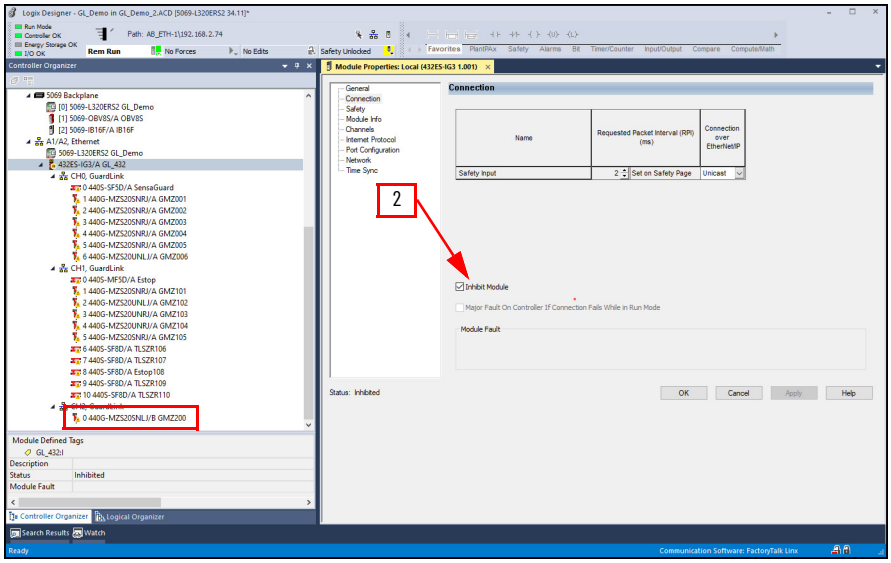
In the following example, the 440G-MZ safety switch is updated at node 0 on CH2.

To update the firmware:

- The tap or 440G-MZ safety switch must have a network connection to the controller.
- The controller must be online (Rem Run, Rem Prog, or Rem Test).
- The controller must be Safety Unlocked.

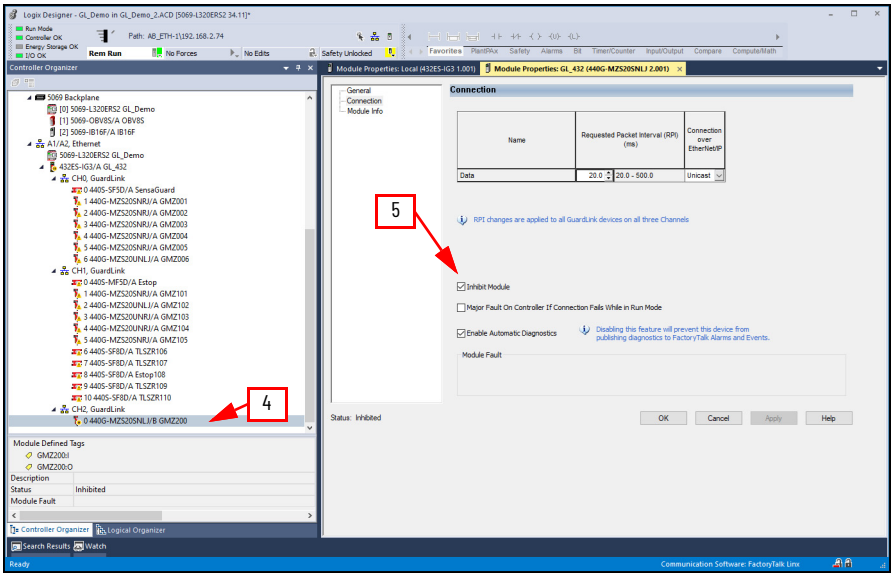
1. Open the Module Properties for the 432ES-IG3 network interface module and navigate to the Connection page.
2. Check the Inhibit Module checkbox.

   Notice that the 432ES network interface module Status is now Inhibited. All devices have a Status of Waiting.
3. Select Apply, and then select Yes to confirm in the follow-up window.



4. Select the 440G-MZ safety switch on CH2 and navigate to the Connection page.
5. Check the Inhibit Module checkbox.

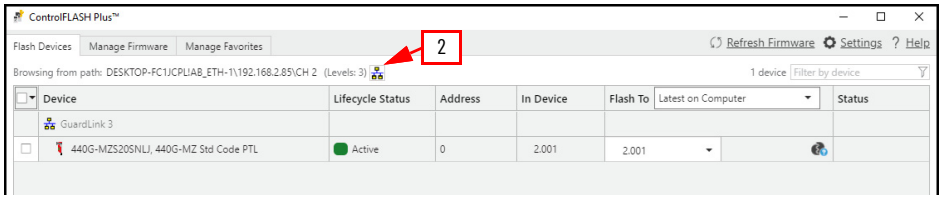
   Notice that the 440G-MZ safety switch Status is now Inhibited. All other devices remain with a Status of Waiting.
6. Select Apply, and then select Yes to confirm in the follow-up window.

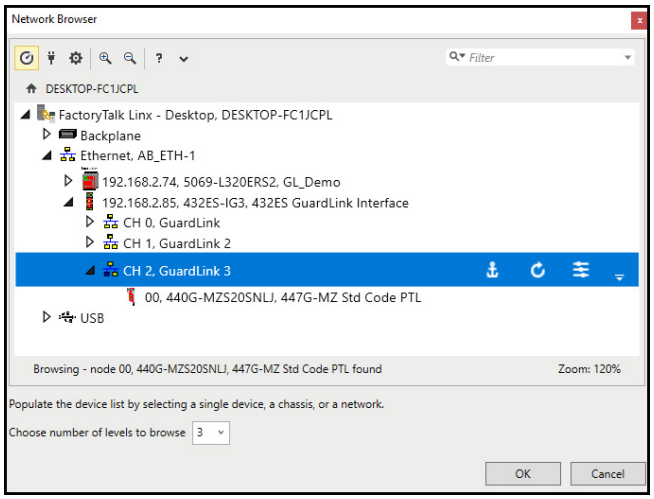


IMPORTANT When your update completes, return to the Connection page and clear the inhibit checkboxes for all devices.

Update Firmware

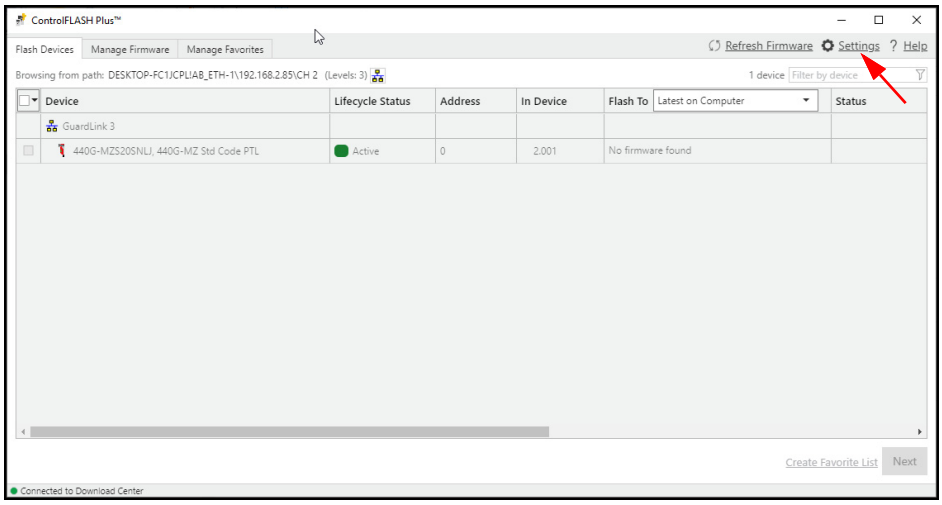
1. From the Start menu, select Flash Programming Tools > ControlFLASH Plus.
2. To choose a device to update, select the network icon to open the network browser.
   - For the 432ES module, navigate to the device.
   - For a safety switch, first navigate to the channel on the 432ES device, then to the safety switch.

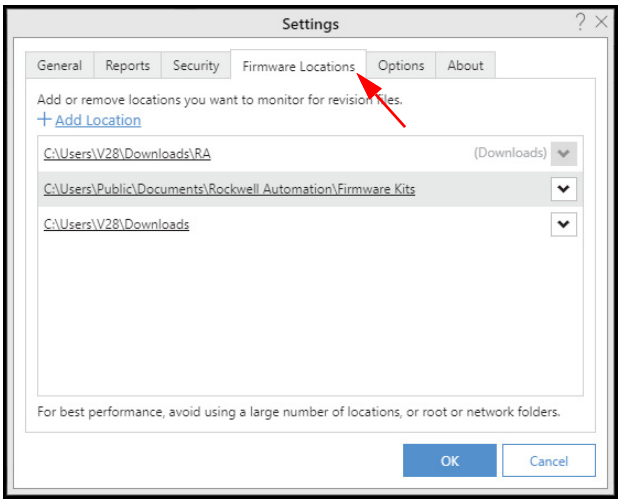




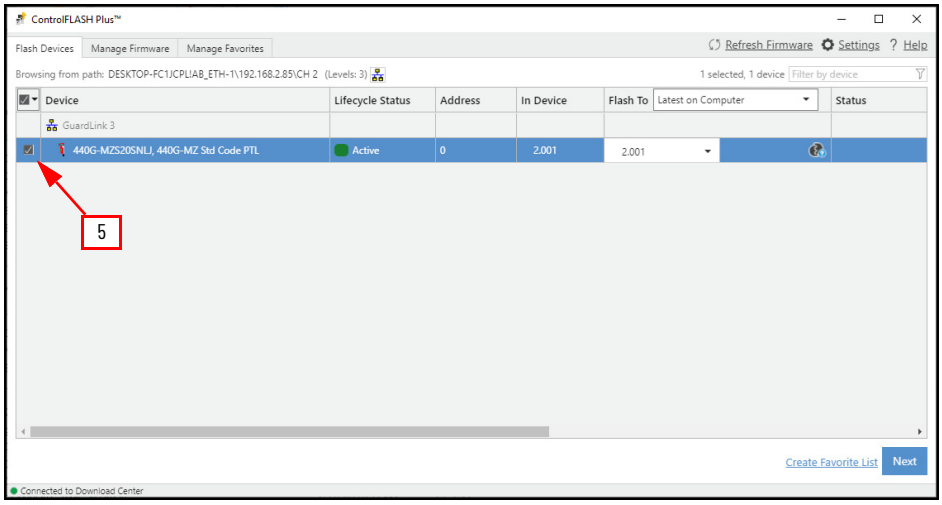
The window populates with all devices on the selected channel, along with the address and firmware in each device. In the following example, there is only one device on channel 0.

3. To navigate to the firmware on your computer, select Settings and select the Firmware Locations tab.



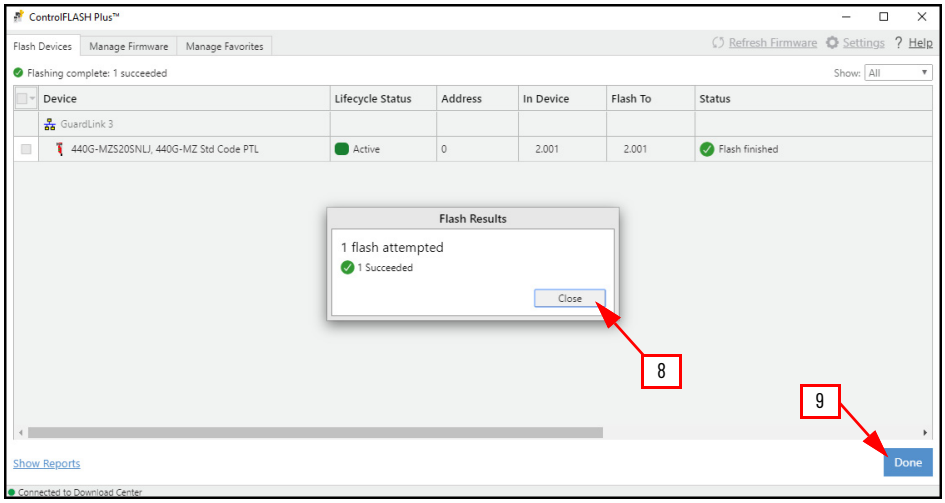


4. After you locate the firmware, select OK.
5. Check the box of the device that you want to update.



6. Select Next.
7. Select Flash.

8. When the update is complete, select Close.
9. Select Done.

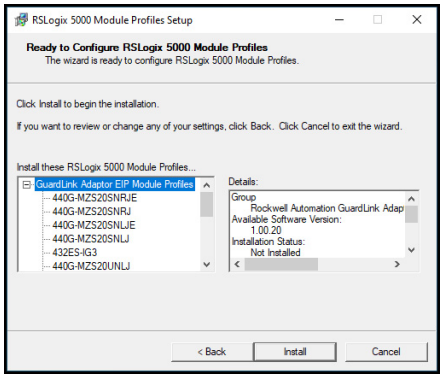


Install the Profile

To install the network interface module profile:

1. Run the MPSetup file.
2. Follow the dialog prompts and select the group of GuardLink EtherNet/IP Module Profiles.

   This action installs module profiles for the 432ES-IG3 network interface module and the other GuardLink-enabled devices.

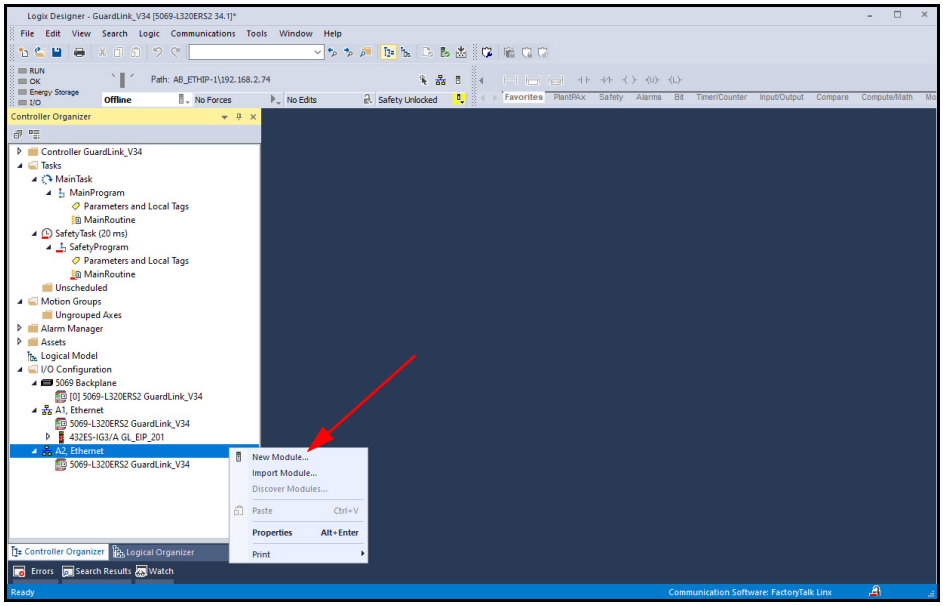


The default location of the installed module profile is:
C:\Program Files (x86)\Rockwell Software\RSLogix 5000\Module Profiles\RA 432ES GL-EIP.

Add the Network Interface Module to a Controller Project

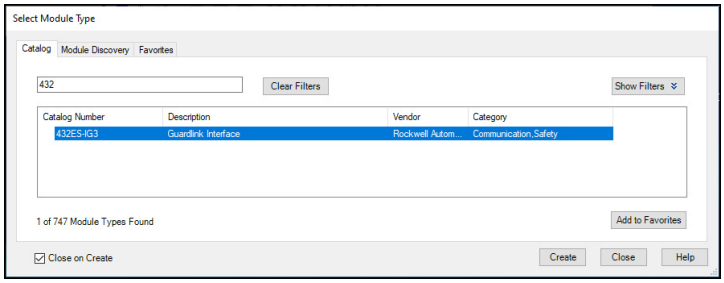
Use the Studio 5000 Logix Designer application to open or create a controller project.

1. Right-click the Ethernet module of the controller with which you want to communicate and select New Module.



2. In the Select Module Type window, type 432 in the filter field.

   The list of available catalog numbers reduces to the 432ES-IG3 network interface module catalog number.



3. Choose 432ES-IG3 and select Create.

   The module window opens.

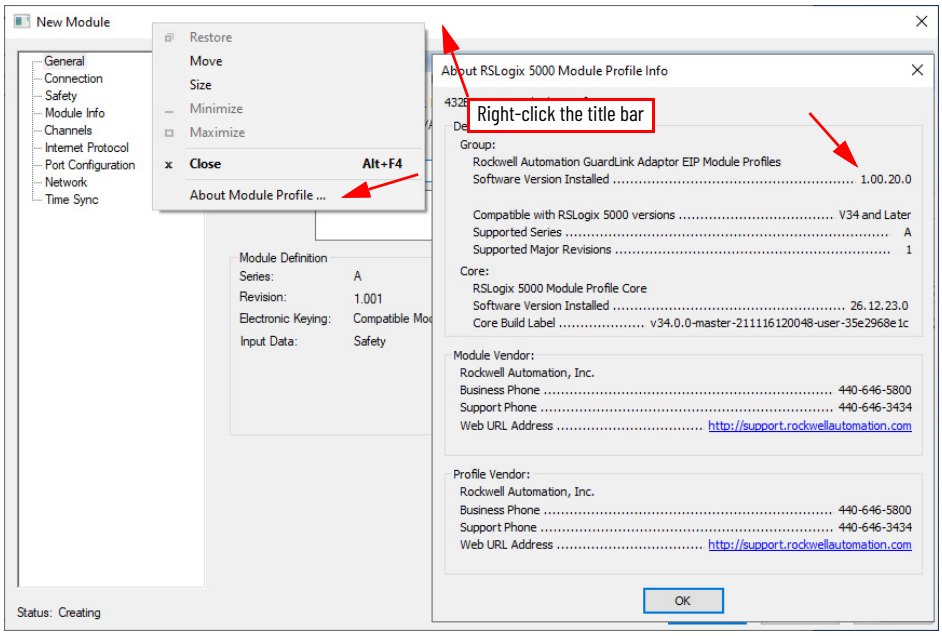
   The navigator column lists the pages that apply to the module (see General Page on page 33). An asterisk next to the page name indicates that a change is made.

You must select OK (or Apply) to accept the change. Be sure to apply any changes made on each page.

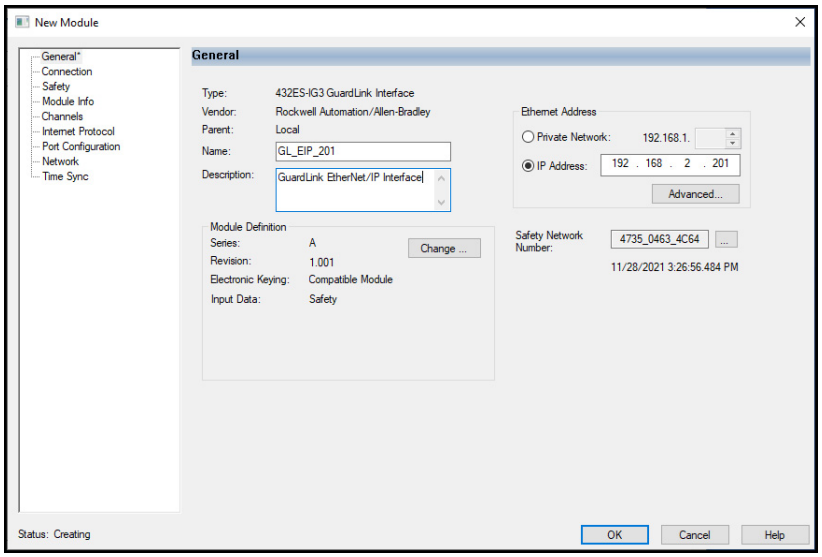
View Module Profile Properties

To view information about the module profile, right-click the New Module title bar (or Module Properties after installation), and then select About Module Profile.

The following screenshot shows 1.00.20.0 as the specific software version of the profile.



General Page

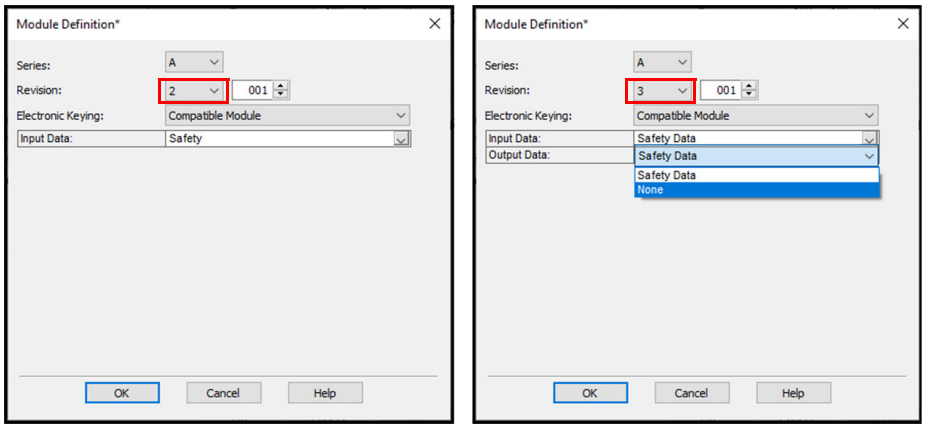


On the General page, these fields are available:

Field	Description
Name	Enter the name of the module (required). It is used to identify the controller tags.
Description	Enter more information about the module (optional).
Ethernet Address	Enter the IP address of the module.
Module Definition on page 34	View the details of the module. Select Change to open the Module Definition window.
Safety Network Number (SNN) on page 34	View the SNN for the 432ES-IG3 network interface module. Select the Ellipsis button (...) to modify the SNN.

Module Definition

From the Module Definition window, you can change the series letter, the major and minor revisions, the electronic keying, and the Output Data (revision 3.001 only). The Module Definition can only be changed when the host computer is Offline with the controller and the controller is not safety locked.



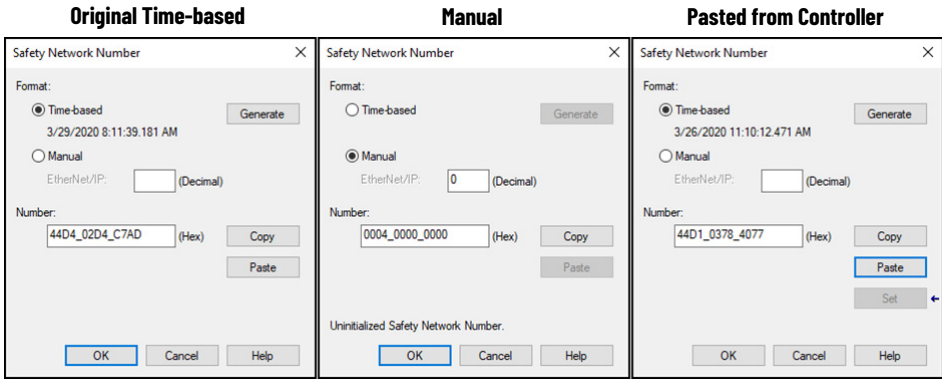
On the Module Definition window, these fields are available:

Field	Description
Series	Select the series letter of the device.
Revision	Select the firmware revision level of the device: • Revision 1.001 was the initial release. • Revision 2.001 added CIP Security. • Revision 3.001 added Lock/Unlock safety rating.
Electronic Keying	Select the desired electronic keying for the device: • Compatible Module - The Vendor ID, Product Type, Product Code, and the major revision of the interface firmware must be correct. The minor revision level is ignored. • Exact Match - The Vendor ID, Product Type, Product Code, Major revision of the interface firmware and the minor revision of the interface firmware must be current.
Input Data	With firmware revision 1.001 and 2.001, the only choice is Safety. With firmware revision 3.001, the only choice is Safety Data.
Output Data	With firmware revision 1.001 and 2.001, output data is not visible (not used). With firmware revision 3.001, output data can be either: • Safety Data - the Lock/Unlock Enable is available for conditional locking/unlocking safety rating. • None - the output assembly is not available; only unconditional locking/unlocking is available. Use this option for backward compatibility with firmware 1.001 and 2.001.

Safety Network Number (SNN)

You can use the following methods to change the SNN:

- In Time-based format, select the Generate button to create an SNN.
- Check the Manual format and edit the number.
- Paste the number from your cache (for example, the SNN copied from the controller). This option automatically changes the format to Time-based.



After you download the SNN and enter Remote Run, you can get this module status and fault message:

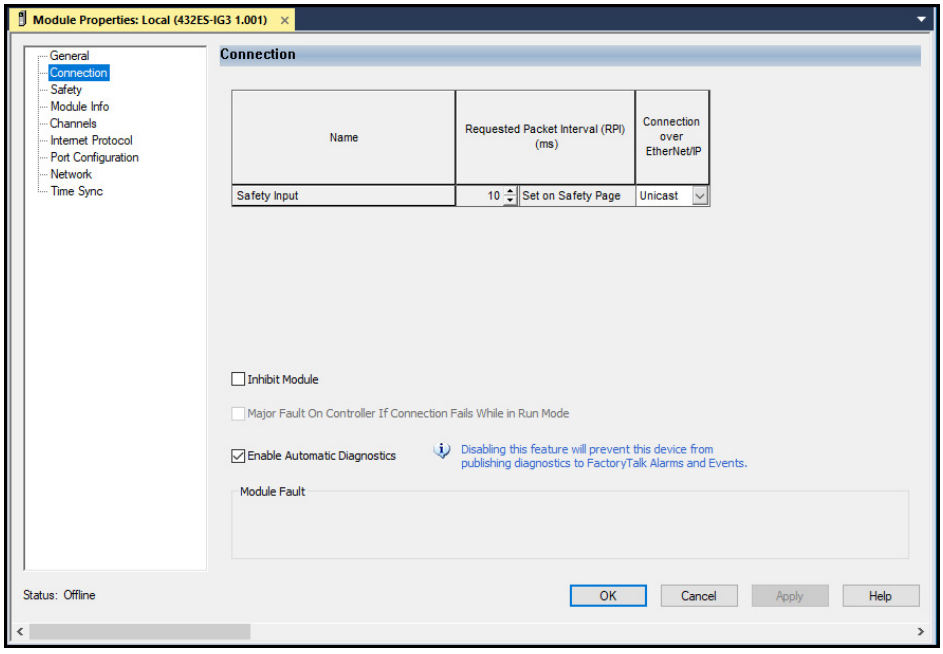
Status	IO Faulted
Module Fault	(Code 16#080e) safety network number mismatch.

This fault occurs because the SNN that resides in the 432ES-IG3 network interface module is not the same as the SNN that resides in the controller. To download the SNN to the 432ES-IG3 network interface module, inhibit the module on the Connection page, and then reset ownership of the interface on the Safety page.

Connection Page

The following screenshot shows an example of the Connection page in an offline controller project.

Figure 16 - Connection Page



On the Connection page, these fields are available:

Field	Description
Requested Packet Interval (RPI)	View the input RPI. To change the RPI, see Safety Page on page 37.
Connection over EtherNet/IP	The only choice is Unicast; Multicast is not supported. Connection is only to the host controller.
Inhibit Module	Leave this box unchecked to allow a connection to the module. Check this box to inhibit connection to this module. You cannot change this box when the controller is Safety Locked or in Run mode.
Major Fault if Connection Fails While in Run Mode	Check this box to allow the controller to show a major fault when a safety input or output connection is lost while the controller is in Run mode.
Enable Automatic Diagnostics	This box is checked by default. When checked, certain diagnostics automatically publish to FactoryTalk Alarms and Events. If unchecked, the messages do not automatically publish. You can only change this box while the controller is offline. See Appendix E on page 87.
Module Fault	This box shows the description of a module fault.
Status	Reports the current condition of the module. Examples include Offline, Creating, Connecting, Faulted, Running, and Waiting.

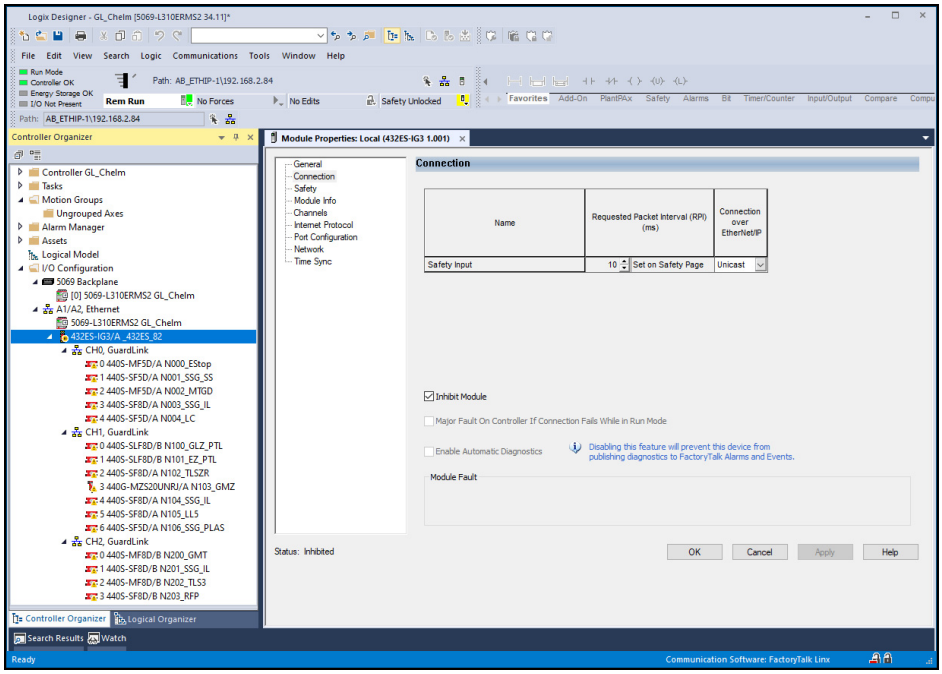
Inhibit Module

You can only inhibit the module if the controller is Safety Unlocked. When the 432ES-IG3 network interface module is inhibited, the status shows Inhibited, and the nodes have a status of Waiting.

The module ConnectionFaulted tag is set to 1, and all three channels revert to a safe state. All other module tags are set to 0. The node tags retain the values at the time that the inhibit is applied. The node tag values remain unchanged until the inhibit is removed.

The following screenshot shows an example with the inhibited 432ES-IG3 network interface module. On the node devices (taps and switches), the Link indicators on all three channels are steady red, and all Device indicators on all three channels flash green.

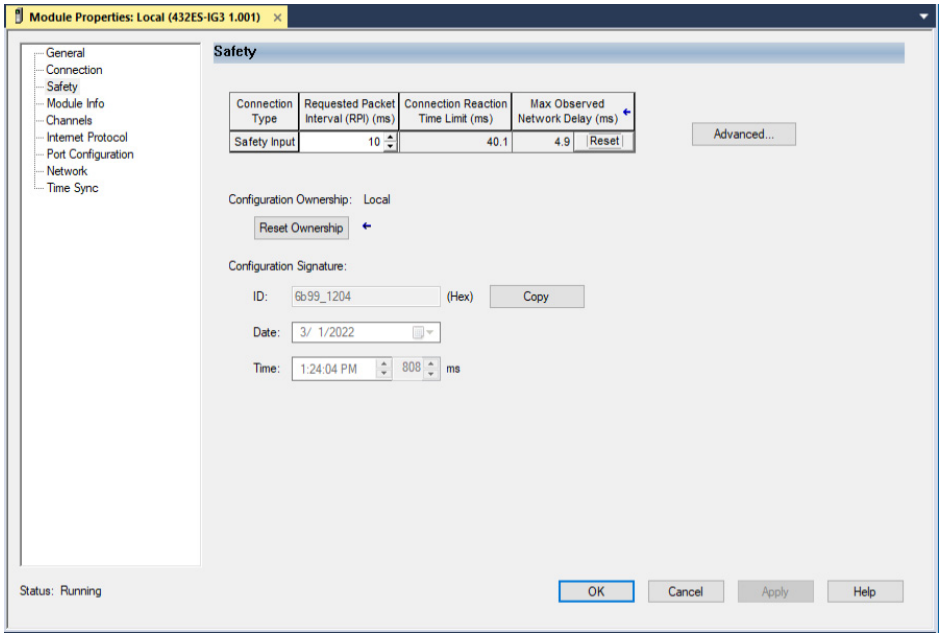
Figure 17 - Module Inhibited



Safety Page

The following screenshot shows an example of the Safety page with an online controller project.

Figure 18 - Safety Page



On the Safety page, these fields are available:

Field	Description
Connection Type	This field is read-only and always shows Safety Input.
Safety Input	The RPI can be adjusted directly between 2...500 ms. Alternatively, select Advanced (see Advanced Connection Reaction Time Limit Configuration on page 38).
Requested Packet Interval (RPI) (ms)	The RPI is the interval in which the controller inquires the status of the module inputs and outputs. A small RPI selection consumes network bandwidth and can cause spurious trips because other devices cannot gain access to the network. Applications that use safety light curtains to guard a hazard require the fastest response possible. The system maintains maximum performance when you select an appropriate RPI. Changes to the RPI momentarily cause a connection fault and all three channels to revert to a safe state.
Max Observed Network Delay (ms)	This field shows the maximum network delay in milliseconds when the controller is online and the module is connected. Select Reset to clear the values and restart the observations.
Configuration Ownership	The Configuration Ownership field has two possible statuses (also see Reset Ownership on page 38): • Local - This status is the desired status. The controller in the project owns the 432ES-IG3 network interface module and is the only controller that can send message instructions to the module. • Not Owned - The controller cannot send messages to or receive messages from the 432ES-IG3 network interface module.
Configuration Signature	The configuration signature defines the configuration of the module. The configuration signature is used to identify the unique configuration of the module. It is not necessary to monitor this signature as the GuardLogix® controller automatically monitors the signature.

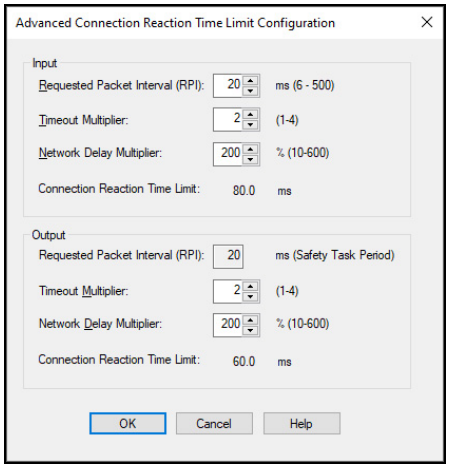
Advanced Connection Reaction Time Limit Configuration

The following screenshot shows the Advanced Connection Reaction Time Limit Configuration window, which allows you to make additional adjustments to the reaction time. The RPI, timeout multiplier, and network delay multiplier can be changed to modify the reaction time.

- Connection Reaction Time Limit (ms) - This field automatically calculates according to the RPI time.

ATTENTION: Add the connection reaction time limit for the safety inputs to the total response time in the GuardLink circuit and safety devices to calculate the safety distance.

Figure 19 - Advanced Connection Reaction Time Limit Configuration



IMPORTANT To determine what is appropriate, analyze each safety channel. The default Timeout Multiplier (2) and Network Delay Multiplier (200) creates a worst-case input connection-reaction time limit of 4 times the RPI. A safety administrator must approve changes to these parameters only after a thorough review.

If the RPI and connection reaction time limit for the network have the appropriate settings, then the Connected tag must remain low. Monitor the connection status bit to verify that it is not spiking intermittently due to timeouts.

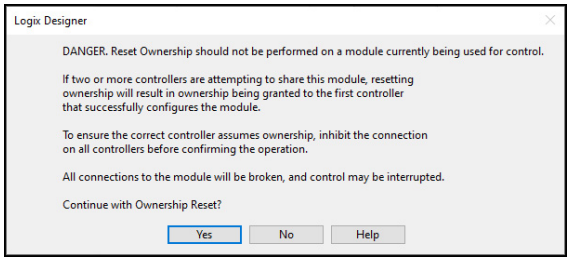
Reset Ownership

When you reset ownership, the SNN passes to the device, which allows the controller to own the 432ES-IG3 network interface module. The controller can be in Program, Run, or Test mode.

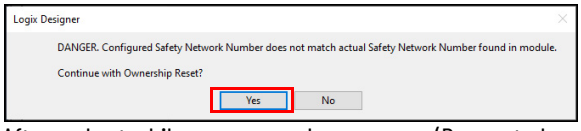
To reset ownership:

1. Confirm that your host computer is online with the controller.
2. Confirm that the controller is in Safety Unlocked mode.
3. From the Connection page, check the Inhibit Module box and select Apply.

4. From the Safety page, select the Reset Ownership button. The Reset Ownership window appears.
   - The Reset Ownership button only works if the connection to the module is inhibited and the controller is online. If you do not complete step 3, an error message displays (Failed to perform the required operation).
   - If previous edits are not applied, an error message displays (Ownership cannot be reset until pending edits are applied). Select the Apply button in the lower right corner.



5. You are prompted to continue. Select Yes.



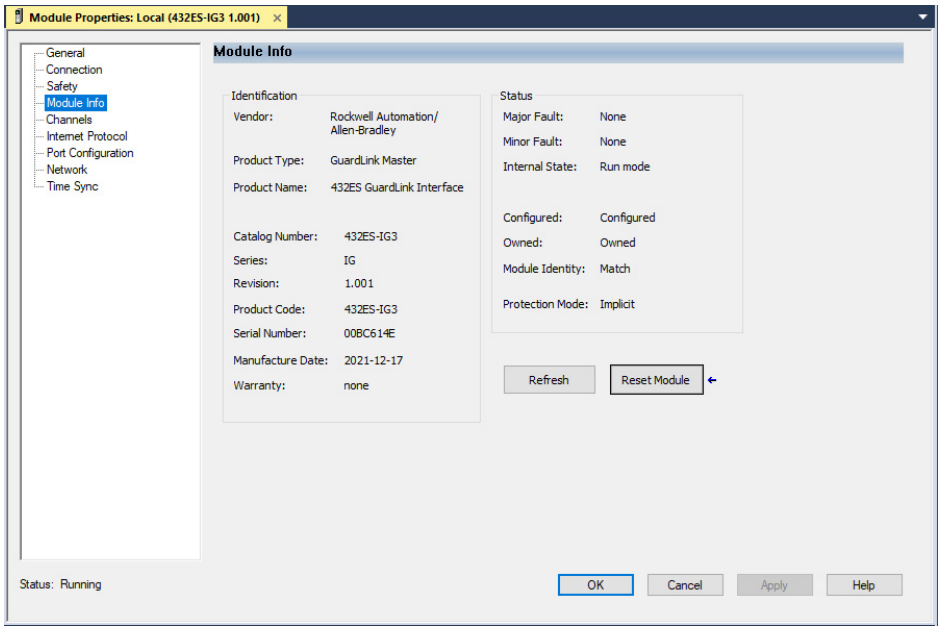
6. After a short while, a message box appears (Requested message timed out). Select OK.
7. From the Connection page, uncheck the Inhibit Module box and select Apply.
8. The SNN passes to the device. On the Safety page, Configuration Ownership shows Local. Now the controller and 432ES-IG3 network interface module SNN match.

Module Info Page

The Module Info page only populates when the controller project is online. The controller can be in Program, Run, or Test mode. The information displays as read-only.

The following screenshot shows an example of the Module Info page with Studio 5000® online. The 432ES-IG3 network interface module is in a running state with no major or minor faults. The module is configured and owned, and the module identity is a match for electronic keying.

Figure 20 - Module Info Page



On the Module Info page, these fields are available:

Field	Description
Identification	View the product identity and attributes.
Major Fault/ Minor Fault	Major and Minor Faults can have three states: • None - The 432ES-IG3 network interface module is functioning properly. • Recoverable - You can clear the fault without needing to cycle power to the 432ES-IG3 network interface module. • Nonrecoverable - Send a DeviceReset command to the 432ES-IG3 network interface module or cycle power by momentarily removing the connection.
Internal State	Internal State can have two states: • Run mode - The RunMode tag is set to 1 and the ConnectionFault tag is set to 0. The 432ES network interface module is operating properly. • Unconnected - The Inhibited module or other cause sets the ConnectionFault tag to 1. Loss of the physical Ethernet connection prevents the Module Info page from being populated.
Configured	Indicates whether the 432ES-IG3 network interface module is configured: • Configured - The 432ES-IG3 network interface module is properly configured. Configuration selects Used on the Channel page to allow a channel to go to an operational state. • No - The 432ES-IG3 network interface module is not properly configured.
Owned	Indicates whether a controller owns the 432ES-IG3 network interface module: • Owned - There is an exclusive owner connection that is open to the device. Owned means that there is a safety connection to the 432ES-IG3 network interface module. • No - There is no safety connection. See Reset Ownership on page 38 to reset ownership.
Module Identity	Indicates whether the series letter and revision in the controller match the values in the 432ES-IG3 network interface module: • Match - The 432ES-IG3 network interface module matches the identity in the controller. • No - The 432ES-IG3 network interface module does not match the identity in the controller.
Protection Mode	The IP address switches set the Protection mode during power-up. • Implicit - The device cannot accept any configuration or parameter changes due to the internal state. This issue can be due to conditions like an active safety connection, active firmware update, device in a nonrecoverable fault. • Explicit - Set by the IP switches and prevents all configuration or parameter changes (regardless of device state). To make such changes, use the IP switches to disable explicit protection. Explicit messages that affect the operation of the device are blocked. Explicit messages can fetch diagnostic information, such as changes to the IP address, reset of the module, and update of the firmware.

On the Module Info page, you can:

- Refresh - Updates the fields while maintaining the connection to the 432ES-IG3 network interface module.
- Reset Module - The Reset Module button only works when the connection is inhibited, which results in the ConnectionFaulted tag being set to 1. The 432ES network interface module performs the equivalent of a power cycle. Upon completion, the Module Info page updates with any changes.

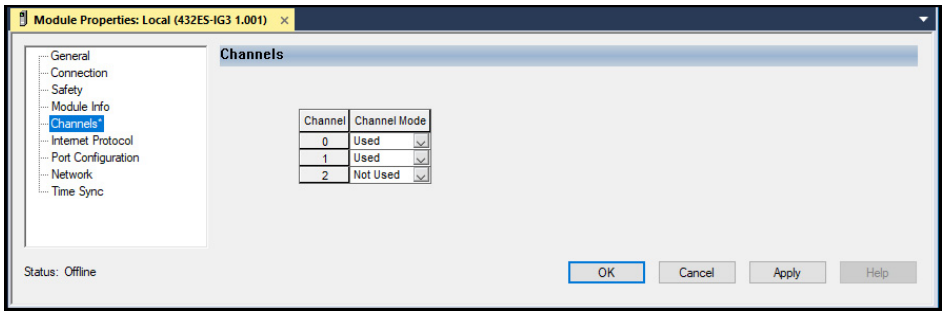
If the module is not inhibited, an error message displays (Failed to perform the required operation).

Channels Page

The following screenshot shows the Channels page that lets you select the mode for each channel. By default, each channel is set to Not Used. Set the desired channels to Used and select Apply. Changes to any channel mode cause the Status bit of all three channels to turn off (0) and then back on (1) momentarily if the Status bit was initially on because the safety connection turns off momentarily to apply the new configuration.

When a channel is not used, the channel Fault bit sets to 1 and the channel SIL 3 Status tag sets to 0. On the 432ES network interface module, the channel indicator flashes red.

Figure 21 - Channels Page

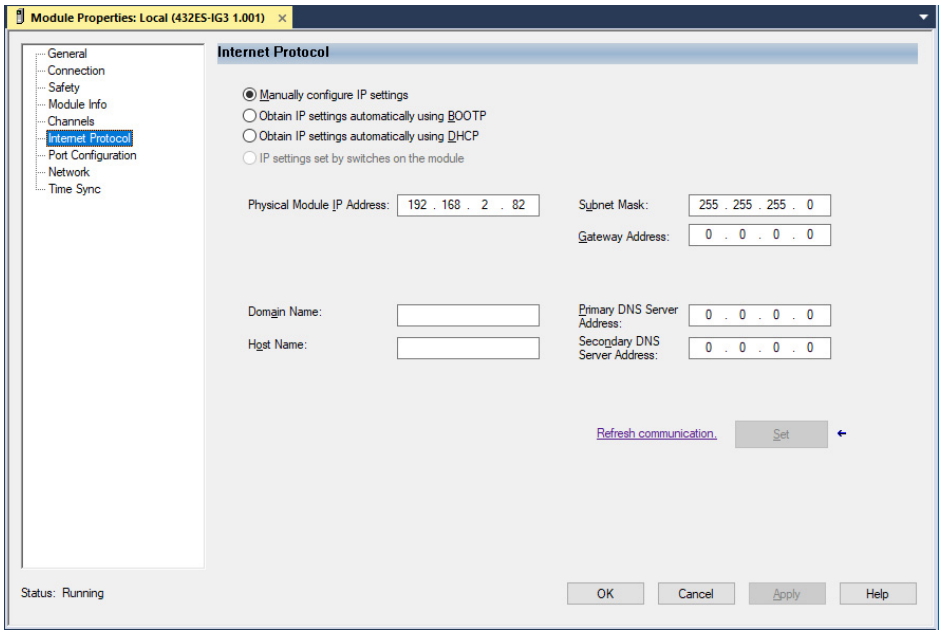


Internet Protocol Page

The following screenshot shows an example of the Internet Protocol page. This page is only populated and editable when the controller is online.

To change information in the fields, select Manually configure the IP settings. After you make changes, select the Set button, which enables as you make changes.

Figure 22 - Internet Protocol Page



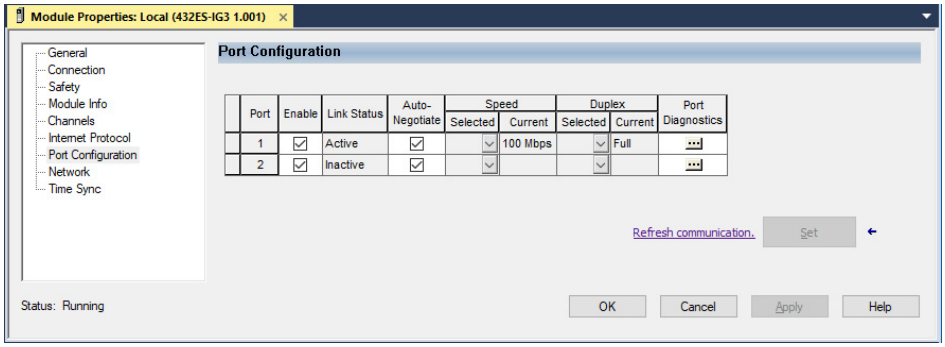
The ideal basic settings are:

- Manually configure IP settings
- Physical Module IP Address - Shows an assigned address
- Subnet mask - 255.255.255.0

Advanced applications:

- Gateway Address - Set to 0.0.0.0 unless you require controllers outside the local network read status data.
- Set button - Applies the changes that are made to the Internet Protocol settings.

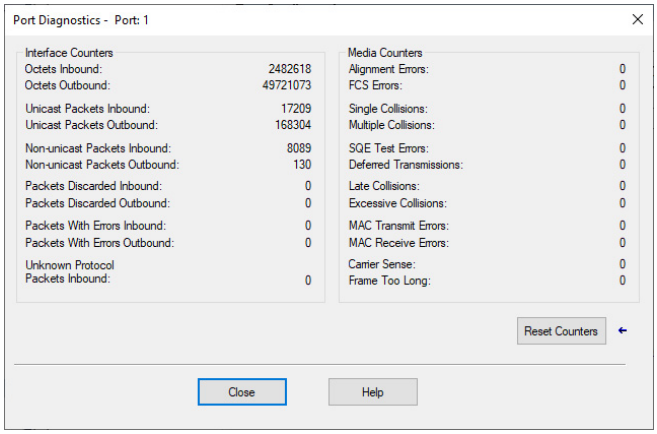
Port Configuration Page



On the Port Configuration page, these fields are available:

Field	Description
Port	Ports available.
Enable	Check the boxes to enable ports. For security purposes, disable the unused port.
Link Status	Shows whether the port is active or inactive. If the port is not enabled, the link status is blank.
Auto-Negotiate	Typically, this option is checked. If unchecked, you must specify the speed of the port. If the port is not enabled, the speed cannot be set.
Speed Selected	If this option is unchecked, you must select either 10 Mbps or 100 Mbps (preferred). The 432ES-IG3 network interface module does not communicate at 1 Gbps. If Auto-Negotiate is checked, this field is blank.
Speed Current	If Auto-Negotiate is checked, this field shows the current speed, either 10 Mbps or 100 Mbps. If Auto-Negotiate is unchecked, the field is read-only.
Duplex Selected	If Auto-Negotiate is unchecked, you must select either half-duplex (communications in one direction at a time) or full-duplex (communications in both directions simultaneously). Full-duplex is the preferred selection
Duplex Current	If Auto-Negotiate is checked, this field shows the current duplex. If Auto-Negotiate is unchecked, the field is read-only.
Port Diagnostics	Select the ellipsis (...). Figure 23 shows an example of the port diagnostics.
Set	When Auto-Negotiate is checked, the Set button is disabled. When Auto-Negotiate is unchecked, the Set button is enabled. After you adjust the configuration, select the Set button to download the changes to the 432ES-IG3 network interface module.

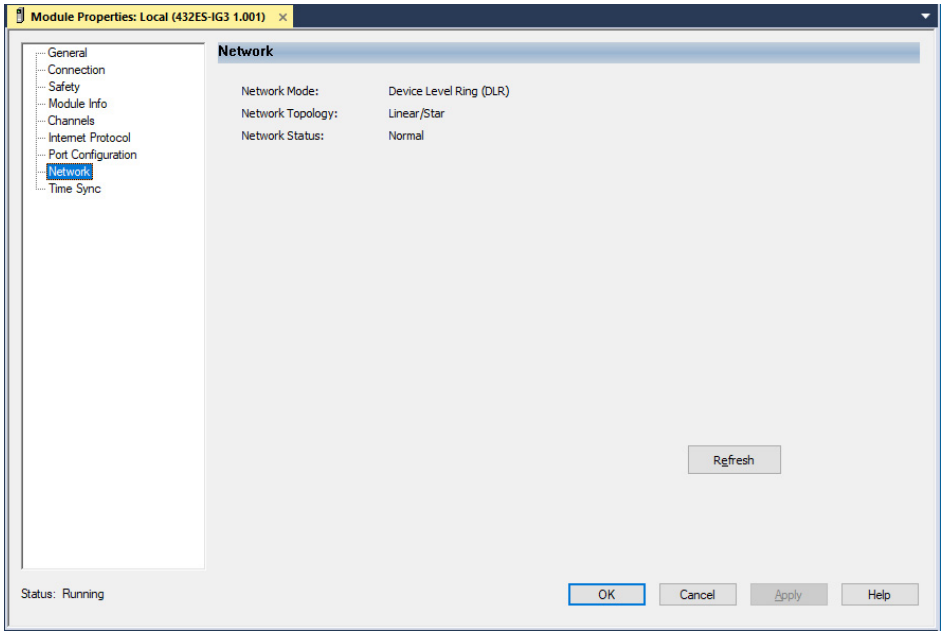
Figure 23 - Port Diagnostics Example



Network Page

The information in the Network page (shown in the following screenshot) is read-only. The fields populate when the controller is online.

Figure 24 - Network Page



The 432ES-IG3 network interface module supports the following topologies:

- Linear topology - A collection of devices that are daisy chained together.
- Device Level Ring (DLR) - Supports a ring topology. As defined by the Open DeviceNet® Vendor Association (ODVA), Device Level Ring is an EtherNet/IP™ protocol. DLR provides a means to detect, manage, and recover from single faults in a ring-based network.
- Star topology - Consists of a number of modules that connect to a central switch. Modules can be added or removed without affecting the rest of the network.

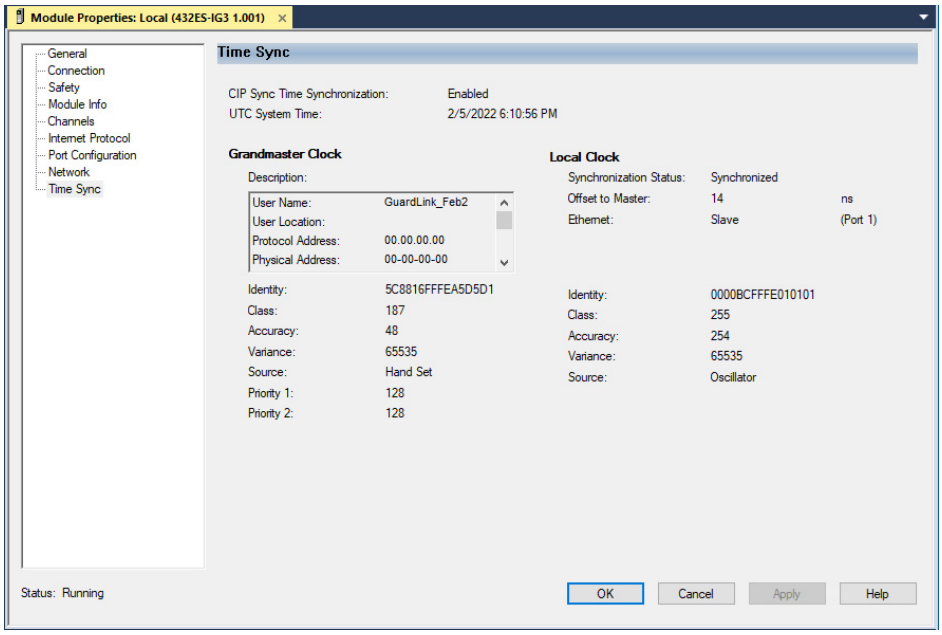
For more information on the supported EtherNet/IP network topologies and other EtherNet/IP features, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

Time Sync Page

The Time Sync page (shown in the following screenshot) displays and status information about the module when the project is online:

- CIP Sync™ Time Synchronization
- UTC System Time
- Grandmaster Clock - Shows the controller on the subnet checks the option (Enable Time Synchronization), and marks the role of the controller (Is the System Time Master).
- Local Clock information

Figure 25 - Time Sync Page



Append GuardLink Nodes

Each node is a GuardLink-enabled tap or a GuardLink-enabled safety switch. Each node must correspond to the controller organizer in the order in which the nodes connect to the host interface.

The order in which the channels populate is not critical; the three channels are independent.

Append GuardLink Nodes to the Network Interface Module

Append nodes to the controller tree in one of two ways:

- Manual method - Select each device individually.
- Discover modules method - Installed nodes can be discovered and loaded onto the controller tree.

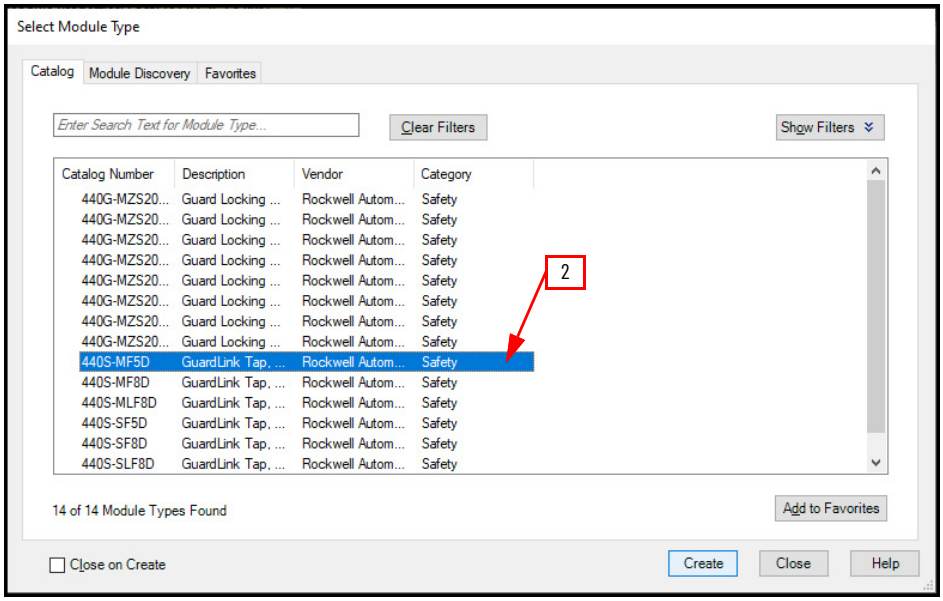
In either method, the controller can be in Rem Run, Rem Prog, or Rem Test mode, and the controller can be either Safety Unlocked or Safety Locked.

If the controller is offline, you can only add nodes manually.

Manual Method

With the 432ES-IG3 network interface module present in the controller tree, add nodes to the controller tree into the GuardLink® channels.

1. Right-click the desired GuardLink channel and select New Module.
2. Navigate to the node that you want to add.



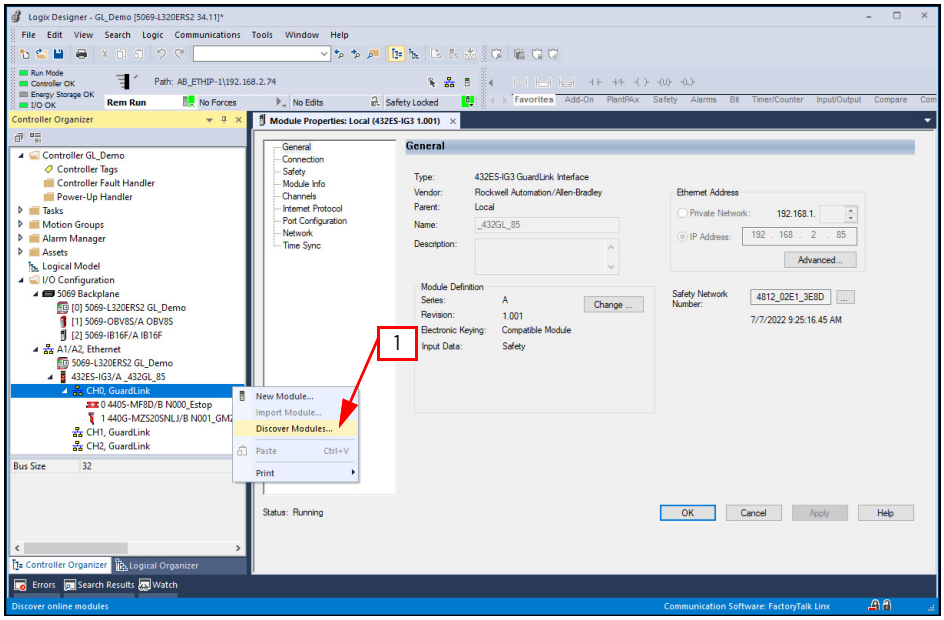
3. Follow the same process as you did to add the network interface module to the controller tree.

Discover Modules Method

To discover the modules, first install and power the nodes. The host computer must also be online with the controller. In this example, the host computer is in Rem Run mode with the controller Safety Locked. The controller owns the 432ES-IG3 network interface module and is in the Running status.

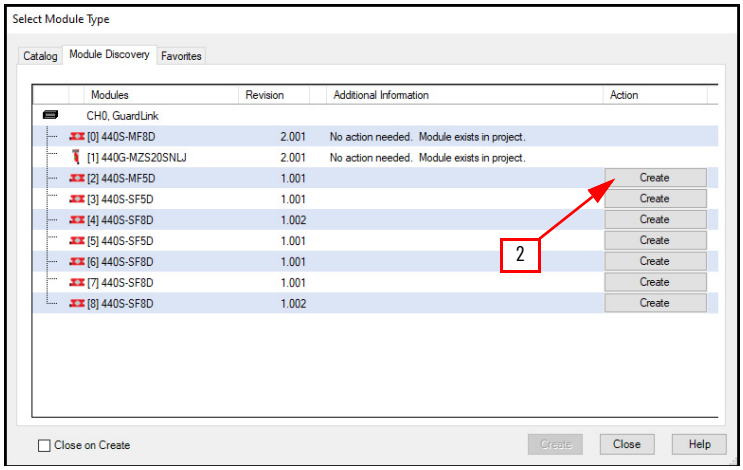
In the example shown in step 1, Ch0 already has two nodes. Additional nodes are added to the GuardLink circuit, then added to the controller tree with the Discover Modules feature.

1. Right-click the desired channel and select Discover Modules.

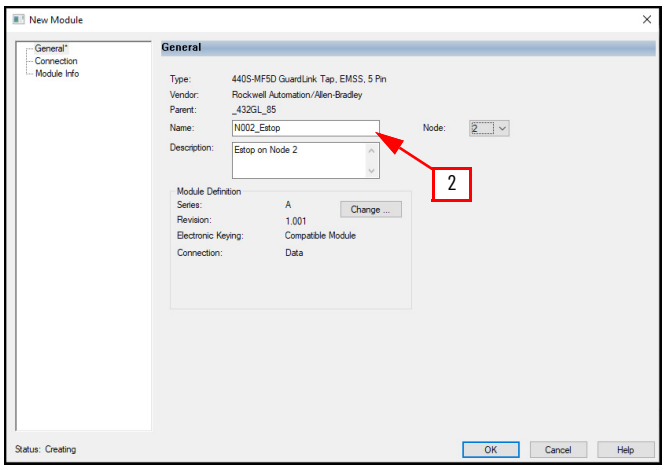


The Select Module Type window opens (see step 2) with the Module Discovery tab. After a short while, the table automatically populates with the list of modules (client devices) that connect to the channel, in the order in which they connect. The table also shows the firmware revision of the device and additional information.

2. Select the Create button for a node to add the node to the controller tree.



The New Module window opens and shows the General Page (see General Page on page 33).



3. The node position automatically populates; no action is needed.

The configuration pages and fields can vary for different nodes. See the online help or user manuals for those nodes for more details about configuration options.

4. Enter a unique node name (required).

Create names that are easy to locate in your controller tree. For example, start with the letter N for node. The first digit is the channel, the next two digits are the position on the channel; node 0...31. Then continue with your own text for additional description.

Example naming scheme:

- N000_freetext
- N001_freetext
- N100_freetext
- N101_freetext
- N200_freetext
- N201_freetext

5. Once you complete all other configuration settings, select OK to add the node to the controller tree.
6. Navigate to the Connection Page (see Connection Page on page 35).

7. Make necessary changes to the Requested Packet Interval (RPI).

   Select the desired RPI value, within the range of 20...500 ms (default 100 ms).

   We recommend that you change the RPI with the controller offline, as those changes apply to all nodes on all channels. Change the RPI of the lowest node (for example, Node 0 on Channel 0), select Apply, and then download the change to the controller.

8. If desired, check the Inhibit Module box.

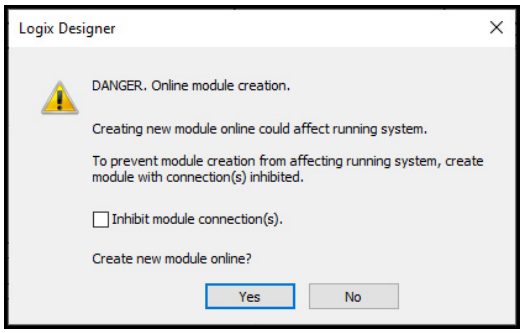
   When you inhibit a node, the 432ES-IG3 network interface module immediately sets its respective channel UnverifiedDevice tag to 1, which sets its Fault tag to 1, which sets its Tripped tag to 1, which finally sets its channel Status tag to 0 (a safe state).

9. Once you complete all necessary changes, select OK.

The Online Module creation message appears (see step 10). This window allows you to inhibit the module during creation.

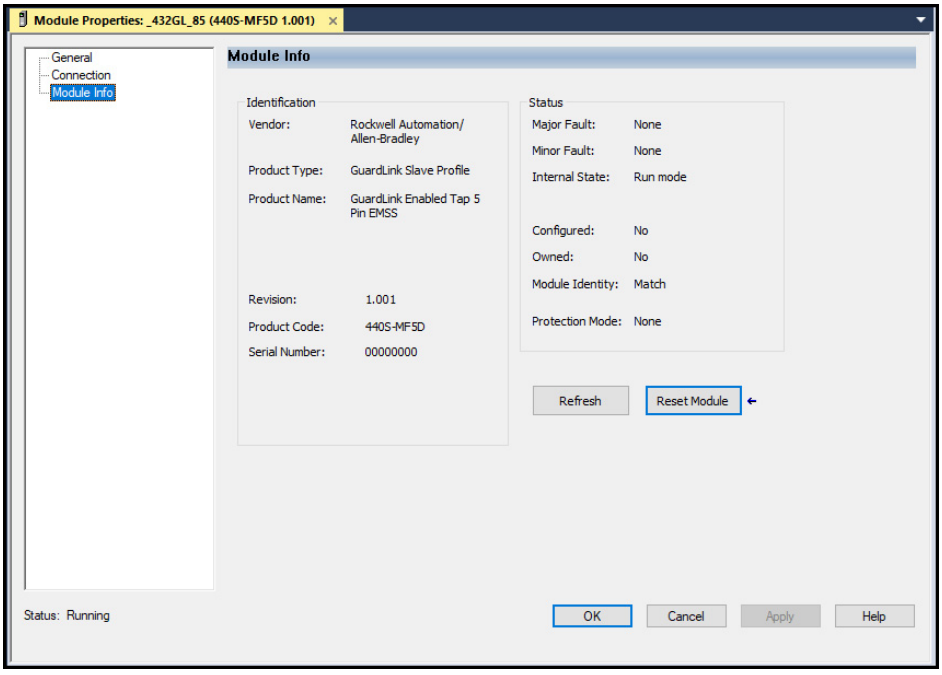
When you check the Inhibit module connections box, the Inhibit Module checkbox on the Connection page also checks and the module is inhibited from use.

10. Review the message and select Yes to accept changes.



The Module Info page (shown in the following screenshot) populates after the module is created and the module is online.

Figure 26 - Example Module Info Page for a Node



Notes:

Modify GuardLink Topology

Overview

Add, change, and/or remove nodes from any of the channels on the 432ES-IG3 network interface module to modify GuardLink® topology.

IMPORTANT	Verify and validate the performance of the safety function for all modifications to the GuardLink topology before you put the machine into a Production mode setting.

Consider the following situations:

- The controller is online with the host computer.
- The controller is Safety Locked or Unlocked.
- The node tags are used in a program routine.

Online Node Changes

The physical nodes on the GuardLink circuit can be changed with power to the 432ES-IG3 network interface module. Understand the role of the terminator.

You can implement some node changes while online with the controller in a remote setting (for example, Rem Run), then switched back to Run mode without stopping production. Changes that allow the system to run:

- Changes to the catalog number of a similar node (cannot change from a tap to a guard locking switch).
- Node tags not used in a program routine.

Other node changes require you to place the host offline, make the change, and then download the change to the controller. The controller stops Production mode to institute the change. Cases that require offline changes:

- Renumbering a node value.
- Node tags used in a program routine.

Controller Online

You can modify some node attributes while the GuardLink circuit is powered and with the controller online in Rem Run, Rem Prog, or Rem Test mode.

You cannot modify nodes if the controller is set to Run mode.

Safety Locked or Unlocked

You can make a limited number of changes to the nodes while the controller is in the Safety Locked mode. If you must download the configuration to the controller, first change the controller mode Safety Unlock.

Node Tags Used in Routines

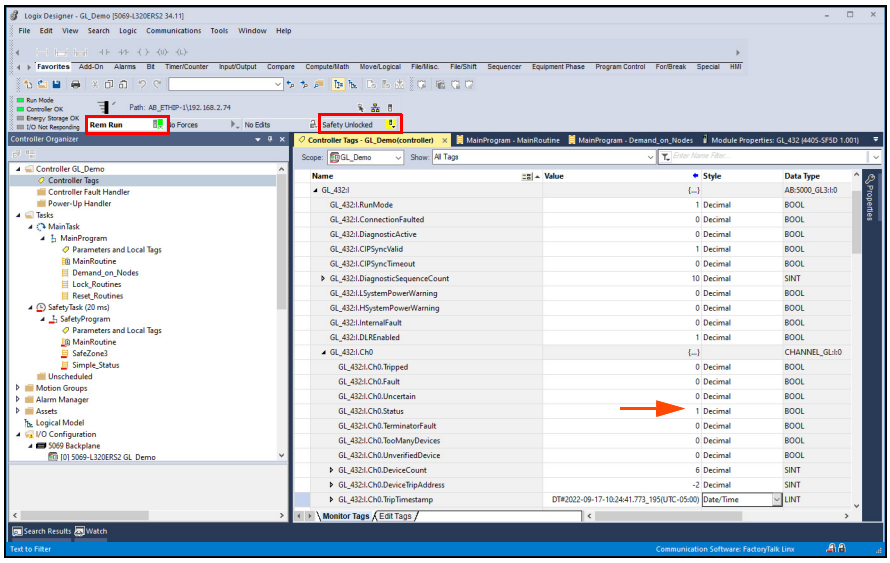
If a node tag is used in a program routine, you cannot modify or delete the node while the controller is online. Take the controller offline, make the changes, and then download the changes to the controller.

Insert a Node

You can only insert nodes while the host computer is offline. Node insertion requires you to reassign the upper node positions, which cannot be accomplished while the controller is online. The following example shows the controller in Rem Run mode and Safety Unlocked.

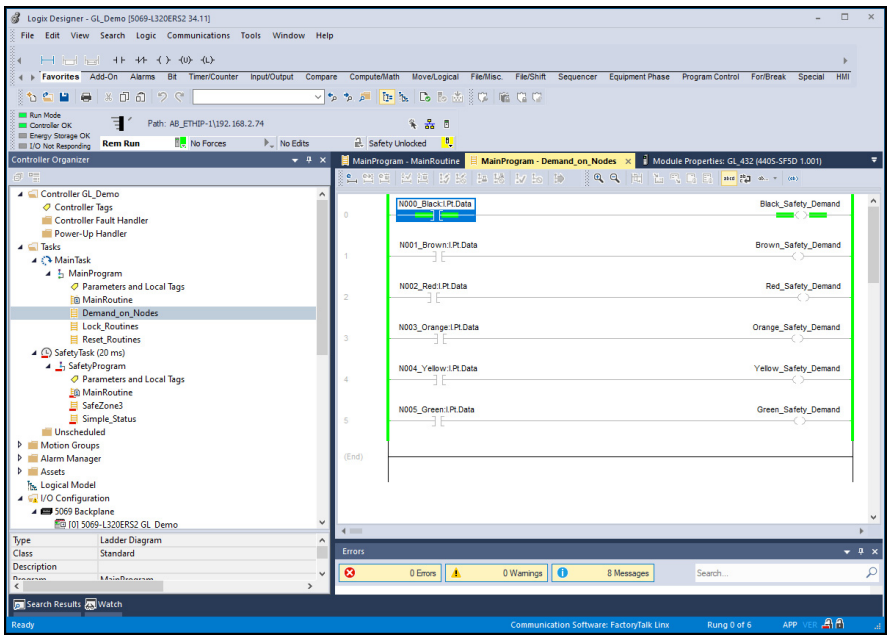
The following steps demonstrate how the 432ES-IG3 network interface module responds when a node is added. In this example, six nodes connect to CH0; the nodes are named as colors. The safety status of channel 0 is 1 (operational).

Figure 27 - Initial State of GuardLink Circuit



A simple program is created to monitor each node. If a safety demand is placed on a node, the node trips and its Pt.Data tag sets to 1. The following screenshot of the MainProgram tab shows that a safety demand is placed on the Black node (Node 0), while all other nodes have no safety demand.

Figure 28 - Simple Program to Identify Safety Demands on Nodes

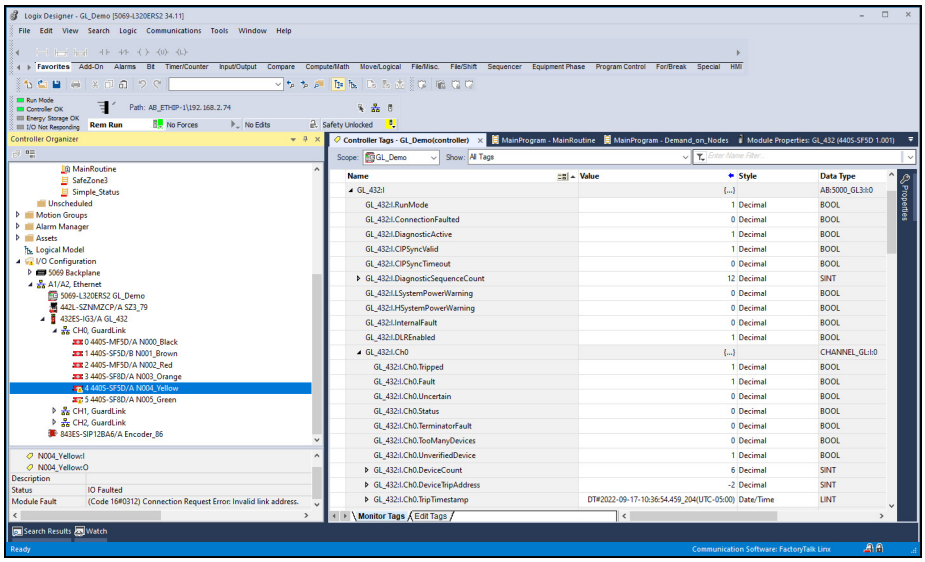


The following screenshot shows an example of inserting a node.

1. Without removing the power to the 432ES-IG3 network interface module, remove the link cable at connector J1 of node 4. The safety system transitions from an operational to a safe state.
   - Ch0.Tripped: 0 to 1
   - Ch0.Fault: 0 to 1
   - Ch0.Status: 1 to 0
   - Ch0.UnverifiedDevice: 0 to 1
   - Ch0.DeviceCount: 6 to 6 to 0

     When the link is broken, the DeviceCount remains at 6. The transition to 0 occurs when the new tap is added to J1 (Link In) and J2 (Link Out) of the new tap is left open.
   - Ch0.DeviceTripAddress: Shows -2 because the trip is due to an external event.
   - Ch0.TripTimestamp: Updated to the date and time when the event occurred.
   - The Controller Organizer shows status errors on nodes 4 and 5 (IO Faulted), an Invalid link address.
   - On the 432ES network interface module, the CH0 indicator flashes red.
   - On the taps, the Link status indicators are steady red, and the Device status indicators flash green.

Figure 29 - Break Link Cable

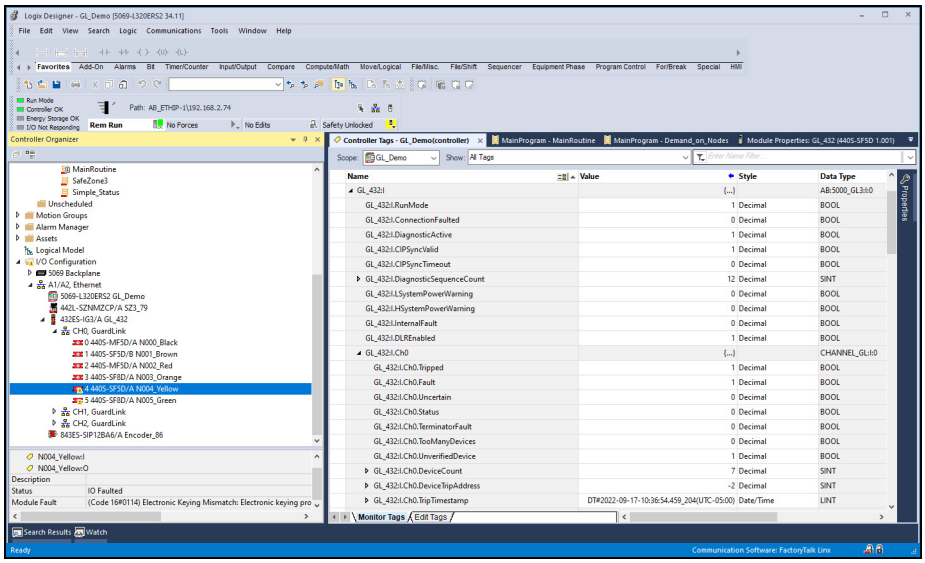


2. Connect the new node to the Yellow node. Then connect the J1 of the new node to J2 of the Orange node.

   This connection completes the GuardLink circuit. The device count gets incremented and there are no additional changes. The safety system remains in a safe state

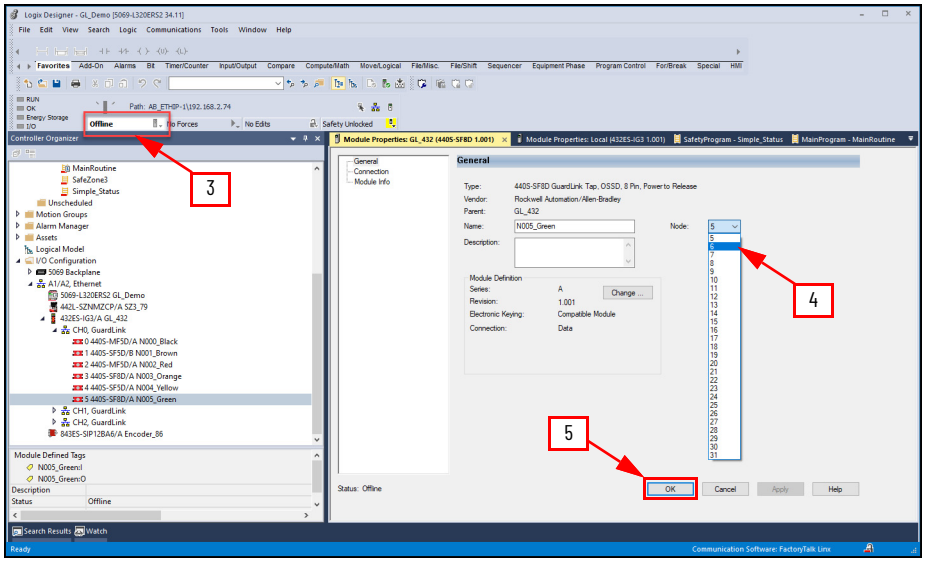
   The following screenshot shows the results after completing the GuardLink connections.
   - Ch0.DeviceCount: 6 to 7
   - The channel is still tripped with a fault and unverified device.
   - Node 4 correctly reports an Electronic Keying Mismatch because the inserted node is a different tap catalog number.

Figure 30 - Node Added to Complete the GuardLink Circuit

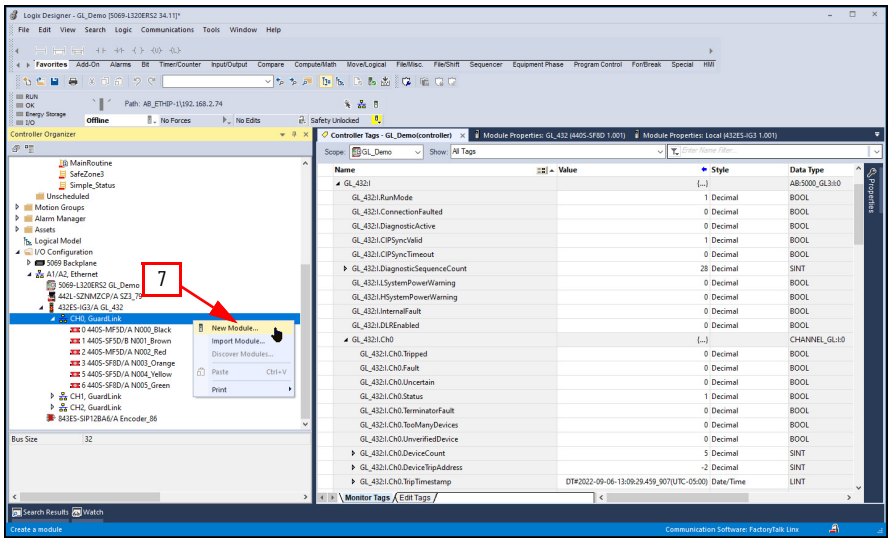


Before you insert the node at position 4 in the Controller Organizer, you must reassign the current nodes Yellow (4) and Green (5) to positions 5 and 6. This change preserves any logic or automatic diagnostic reporting that is associated with nodes 4 and 5 because the logic is associated with the node name, not the node number.

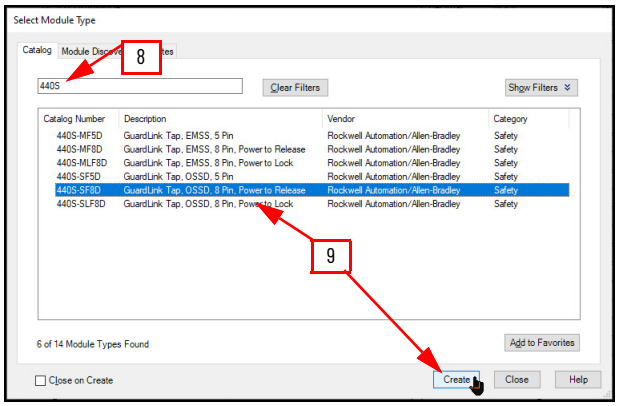
3. Take the controller offline.
4. Change the node position from 5 to 6.
5. Select OK.
6. To change node position 4 to position 5, repeat step 3...step 5.



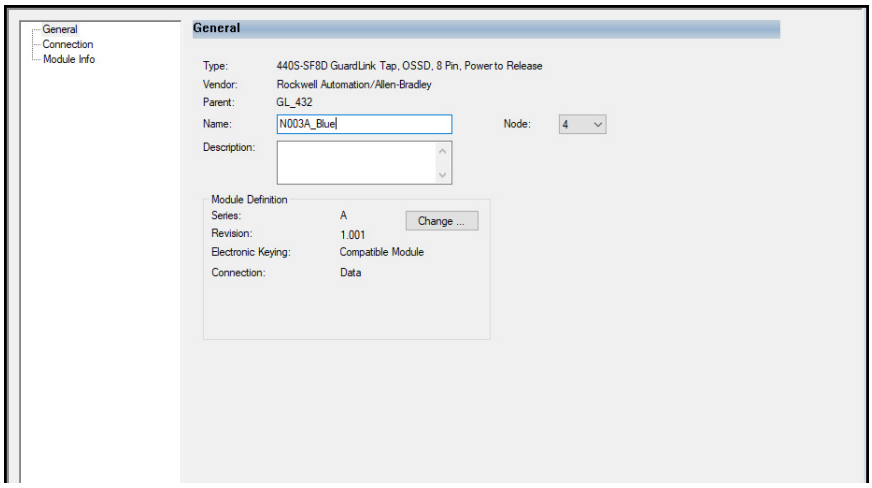
7. The Controller Organizer shows the updated nodes, with node 4 missing. Right-click the CH0, GuardLink branch and select New Module.



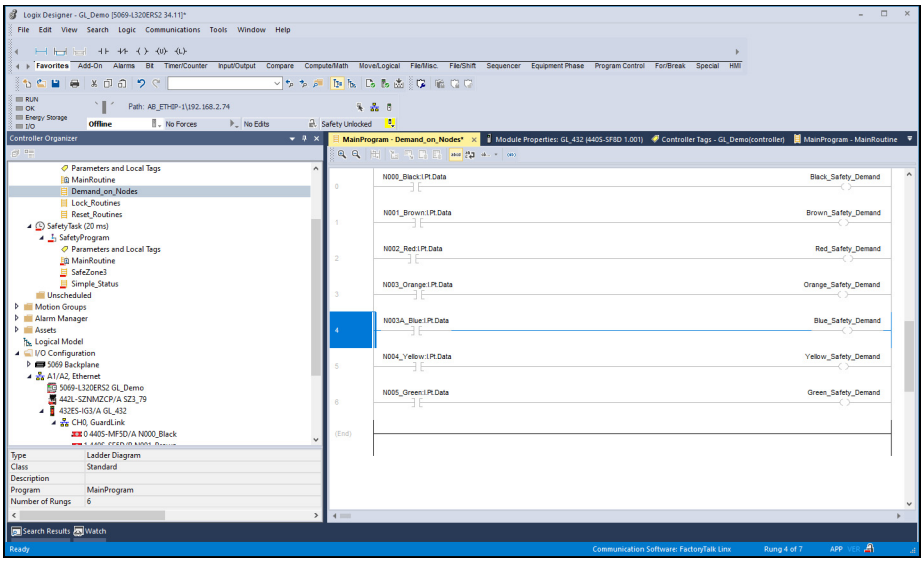
8. In the Select Module Type window, type 440S in the filter field.
9. Highlight the tap that you want to add and select Create.



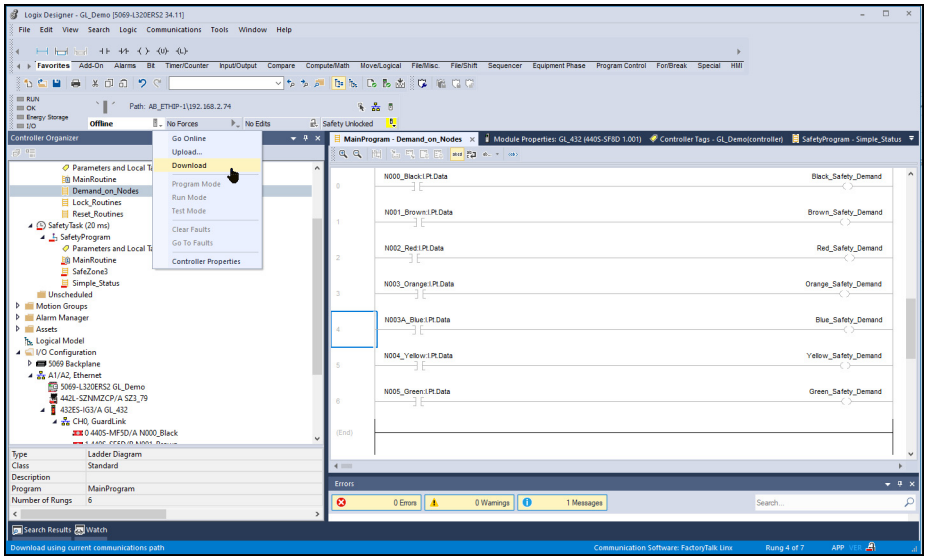
10. The New Module window automatically populates with the first available node position (4). Type in a unique name (Blue in this example) for the node and select OK.
    - By default, the electronic keying is set to Compatible.



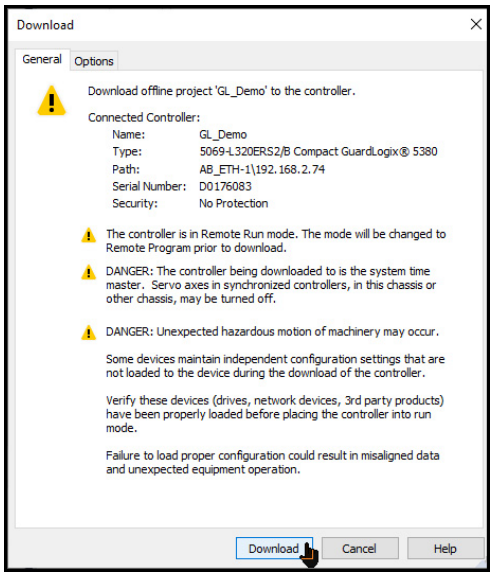
11. The Blue node appears in position 4. You can now add code to the Main Routine to capture the event when the Blue node trips.



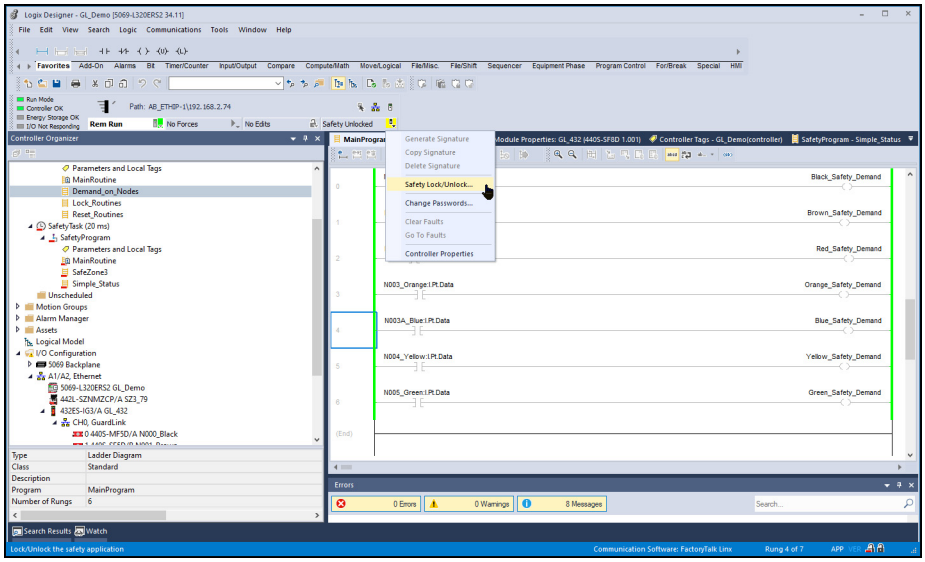
12. The changes download to the controller.



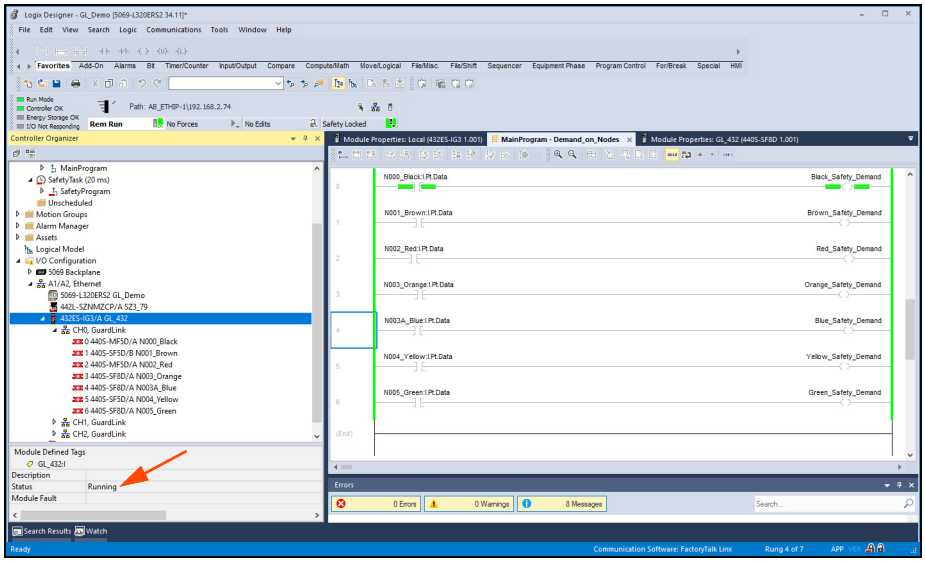
13. Read the download messages, and select Download.



14. In the follow-up message, select Yes to change the mode back to Remote Run.
15. Set the mode back to Safety Locked.



The 432ES-IG3 network interface module system is Running.



Change a Node

In this example, the 440S-SF8D in node position 4 changes to a 440S-SF5D. This change can take place while the 432ES-IG3 network interface module is powered. There are two cases:

- Case1 - If the Logix Designer application does not use any of the node 4 tags in a program routine, then the node can change with the controller in Rem Run and Safety Locked modes.
- Case2 - If the Logix Designer application uses a node 4 tag in a program routine, the controller must be offline and Safety Unlocked. Delete the existing node, create a node, and give the node the same name. The program routine for node 4 is retained after you return the controller online, as long as the name of the node remains the same.

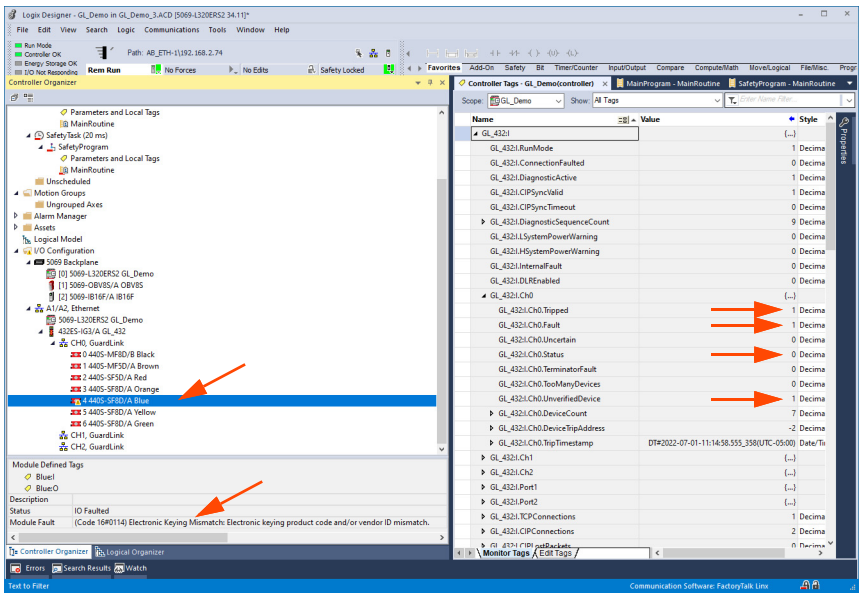
This example demonstrates Case1. The Blue Safety Demand ladder logic from the Insert a Node section is removed from the main routine. In addition, the safety demand on the Black node is removed.

While you replace the tap, the Link cables are disconnected. The channel is in a safe state with the following CH0 channel tags:

- Ch0.Tripped: 1
- Ch0.Fault: 1
- Ch0.Status: 0
- Cho.UnverifiedDevice: 1

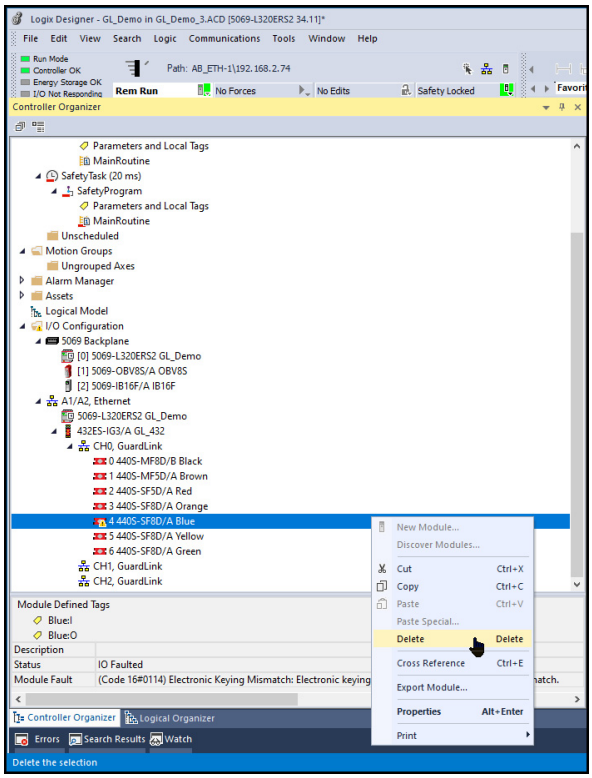
When you install the new tap with the link cables connected and the new switch operational, the Logix Designer application reports an electronic keying error at node 4. The CH0 channel tags remain unchanged.

Figure 31 - Node 4 Has a Keying Error

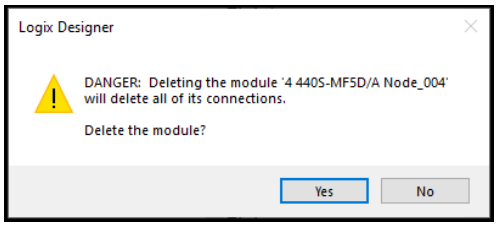


To correct this error, first delete the node, and add the correct catalog number.

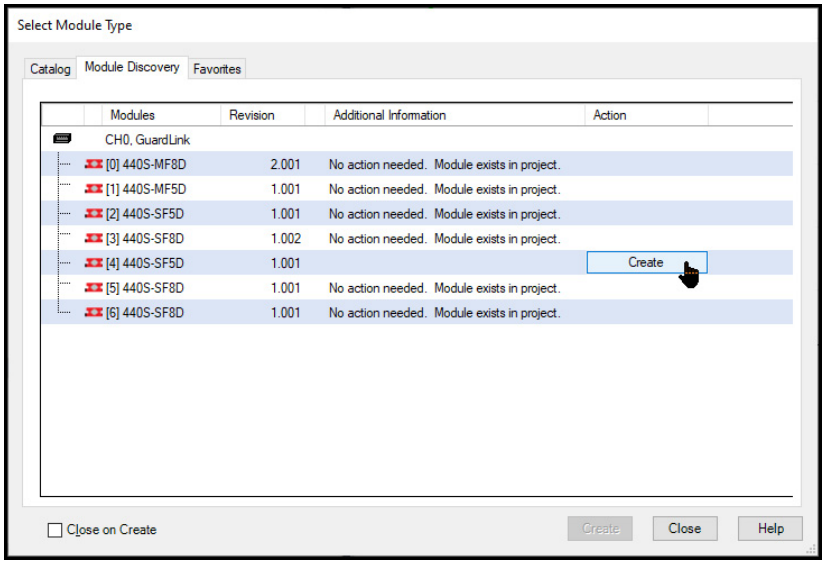
1. Right-click the node and then select Delete.



2. The Logix Designer application presents a danger warning. Select Yes if no danger exists.

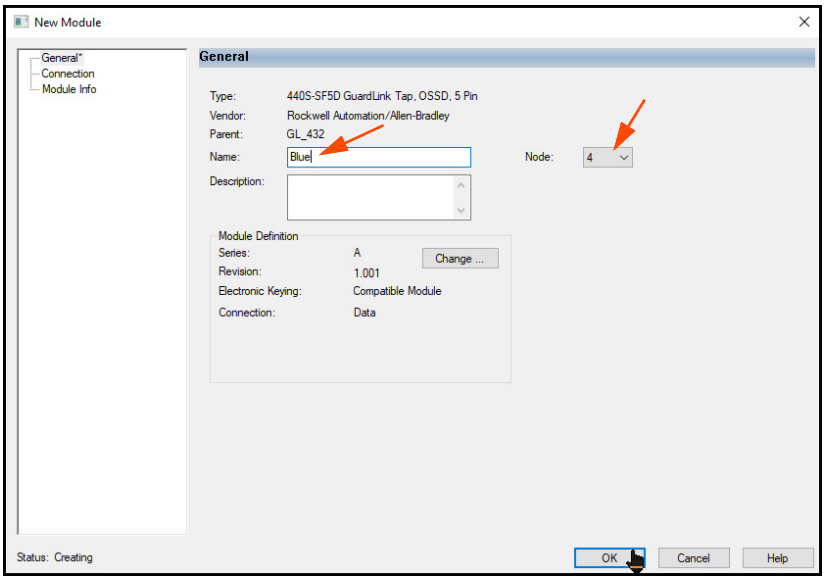


3. Right-click the CH0, GuardLink channel and then select Discover Modules.
4. Select Create to add the new modules to the Controller Organizer.

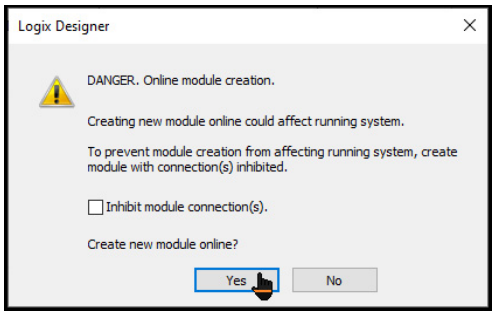


The node number automatically assigns to the first open position, which is position 4.

5. In this example, none of the tags for node 4 are used in a program routine. Therefore, you can assign a unique name to the node or assign the same name as the node it replaced.
6. To apply the name, select OK, then close the window.

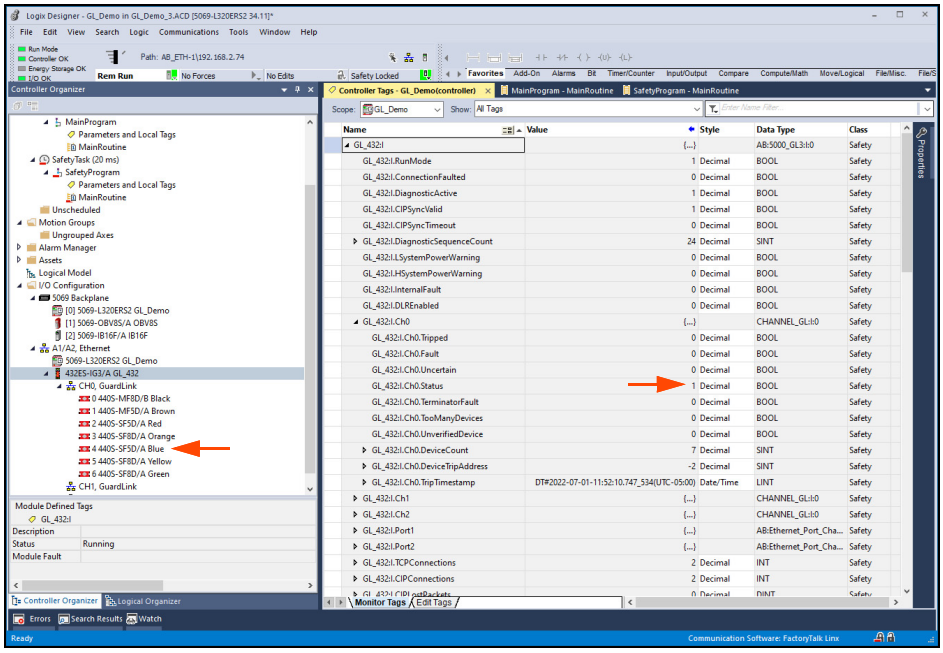


7. The online module creation message appears. This window allows you to inhibit module connection. In this example, leave the box unchecked and select Yes.



8. Close the Module Discovery window.

The new 440S-SF5D tap replaces the 440S-SF8D tap at node position 4, and CH0 transitions to an operational state with Status at a value of 1.



Append a Node

In this example, an additional node is added after the last node. Node topology can change while power is applied to the 432ES-IG3 network interface module.

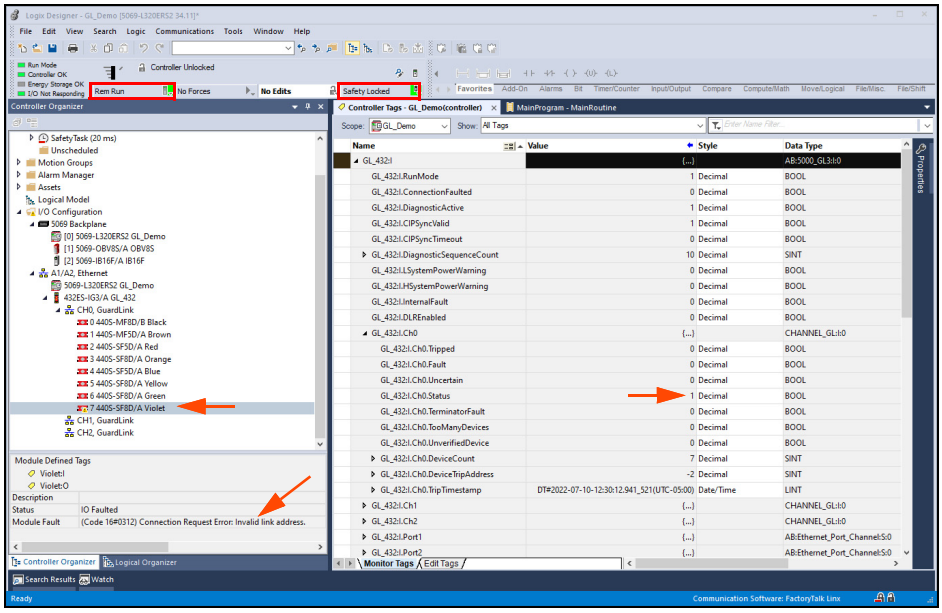
When you increase the number of nodes in a GuardLink circuit, you must first understand the role of the terminator, see Terminator on page 17. When appending additional nodes, remove power from the last node by removing the Link In connection.

ATTENTION: When you append nodes to a GuardLink circuit, remove the Link In cable from the last node. After you add the additional nodes with the terminator at the last node, reconnect the Link In cable.
Failure to break the link signal does not allow the appended node to activate. Subsequent operation of the appended safety device does not affect the safety function and can lead to personnel injury.

Conclude changes to the safety system configuration with a risk assessment verification test.

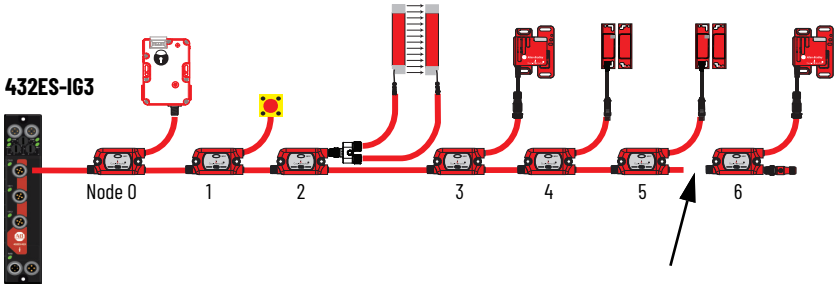
With the terminator that is connected to the last node, connect the link cables, and the GuardLink system automatically determines the correct number and type of nodes.

In this example, the node is added in the Logix Designer application first, and then the hardware is added afterwards. Node 7 is manually added to CH0 in the Logix Designer application first. The node shows a fault message (Invalid link address). Although a new node is appended, the CH0 Status remains at 1 (in an operational state) since the hardware has not changed.

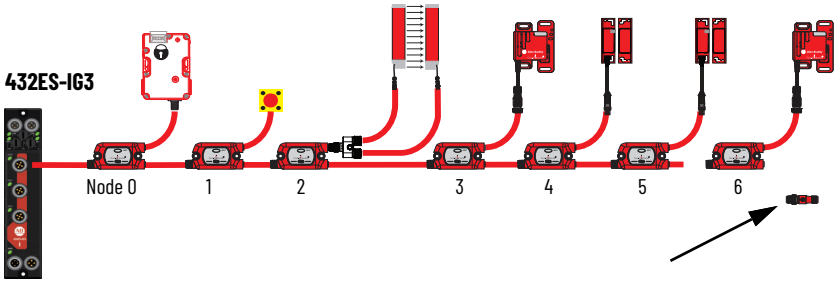


The following recommended steps show how to add nodes to a channel. You can perform these steps with power applied to the 432ES-IG3 network interface module.

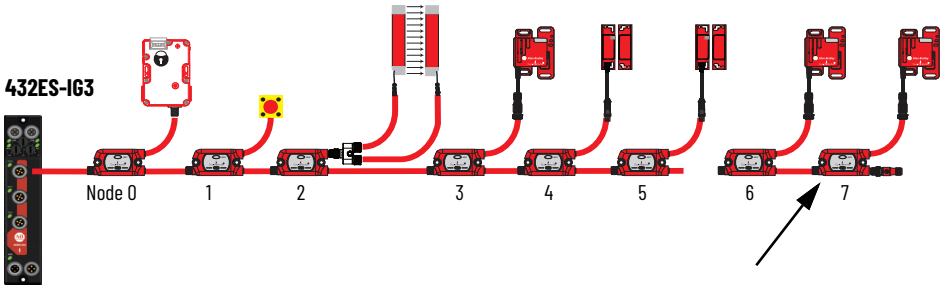
1. Remove the Link In connection to node 6. This action removes node 6 as the GuardLink Safety Source. Observe these tag changes:
   - Ch0.Tripped: 0 to 1
   - Ch0.Fault: 0 to 1
   - Ch0.Status: 1 to 0
   - Ch0.UnverifiedDevice: 0 to 1
   - Device Count remains unchanged.
   - Node 6 shows a fault (Invalid link address).



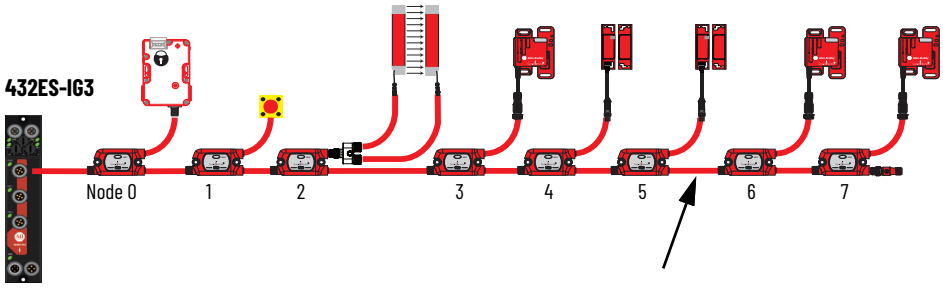
2. Remove the terminator from node 6.



3. Connect the new tap, with the terminator and safety device to node 6.



4. Reconnect the Link In connection to node 6. Node 7 is the new GuardLink Safety Source. Observe these tag changes:
   - Ch0.Tripped: 1 to 0
   - Ch0.Fault: 1 to 0
   - Ch0.Status: 0 to 1
   - Ch0.UnverifiedDevice: 1 to 0
   - Device Count: 7 to 8



Delete a Node

You must remove the inner nodes with the controller offline. While offline, the nodes can be renumbered to maintain a consecutive sequence.

ATTENTION: If you delete nodes while the controller is online, unexpected behavior, including a nonrecoverable fault that requires a power cycle of the controller, can occur.

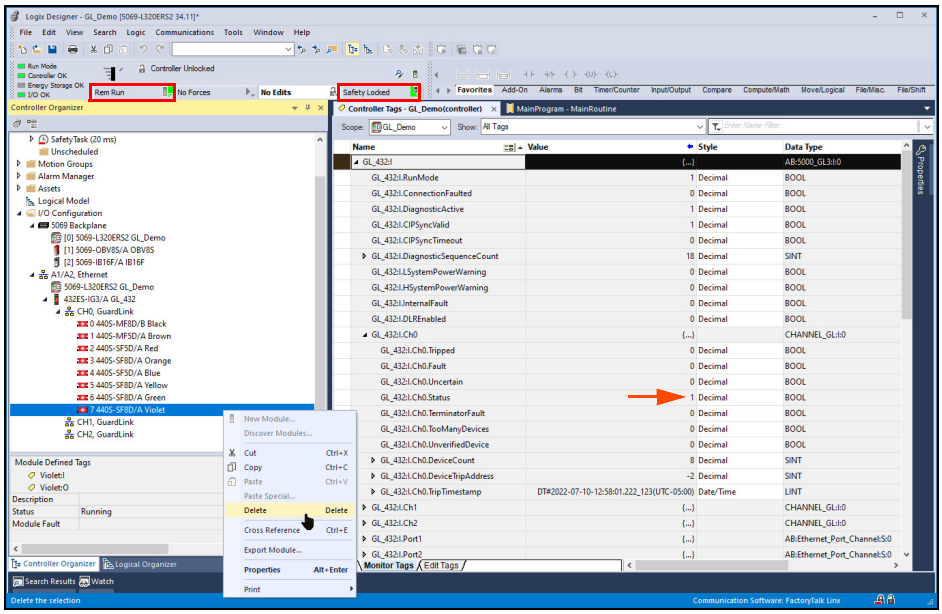
If you remove the last node, you can delete the node with the controller while the host is online. The controller can be Safety Locked or Unlocked.

- If the tags of any node are used in a program routine, perform the change offline and download to the controller. Remove both the node and its associated program lines.
- If no node tags are used in a program routine, consider the position of the node.

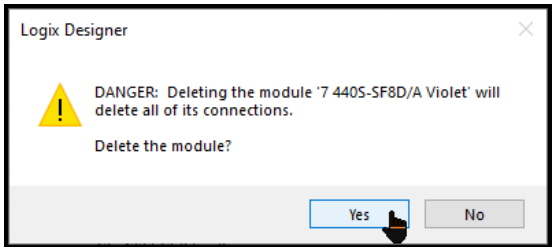
Remove the Last Node

In this example, the program routines do not use any tags from the last node. The controller is online, and Safety Locked. The CH0 Status tag is 1 (in an operational state).

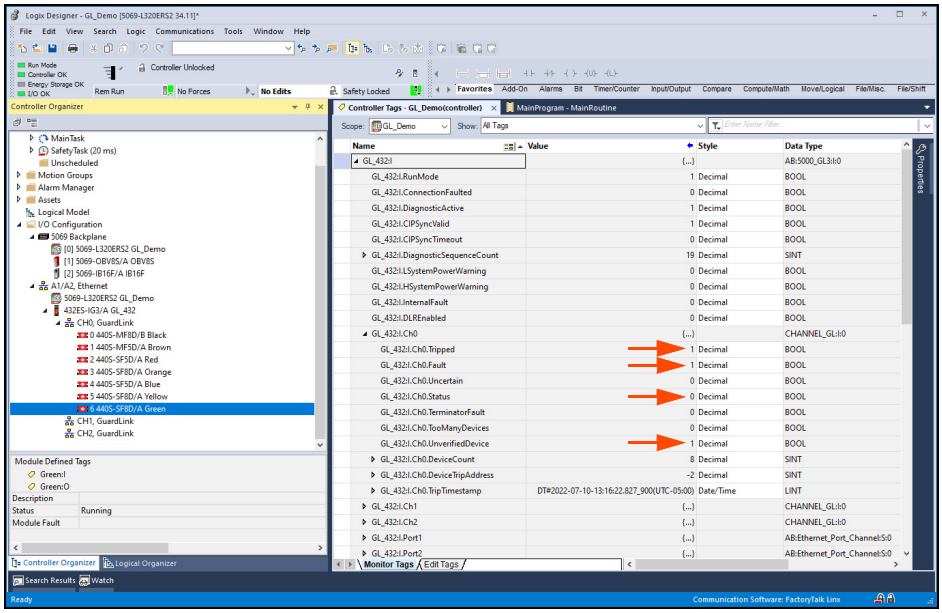
1. Right-click the node and select Delete.



2. Select Yes to confirm the deletion.

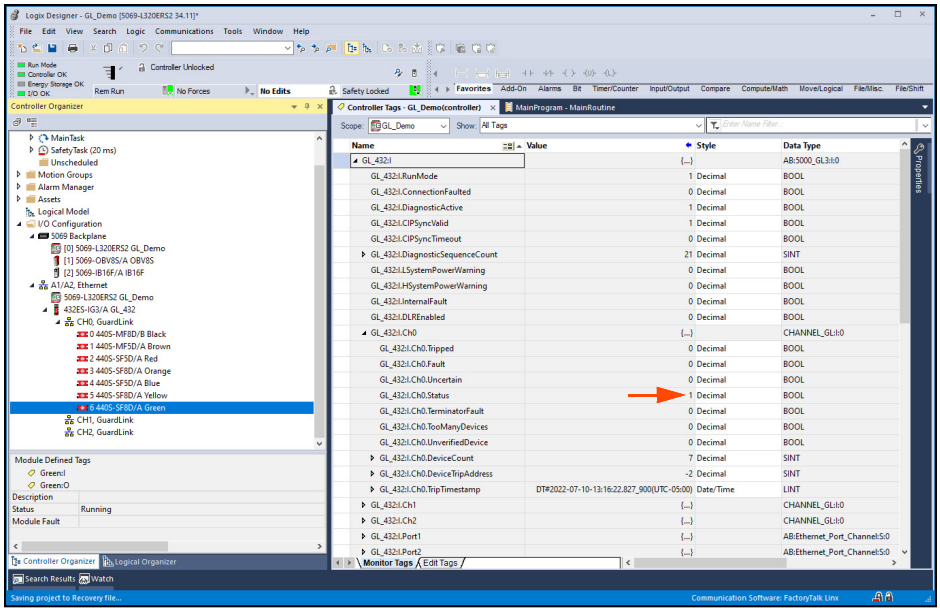


With the node removed, the 432ES-IG3 network interface module detects an unverified device (tag = 1). This change causes the Fault tag to be a value of 1, which causes the Tripped tag to be a value of 1. As a result, CH0 transitions to a safe state; the Status tag shows 0.



3. Remove the node 7 hardware.
   a. Remove the Link In cable to node 6.
   b. Remove the Link Out cable from node 6.
   c. Add the terminator to node 6.
   d. Reconnect the Link In cable to node 6.

Node 6 is now the GuardLink Safety Source. The CH0 Status bit returns to a value of 1 (operational state).



Controller Tags

This chapter contains the controller tags for the GuardLink® system. There are three different AOPs:

- 432ES-IG3 network interface module
- 440S taps
- 440G guard locking switches

Every tap has the same AOP and every guard locking switch has the same AOP.

Interface Input Tags

The following table shows the descriptions of the input tags for the 432ES-IG3 network interface module.

Table 6 - Interface Input Tags

Tag Name	Automatic Diagnostic	Data Type	Description
RunMode	No	BOOL	Indicates whether the 432ES-IG3 network interface module is in Run mode or a faulted state. • 0 = Not in Run mode, or in a fault state (includes recoverable and nonrecoverable faults). When 0, all three SIL 3 channel status bits report as in the safe state. • 1 = Run mode
ConnectionFaulted	No	BOOL	Indicates whether the 432ES-IG3 network interface module has a connection to a controller. The controller sets this bit. • 0 = Connection OK • 1 = No connection
DiagnosticActive	No	BOOL	Indicates whether the 432ES-IG3 network interface module has one or more diagnostics bits set. • 0 = No diagnostics active • 1 = One or more diagnostics codes are present
CIPSyncValid	No	BOOL	Indicates whether the 432ES-IG3 network interface module is synchronized with a 1588 Grandmaster clock. • 0 = Not synchronized • 1 = Synchronized
CIPSyncTimeout	No	BOOL	Indicates whether the 432ES-IG3 network interface module was once synchronized with a 1588 Grandmaster clock but is not now synchronized. • 0 = No timeout • 1 = Timeout has occurred
DiagnosticSequenceCount	No	SINT	Increments for each time a distinct diagnostic condition is detected and each time a distinct diagnostic condition transitions from detected to not detected. Set to zero by a power cycle. Wraps from 255…1, skipping zero. For example, if the 24V supply drops momentarily to 16V and returns to 24V. The diagnostic sequence count increments by 2 (by 1 for the transition to 16V and again by 1 for the transition back to 24V).
LSystemPowerWarning	Yes, M-LOPWR	BOOL	Voltage Too Low: Indicates whether the module power voltage supply is too low, below 20.3V. Increase the voltage to at least 20.4V to clear the warning. • 0 = Voltage not too low • 1 = Voltage too low
HSystemPowerWarning	Yes, M-HIPWR	BOOL	Indicates that the supply voltage level to the interface is too high. The trip point occurs between 27V to 28.3V. The voltage must be reduced to a level between the specified ranged of 20.4V to 26.4V. • 0 = Voltage not too high • 1 = Voltage too high
InternalFault	Yes, M-IFLT	BOOL	• 0 = No internal fault present • 1 = An internal fault is present
DLREnabled		BOOL	Indicates whether the device or port pair is in DLR mode. • 0 = Device is not in DLR mode • 1 = Device is in DLR mode
Ch0	-	CHANNEL_GL:I:0	-
Ch0.Tripped	No	BOOL	• 0 = No devices have demand on safety function • 1 = At least one device has demand on safety function

Table 6 - Interface Input Tags (Continued)

Tag Name	Automatic Diagnostic	Data Type	Description
Ch0.Fault	Yes, CH-FLT	BOOL	Indicates whether the GuardLink channel detects a fault. If the channel is disabled, the fault bit sets to 1. • 0 = Channel fault is not detected; channel has normal data • 1 = Channel fault detected This tag is a roll-up of all diagnostic conditions for this channel. This Fault member triggers both the DiagnosticActive member and increments/decrements the Diagnostic Sequence Count.
Ch0.Uncertain	No	BOOL	Indicates whether the data on the channel is uncertain. • 0 = Data is valid • 1 = Data validity is questionable
Ch0.Status	No	BOOL	Indicates whether the GuardLink channel is operational. This tag is the SIL3/PLe safety bit. • 0 = The channel is in a safe state • 1 = The channel is in an operational state; the safety conditions for each node on the channel are valid.
Ch0.TerminatorFault	Yes, CH-TFLT	BOOL	Indicates whether a faulted terminator is detected at the end of the GuardLink circuit. This fault does not indicate a missing terminator. • 0 = The terminator is present and functions properly • 1 = The terminator does not function properly
Ch0.TooManyDevices	Yes, CH-DEVCNT	BOOL	Indicates whether more than 32 devices are detected on the channel. A missing terminator sets this tag to 1. A break anywhere in the channel Link (trunk) cable sets this tag to 1. • 0 = Number of devices is no more than 32 • 1 = Too many devices found on the channel (greater than 32).
Ch0.UnverifiedDevice	Yes, CH-DEVUNV	BOOL	Indicates that there are client devices that keying did not verify. A missing terminator sets this tag to 1. In FW 2.001 running with 1.0 taps, an open trunk cable generates an unverified device value of 1. This fault can require you to cycle power to the channel to clear the fault. • 0 = All devices have been verified • 1 = Unverified devices present
Ch0.DeviceCount	No	SINT	Indicates the number of client devices (hardware) detected on the channel.
Ch0.DeviceTripAddress	No	SINT	Indicates the client device or event that caused the last transition from the operational to the safe state. • -1 = After power up. • -2 = Shows if the device that caused the trip is not known or if the channel is running protocol 1.0. Examples include an open link cable and a node that cannot respond due to a fault. • -3 = Shows that you sent an unlock command to one or multiple devices while the channel is in operational mode. FW 3.001 (with Output Data set to Safety Data in the Module Definition) shows that you set the LockUnlockEn channel output tag to 1. • -4 = The channel is set to Not Used on the Channels page of the module properties (see Channels Page on page 40). • 0...31 = The non-locking client device that caused the transition. If Node 0 caused the transition, the value is 0. If Node 17 caused the transition, the value is 17. After the first node causes the trip, subsequent device trips do not change the DeviceTripAddress, because the subsequent trips did not cause the Status to transition from 1 to 0.
Ch0.TripTimestamp	No	LINT	Indicates the time stamp of the last transition from an operational to a safe state. The time stamp is updated for all causes, whether the cause was due to a device, an inhibit command, a connection fault, or other cause. In the list of Controller Tags, change the Style to Date/Time to show the value as a date and time. A decimal value of 0, shown as a Date/Time, is DT#1969-12-31-19:00:00.000 (UTC-5:00) - adjusted for your time zone.
Ch1	-	CHANNEL_GL:I:0	See descriptions in Ch0.
Ch2	-	CHANNEL_GL:I:0	See descriptions in Ch0.
Port1	-	AB:Ethernet_Port_Channel:S:1	—
Port1.Fault	Yes, PORT-FLT	BOOL	• 0 = No fault • 1 = Fault present on port, or the port is used but not connected.
Port1.Uncertain	No	BOOL	Indicates whether the data on the port is uncertain. • 0 = Data is valid • 1 = Data validity is questionable
Port1.Connected	No	BOOL	• 0 = The port is not connected • 1 = The port is connected to a network.
Port1.FullDuplex	No	BOOL	• 0 = Half-duplex • 1 = Full-duplex

Table 6 - Interface Input Tags (Continued)

Tag Name	Automatic Diagnostic	Data Type	Description
Port1.AutonegotiationStatus	No	SINT	Indicates the status of link auto-negotiation. • 0 = Auto-negotiation in progress. • 1 = Auto-negotiation and speed detection failed. Using default values for speed and duplex. Default values are product-dependent; recommended defaults are 10 Mbps and half-duplex. • 2 = Auto negotiation has failed but detected speed. Duplex was defaulted. Default value is product-dependent; recommended default is half-duplex. • 3 = Successfully negotiated speed and duplex • 4 = Auto-negotiation not attempted. Forced speed and duplex.
Port1.Speed	No	INT	Network speed. • 10 = 10 Mbps • 100 = 100 Mbps • 1000 = 1000 Mbps (not supported by the 432ES-IG3 network interface module)
Port2	-	AB:Ethernet_Port_Channel:S:1	See descriptions in Port1.
TCPConnections	No	INT	The number of TCP/IP connections currently open to the adapter. This number will change over time, as connections are opened and then closed automatically.
CIPConnections	No	INT	The number of CIP™ connections currently open to and through the adapter. This tag consists of 1 safety connection plus one connection for each used channel. In addition, a channel with over 24 devices use an additional connection. The max number of expected CIP connections is 7.
CIPLostPackets	No	DINT	A running sum of the number of Sequenced Address Item Sequence Numbers that are skipped in Class 0 and Class 1 connections that the adapter and its children consume.
CIPTimeouts	No	DINT	A running count of the number of connections that time out, both originated and targeted, both to and through the adapter.
HMIPacketRate	No	DINT	The number of Class 3 packets and unconnected packets that the device sends and receives in the previous second.
IOPacketRate	No	DINT	The number of class 0 and class 1 packets that the adapter transmits and receives in the previous second.
EthernetErrors	No	DINT	The sum over all ports of the following Ethernet Link object values: In Discards, In Errors, In Unknown Protos, Out Discards, Out Errors, Alignment Errors, FCS Errors, Single Collisions, Multiple Collisions, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC Transmit Errors, Carrier Sense Errors, Frame Too Long, and MAC Receive Errors.
CPUUtilization	No	INT	The percentage of the capacity of the compute engine of the product (whether that is a CPU, a core of a CPU, or a thread) most important to the performance of communication of packets by the product. Due to the variations in communication architectures of various products, each product must define this value that is based on its design.
DLRNetworkState	No	SINT	The current value of the Network Status instance attribute of the DLR object for devices with multiple Ethernet ports that support DLR. Values: • 0 = Normal • 1 = Ring Fault • 2 = Unexpected Loop Detected • 3 = Partial Network Fault • 4 = Rapid Fault/Restore Cycle
DLRSupervisorState	No	SINT	Reports as a DLS supervisor. • 0 = Not a supervisor • 1 = Supervisor
LocalClockOffset	No	LINT	The offset in nanoseconds from the local clock to the system time. This value is useful for the detection of steps in time. This value updates when a PTP update is received.
LocalClockOffsetTimestamp	No	LINT	The time when the Local Clock Offset was most recently sampled. This value is zero and the first-time stamp occurs when the module synchronizes with the Grandmaster clock.
GrandMasterClockID	No	SINT[8]	The EUI-64 Identity of the CIP Sync™ Grandmaster clock to which the module is synced.

Interface Output Tags

The following table shows the descriptions of the output tags for the 432ES-IG3 network interface module. Each channel has a Lock/UnlockEn tag. The Lock/UnlockEn is a safety-rated signal and should be used in a safety task to allow or prevent locking and unlocking commands to be processed by the client devices.

The LockUnlockEn tag is only visible and used when firmware 3.001 is selected and the Output Data is set to Safety Data in the Module Definition.

Table 7 - Interface Output Tags

Tag Name	Automatic Diagnostic	Data Type	Description
LockUnlockEn	No	BOOL	• 0 = Prevents the execution of the lock and unlock commands to the client devices. The channel can transition to an operating state if all the clients are safety satisfied. • 1 = Immediately sets the channel to a safe state and allows the lock and unlock commands to be sent to the client devices.

Tap Input Tags

The following table lists the controller tags of Bulletin 440S GuardLink-enabled taps. The tags that Automatic Diagnostics reports update when the tap is in a safe state.

Table 8 - Tap Input Tags

Tag Name	Automatic Diagnostic	Data Type	Description
RunMode	No	BOOL	• 0 = Not Run mode • 1 = Run mode
ConnectionFaulted	No	BOOL	The device always reports the value as 0. The controller modifies the value. If the connection is faulted, the device cannot report a fault value, therefore the controller sets the value to 1. • 0 = Connection not faulted • 1 = Connection faulted
DiagnosticActive	No	BOOL	• 0 = No diagnostics active • 1 = One or more diagnostic or prognostics thresholds reached
DiagnosticSequenceCount	No	SINT	Increments for each time a distinct diagnostic condition is detected and each time a distinct diagnostic condition transitions from detected to not detected. Set to zero by product reset or power cycle. Upon power-up, the channels are in a fault state until a safety connection is made. Therefore, at least 1 fault always exists after the reset. Wraps from 255 (-1) to 1, zero is skipped.
Pt	-	CHANNEL_DI:I:0	-
Pt.Data	No	BOOL	• 0 = No demand on safety function • 1 = Device has demand on safety function
Pt.Fault	No	BOOL	Indicates whether a fault has occurred within the GuardLink-enabled tap. This tag is a roll-up of all diagnostic conditions for this tap. This fault member triggers both the DiagnosticActive member and increments/decrements the diagnostic sequence count. • 0 = No fault • 1 = Fault present
Pt.Uncertain	No	BOOL	• 0 = Normal data • 1= Uncertain status
DataAux	No	BOOL	Status of the aux pin, reported by FW 2.00x or later. DataAux applies only to 8-pin OSSD taps. • 0 = Aux pin off • 1 = Aux pin on
DataA	No	BOOL	Reported only with FW 2 or later. Reports the status of the Node Channel A. • 0 = Channel A off • 1 = Channel A on
DataB	No	BOOL	Reported only with FW 2 or later. Reports the status of the Node Channel B. • 0 = Channel B off • 1 = Channel B on
InternalFault	Yes, M-IFLT	BOOL	Device requires a reset. To clear the fault condition, send a DeviceReset command. To clear the fault, cycle power to the tap, the channel, or the 432ES-IG3 network interface module. • 0 = No internal fault • 1 = Internal fault
ShortCircuit	Yes, M-SHCI	BOOL	Indicates whether a short circuit between connector pins is present. To clear the fault, cycle power to the tap, the channel, or the 432ES-IG3 network interface module. • 0 = No short circuit • 1 = Short circuit present

Table 8 - Tap Input Tags (Continued)

Tag Name	Automatic Diagnostic	Data Type	Description
GuardLinkSignalFault	Yes, M-SIGFLT	BOOL	Indicates whether the GuardLink safety signal is corrupt, which can be due to electromagnetic interference (EMC). Possible sources include closely coupled cabling, transients on the ground conductor, internal fault on a downstream (higher node number) tap, or other possible causes. To clear the fault, a power system to the 432ES-IG3 network interface module can be required. • 0 = Valid safety signal • 1 = Invalid safety signal
LSystemPowerWarning	Yes, M-LOPWR	BOOL	Input voltage is below the minimum specification. The device can continue to operate. For devices operating at firmware 1, the LSystemPowerWarning is set to 1 if the voltage supply is out of range (high or low). Increase the supply voltage to at least 20.4V and cycle power to the 432ES network interface module to clear the warning. • 0 = No warning • 1 = Voltage supply is below minimum specification
HSystemPowerWarning	Yes, M-HIPWR	BOOL	Indicates that the supply voltage level at the tap is too high. The trip point typically occurs between 27…28.3V. The voltage must reduce to a level between the specified ranged of 20.4…26.4V. For devices operating at firmware 1, the LSystemPowerWarning is set to 1 if the voltage supply is out of range (high or low). • 0 = No warning • 1 = Voltage supply is above specification
DiscrepancyFault	Yes, M-DSCFLT	BOOL	A signal discrepancy between the tap input channels A and B is detected. Check the device wiring and operation. Perform a functional test of the device and confirm consistent performance of the device outputs. This fault typically occurs with mechanically operated contacts and can be cleared by cycling the device. • 0 = No discrepancy warning • 1 = Discrepancy warning

Guard Locking Input Tags

The following table shows unique tags of guard locking switches. The tags that Automatic Diagnostics reports update when the tap is in a safe state.

Table 9 - Guard Locking Input Tags

Tag Name	Automatic Diagnostic	Data Type	Description
RunMode	No	BOOL	• 0 = Not Run mode • 1 = Run mode
ConnectionFaulted	No	BOOL	The device always reports the value as 0. The controller modifies the value. If the connection is faulted, the device cannot report a fault value, therefore the controller sets the value to 1. • 0 = Connection not faulted • 1 = Connection faulted
DiagnosticActive	No	BOOL	• 0 = No diagnostics active • 1 = One or more diagnostic or prognostics thresholds reached
DiagnosticSequenceCount	No	SINT	Increments for each time a distinct diagnostic condition is detected and each time a distinct diagnostic condition transitions from detected to not detected. Set to zero by product reset or power cycle. Wraps from 255 (-1) to 1, zero is skipped.
Pt	-	CHANNEL_DI:I:1	_
Pt.Data	No	BOOL	• 0 = No demand on safety function • 1 = Device has demand on safety function
Pt.Fault	No	BOOL	Indicates whether a fault has occurred within the GuardLink-enabled switch. This tag is a roll-up of all diagnostic conditions for this switch. This fault member triggers both the DiagnosticActive member and increments/decrements the diagnostic sequence count. • 0 = No fault • 1 = Fault present
Pt.Uncertain	No	BOOL	• 0 = Normal data • 1= Uncertain status
DoorClosed	No	BOOL	Status of the door position. For firmware 1, this tag indicates that the door is both closed and locked. For firmware, 2, this tag indicates that the door is closed and ready to lock. • 0 = Door open • 1 = Door closed
DoorLocked	No	BOOL	Status of the lock. For firmware 1, this tag is not used. For firmware, 2, this tag indicates that the door is both closed and locked. • 0 = Can be closed, but is not locked • 1 = Closed and locked
InternalFault	Yes, M-IFLT	BOOL	Device requires a reset; send a DeviceReset command to clear the fault condition or cycle power to the GuardLink device. • 0 = No internal fault • 1 = Internal fault

Table 9 - Guard Locking Input Tags (Continued)

Tag Name	Automatic Diagnostic	Data Type	Description
InvalidActuatorFault	Yes, M-ACTFLT	BOOL	This tag name applies to unique coded locking switches. Verify that the actuator is a unique (not standard) coded actuator that has not been previously taught to this switch. A switch that requires a unique coded actuator cannot validate standard actuators. • 0 = No fault • 1 = Invalid actuator fault
TeachLimitExceeded	Yes, M-ACTLIM	BOOL	This tag name applies to unique coded locking switches. No more learns are allowed. The teach process was locked after the last actuator was taught or the switch has already learned 8 actuators. The eighth actuator remains functional. • 0 = No fault • 1 = Teach limit fault
TeachProcessError	Yes, M-ACTTCH	BOOL	This tag name applies to unique coded locking switches. Actuator moved out of range during teach process. Cycle power to switch and restart the teach process. • 0 = No fault • 1 = Fault
LockDetectionFault	Yes, M-LCKDET	BOOL	During the operational state, the device failed to detect the movement of the internal solenoid-driven locking bolt to the lock position. If installed, check to see if the escape release button has been pressed. We only detect the bolt extended, not retracted. The DiagnosticActive bit is set to 1, and the DiagnosticSequenceCount increments by 1. • 0 = No fault • 1 = Fault
LockingFault	Yes, M-LCKFLT	BOOL	In the safe state, the device attempted to lock or unlock for a specified attempt length, but status input did not indicate the device locked/unlocked. Device failed to lock or unlock. Check for excessive sideload and misalignment. The DiagnosticActive bit is set to 1, and the DiagnosticSequenceCount increments by 1. • 0 = No fault • 1 = Fault
ActuatorDetectionFault	Yes, M-ACTDET	BOOL	During the operational state, the device failed to detect the actuator. The DiagnosticActive bit is set to 1, and the DiagnosticSequenceCount increments by 1. • 0 = No fault • 1 = Fault
ActuatorNotPairedFault	Yes, M-ACTNPR	BOOL	The actuator present is not the actuator that is paired with the switch. The DiagnosticActive bit is set to 1, and the DiagnosticSequenceCount increments by 1. • 0 = No fault • 1 = Fault
TeachDisabled	No	BOOL	Reports whether a guard locking switch has reached its limit of 8 for learning a new actuator, or additional teaches are prevented during configuration. The eighth or the last taught actuator remains functional. • 0 = Additional learns remain • 1 = No more learns allowed
EndOfLifeWarning	No	BOOL	Device has reached 100% of its rated mechanical life. • 0 = End of Life not reached • 1 = End of Life reached
OverTemperature	Yes, M-OTMP	BOOL	• 0 = Temperature does not exceed rated specification • 1 = Temperature exceeds rated specification
UnderTemperature	Yes, M-UTMP	BOOL	• 0 = Temperature not lower than rated specification • 1 = Temperature lower than rated specification
GuardLinkSignalFault	Yes, M-SIGFLT	BOOL	Indicates whether the GuardLink safety signal is corrupt, which can be due to electromagnetic interference (EMC). Possible sources include closely coupled cabling, transients on the ground conductor. • 0 = Valid safety signal • 1 = Invalid safety signal
LSystemPowerWarning	Yes, M-LOPWR	BOOL	Input voltage is below the minimum specification. The device can continue to operate. For devices operating at firmware 1, the LSystemPowerWarning is set to 1 if the voltage supply is out of range (high or low). Increase the supply voltage to at least 20.4V to clear the warning. • 0 = No warning • 1 = Voltage supply is below minimum specification
HSystemPowerWarning	Yes, M-HIPWR	BOOL	Indicates that the supply voltage level at the tap is too high. The trip point typically occurs between 27…28.3V. The voltage must reduce to a level between the specified ranged of 20.4…26.4V. For devices operating at firmware 1, the LSystemPowerWarning is set to 1 if the voltage supply is out of range (high or low). • 0 = No warning • 1 = Voltage supply is above specification

Tap and Guard Locking Output Tags

The following table shows the node output tags. These tags apply to Bulletin 440S GuardLink-enabled taps and Bulletin 440G GuardLink-enabled switches. When a non-guard locking device connects to a tap, the connected device ignores the lock and unlock commands. All devices can execute the ResetDevice.

Table 10 - Node Output Tags

Tag Name	Automatic Diagnostic	Data Type	Description
Lock	No	BOOL	• 0 = Cancels the previous lock command for the client device (does not unlock the device) • 1 = On the transition from 0 to 1, sends a lock command to the client device
Unlock	No	BOOL	• 0 = Cancels the previous unlock command for the client device (does not lock the device) • 1 = On the transition from 0 to 1, sends an unlock command to the client device
ResetDevice	No	BOOL	• 0 = Cancels the previous ResetDevice command for the client device • 1 = On the transition from 0 to 1, sends a power cycle reset command to the client device. Use this command to clear a fault in the client device.

Notes:

Troubleshooting

Diagnostic Status Indicators

The following image and table define the diagnostic status indicators on the 432ES-IG3 network interface module.

Figure 32 - Diagnostic Status Indicators

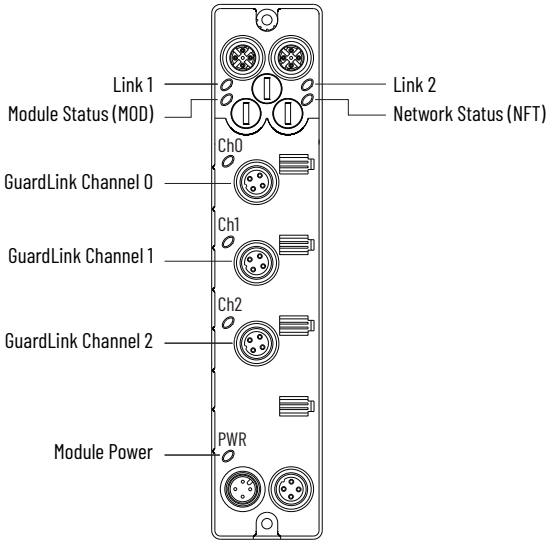


Table 11 - Diagnostic Status Indicators

Indicator	Status	Description
Module status (MOD)	Off	Module is not powered.
	Flashing red/ green	Module is not configured with an IP address, or module is in self-test.
	Flashing green	Module is idle. Waiting for connection from controller.
	Steady green	Module is powered, configured, and operating correctly (Running mode).
	Flashing red	Update in progress (Configuration mode). IP/ Target Unique Network Identifier (TUNID) mismatch - reset ownership with controller. Recoverable fault - cycle power to reset. Special modes: 000 - Disable explicit protection 888 - Restore factory default 900 - Set explicit protection
	Steady red	Unrecoverable fault detected (Critical Fault mode). Cycle the power and verify that the network is working properly.
Network status (NET)	Off	The module does not have an IP address and is operating in DHCP mode. Special modes: 000 - Disable explicit protection 888 - Restore factory default 900 - Set explicit protection
	Flashing green	The module has an IP address, but no CIP™ connections are established. A module connection can be inhibited.
	Steady green	The module has an IP address and CIP connections are established; operating normally.
	Flashing red	An exclusive owner connection has timed out.
	Steady red	The module detected an error that prevents communication on the network, such as a duplicate IP address.

Table 11 - Diagnostic Status Indicators (Continued)

Indicator	Status	Description
LINK1 or LINK2 status	Off	No link/no activity.
	Steady green	Link established.
	Flashing green	Transmit or receive activity.
Ch0...Ch2 status	Off	No GuardLink® communications established. The channel is set to unused and has no client devices connected.
	Green	Channel is in an operational state. Communication OK, operating normally.
	Flashing red/ green	The client is updating on this link. The link is in a safe state.
	Flashing red	• Incorrect configuration. • Short circuit on the link. • Client number mismatch. • GuardLink-enabled device mismatch. • The terminator is not on one of the used GuardLink channels. • A channel is set to unused and has at least one connected client device. • A channel is set to used but does not have a connected client device. • The GuardLink Host adapter is not getting a response from all client devices when establishing the channel at power up. • If the last device to respond to a broadcast message is the same device for 10 consecutive requests. • More than 32 devices on the GuardLink Channel. • Fault on the CLU line. Invalid pattern or short. • The configuration of each client device on the channel does not match expected client device configuration on Studio 5k (AOP). • A GuardLink 1.0 client device is on the host adapter channel 2
	Red	Channel is in Safe mode.
Module power	Off	No power is applied, or severe input power overvoltage.
	Steady green	Normal operation (20.6...26.4V)
	Steady red	Input power out of specification (outside of 20.4...26.4V)

Faults

Faults report at three different levels:

- Controller Organizer faults
- Channel faults
- Node faults

The Studio 5000 View Designer® and Logix Designer application aid in the identification and remediation of faults. See Controller Tags on page 63. The descriptions of each tag can provide insight into the possible causes of a nonoperating condition.

Controller Organizer Faults

The Controller Organizer reports faults with the architectural structure. The controller compares the nodes that connect to each channel compared to the nodes that are listed in the controller tree.

If multiple nodes show faults on a channel, correct the lowest-numbered node first. Occasionally, higher-numbered nodes can show faults due to the lower-numbered faults.

Invalid Link Address

This fault can occur if:

- The node exists in the controller tree, but the hardware is not present.
- The link cable is disconnected at some point in the channel. The controller tree shows that the link is broken between the running node and all nodes that have an exclamation icon (!). If all nodes show an exclamation icon, check the cable between the 432ES network interface module and the first node.
- The terminator is removed from the channel and power is cycled to the channel.

Electronic Keying Mismatch

This fault occurs if major and/or minor revisions are invalid or incorrect. For example:

- You replace a Series A product with a Series B product without changing the Module Definition.
- You replace a tap with another type of tap, such as an 8-pin OSSD replaces an 8-pin EMSS.

Take the channel offline and correct the Module Definition.

Channel Faults

The channel fault bit indicates a channel fault. If the channel fault bit is set to 1, check if other bits are set to 1.

If no other bits show a fault, check the value of the DeviceTrip Address. If the value is -1, then no nodes caused the fault. A disconnected cable or the channel set to Unused can cause the fault.

Node Faults

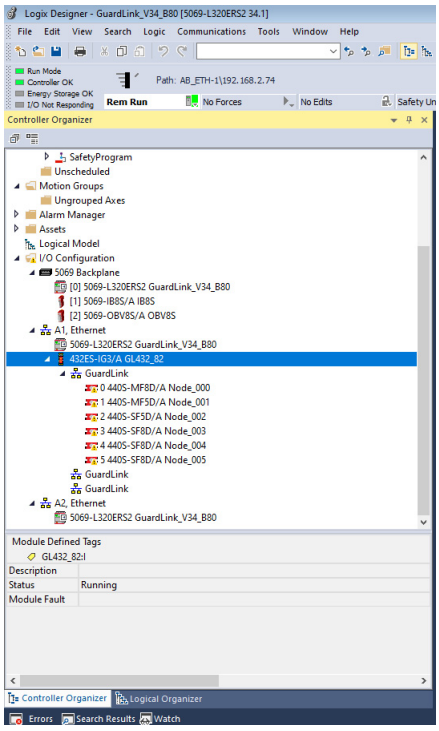
Fault Status Indicators

There are status indicators on the taps, 440G-MZ safety switches, and the network interface module.

If the device status indicators on all taps flash green and the link status indicators show steady red, and the channel status indicator on the 432ES network interface module flashes red, then:

- Hardware nodes are added, but not added to the controller tree.
- The Channels page of the 432ES network interface module shows Unused.

All Nodes Faulted



Review the GuardLink Channel tags in the Controller tags:

- TerminatorFault: 1 (indicates a terminator fault)
- Tripped bit: 1 (set because the Fault bit is 1)
- Status bit: 0 (safe state)
- Fault bit: 1 (fault is present)
- DeviceTripAddress: -1 (none of the nodes caused the fault)
- Terminator bit: 1

Replace the terminator and cycle power to the channel or to the network interface module. The controller recognizes all nodes and removes the fault status.

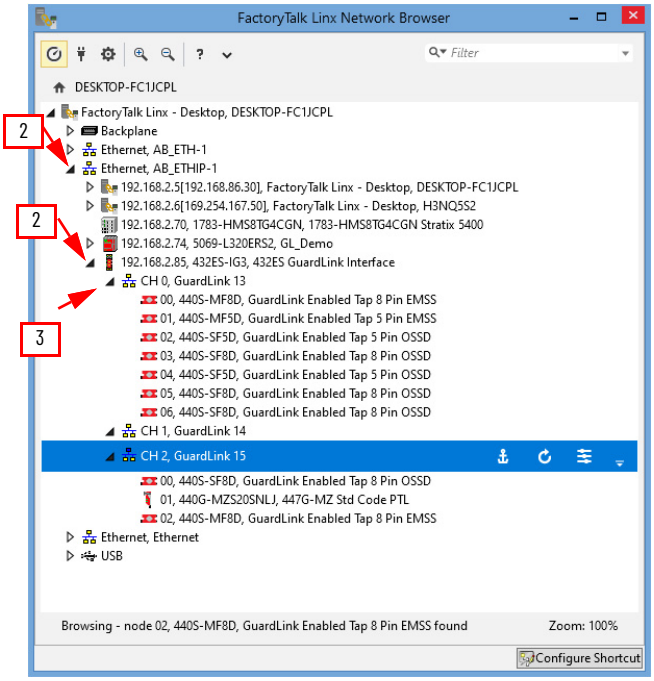
Verify Module Properties

Use the FactoryTalk® Linx Network Browser to verify that devices are on the network, to gather information about the devices, and to upload the EDS file, which gets the proper icon.

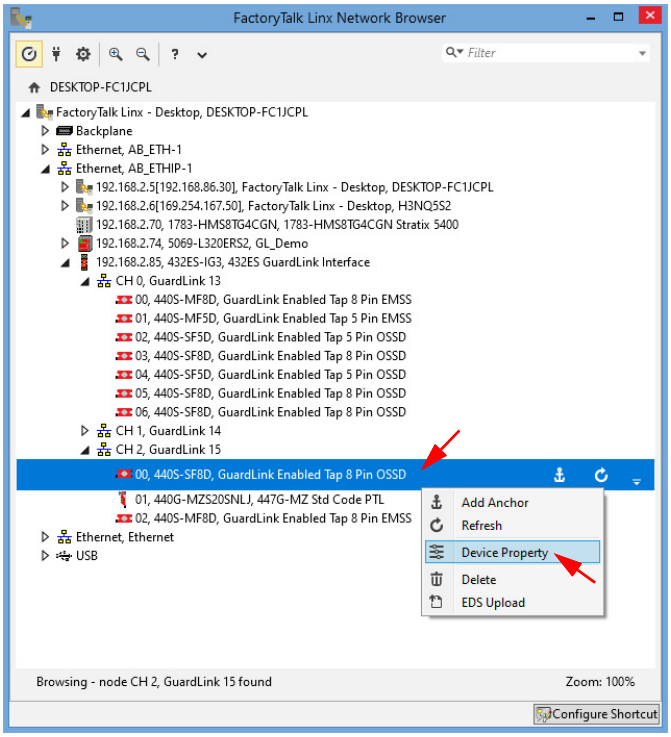
1. On the Start menu, select Rockwell Software® > FactoryTalk Linx Network Browser.
2. Expand the Ethernet node and expand the GuardLink® Interface.
3. Expand each of the GuardLink channels.

   The GuardLink number is sequential and is automatically assigned, based on earlier installations of a GuardLink interface. In the following example, the network browser has three GuardLink channels:

   - CH 0, GuardLink 13 (seven nodes connected)
   - CH 1, GuardLink 14 (zero nodes connected)
   - CH 2 GuardLink 15 (three nodes connected)



4. Highlight a device, right-click, and select Device Property.



The general properties show a GuardLink-enabled tap with firmware revision 2.001. Additional properties will be added in future firmware updates.

Verify Device on the Network

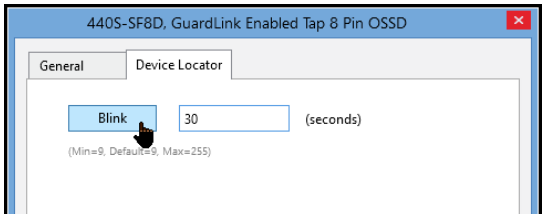
Use the FactoryTalk Linx Network Browser to verify that devices are on the network. This feature is only available when the channel is in a safe state, a demand is placed on the safety system, or a node is inhibited.

This feature only applies to nodes with firmware revision 2 or higher. All devices on the channel must be 2 or higher. If the channel includes a device with firmware 1, the device locator function cannot be used.

To determine the revision level of all devices on a channel, use the Discover Modules feature in the Logix Designer application. Establish the host computer online with the controller, double-click the desired channel, and select Discover Modules. All nodes are listed with their firmware revision.

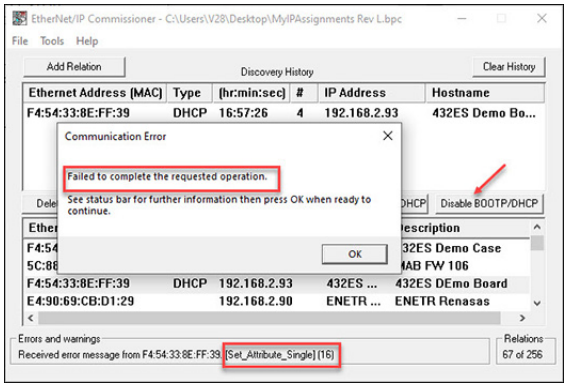
When a channel is in safe state, the Link status indicator is steady red on all nodes (devices). When the Device Locator function is used, the Link status indicator alternates flashing red 0.5 second and green 0.5 second for the specified duration.

The following example shows where the blink duration is adjusted from the default of 9 seconds to 30 seconds. Select Blink to initiate 30 seconds to find the device.



Cannot Disable DHCP

If the 432ES-IG3 network interface module is connected to a Logix controller during configuration, DHCP cannot be disabled. In the EtherNet/IP™ Commissioner window, the communication error is, "Failed to complete the requested operation." [Set_Attribute_Sinlge] (16).



Fix this error in one of two ways:

- Connect the 432ES-IG3 directly to the EtherNet/IP Commissioner (or BOOTP/DHCP tool) or
- Remove the controller from the network.

Then, take the following steps:

1. Reset the 432ES-IG3 with IP address 888 and cycle the power.
2. Return the IP address switches back to 999 and cycle power.

   The EtherNet/IP Commissioner can now be used to set the IP address and disable DHCP. During this process, the Module Status indicator flashes red/green.
3. Connect the Ethernet cables to restore the network.

   After the controller makes the connection, the Module Status indicator changes to steady green.

Specifications

Catalog Number Explanation

Table 12 - 432ES-IG3 GuardLink Network Interface Module

432	E	S	-	I	G	3
a	b	c		d	e	f

a	
Code	**Description**
432	Bulletin number [1]

(1) Safety on-machine module.

b	
Code	**Description**
E	EtherNet/IP

c	
Code	**Description**
S	Safety

d	
Code	**Description**
I	Inputs

e	
Code	**Description**
G	GuardLink input

f	
Code	**Description**
3	Number of input channels

General

Attribute	**Value**			
	Temp/Voltage	**20.4V**	**24V**	**26.4V**
Power supply	24V DC +10/-15%, NEC Class 2, PELV (SELV when alternative ground fault detection is used)			
Power supply cable length, max	30 m (98.42 ft)			
Operating current (typical) [1]	-20 °C (-4 °F)	84 mA	74 mA	68 mA
	25 °C (77 °F)	86 mA	75 mA	70 mA
	60 °C (140 °F)	87 mA	76 mA	71 mA
Safety response time	30 ms			
Communication rate	EtherNet/IP™ 10/100 Mbps			
Internet Protocol	IPv4 addressing			
CIP Sync	CIP Sync™/IEEE 1588 end-to-end transparent clock supported			
CIP Safety™ standards	IEC 61784-3-2: Functional safety fieldbus Additional specifications for CPF 2 according to: • IEC 61158-1: Overview and guidance for the IEC 61158 and IEC 61784 series • IEC 61158-3-2: Datalink layer service definition - Type 2 elements • IEC 61158-4-2: Datalink layer protocol specification - Type 2 elements • IEC 61158-5-2: Application layer service definition - Type 2 elements • IEC 61158-6-2: Application layer protocol specification - Type 2 elements			

(1) Operating with two active Ethernet ports and no GuardLink® connections.

Environmental

Attribute	Value
Operating temperature	-20…+60 °C (-4…+140 °F)
Storage temperature	-40…+85 °C (-40…+185 °F)
Relative humidity	Up to 95%, noncondensing
Pollution degree	3
Emissions	CISPR 11, Group 1, Class A
Enclosure type rating	IP20 with no QD connections IP66, 67, 69K with connectors and the sealed covers installed properly • Covers torque: 0.15 ±0.005 N•m (1.34 ±0.04 lb•in)
Vibration	• 10…57 Hz, 0.762 mm (0.002 in.) • 57…500 Hz, 5.0 g
Shock	• Powered: 30 g, 11 ms • Unpowered: 50 g, 11 ms
ESD immunity	In Operational mode, IEC 61000-4-2 to performance criteria A per IEC 61326-1 • 6 kV contact, 8 kV air discharge In Safe mode, IEC 61000-4-2 to performance criteria DS per IEC 61000-6-7 • 8 kV contact, 9 kV air discharge
Radiated RF immunity	In Operational mode, IEC 61000-4-3 to performance criteria A per IEC 61326-1 • 10V/m with 1 kHz sine wave 80% AM from 80 MHz…2.0 GHz • 10V/m with 200 Hz 50%, pulse 100% AM at 900 MHz • 10V/m with 200 Hz 50%, pulse 100% AM at 1890 MHz • 3V/m with 1 kHz sine wave 80% AM 2.0…2.7 GHz • 3V/m with 1 kHz sine wave 80% AM 2.7…6.0 GHz In Safe mode, IEC 61000-4-3 to performance criteria DS per IEC 61000-6-7 • 20V/m with 1 kHz sine wave 80% AM from 80 MHz…2.0 GHz • 20V/m with 200 Hz 50%, pulse 100% AM at 900 MHz • 20V/m with 200 Hz 50%, pulse 100% AM at 1890 MHz
EFT immunity	In Operational mode only, IEC 61000-4-4 to performance criteria B per IEC 61326-1 • ±3 kV at 5 kHz on power ports • ±3 kV at 5 kHz on Communication ports • ±3 kV at 5 kHz on GuardLink Channel ports
Surge transient immunity	In Operational mode, IEC 61000-4-5 to performance criteria B per IEC 61326-1 • ±500V line-to-line (Differential mode) and +/-1 kV line to Earth (Common mode) on GuardLink ports with 42 Ω source • ±2 kV line to Earth (Common Mode) on communication ports with 42 Ω source In Safe mode, IEC 61000-4-5 to performance criteria DS per IEC 61000-6-7 • ±2 kV line to ground (Common mode) on power ports with 12 Ω source • ±2 kV line to ground (Common mode) on GuardLink ports with 42 Ω source • ±2 kV line to ground (Common mode) on communication ports with 42 Ω source
Conducted RF immunity	In Operational mode, IEC 61000-4-6 to performance criteria A per IEC 61326-1 • 10V rms with 1 kHz sine wave 80% AM from 150 kHz to 80 MHz on all ports In Safe mode, IEC 61000-4-6 to performance criteria DS per IEC 61000-6-7 • 20V rms with 1 kHz sine wave 80% AM from 150 kHz to 80 MHz on all ports
EMC emissions	In Safe mode only, CISPR 11: Group 1, Class A
EMC voltage dips	In Operational mode only, IEC 61000-4-29 to performance criteria DS per IEC 61326-3-1 • Voltage dips; 40% of rated voltage for 10 ms on DC power
EMC magnetic field	In Operational mode only, IEC 61000-4-8 and Volume 2: EtherNet/IP Adaptation of CIP™, edition 1.26, table 8-9.2 • 30 AM, 50 Hz, 60 Hz, 1 min

Certifications and Directives

Agency and Directive Marks

Region/Body	Mark	Description
U.S.A./Canada		UL Listed Industrial Control Equipment that is certified for US and Canada.
United States		ODVA conformance tested to EtherNet/IP™ specifications and CIP Safety™, CIP Sync™, and CIP Security™ requirements.
European Union		CE Marked for all applicable directives.
		Waste Electrical and Electronic Equipment (WEEE) - At the end of its life, this equipment must be collected separately from any unsorted municipal waste.
Australia/New Zealand		RCM: Australian Radiocommunications Act compliant with AS/NZS CISPR 11: Industrial Emissions.
Korea		Korean Registration of Broadcasting and Communications Equipment, compliant with: Article 58-2 of the Radio Waves Act, Clause 3.
United Kingdom		The UK Conformity Assessed mark is used for goods being placed on the market in Great Britain (England, Wales, and Scotland).
Morocco		Mandatory conformity mark for electronics and electrotechnical products.
China		RoHS (Restriction of Hazardous Substances), environment-friendly use period of 25 years.

Declaration of Conformity

CE Conformity

This product is CE marked and is approved for installation within the European Union and EEA regions. This product is designed and tested to meet the European Council Directive 2006/42/EC on machinery and the following standards.

- IEC/EN 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC/EN 62061 - Safety of machinery - Functional safety of safety-related electrical, electronic, and programmable electronic control systems
- EN ISO 13849-1 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

This product is intended for use in an industrial environment. For a comprehensive CE certificate visit rok.auto/certifications.

UKCA Conformity

This product is UKCA marked and is approved for installation within the United Kingdom regions. This product is designed and tested to meet the Supply of Machinery (Safety) Regulations 2008 No. 1597 on machinery and the following standards.

- IEC/EN 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC/EN 62061 - Safety of machinery - Functional safety of safety-related electrical, electronic, and programmable electronic control systems
- EN ISO 13849-1 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

This product is intended for use in an industrial environment. For a comprehensive UKCA certificate visit rok.auto/certifications.

SIL Rating

This product meets the requirements of the safety integrity limit of SIL 3 per IEC/EN 61508. The SIL 3 rating only applies to the GuardLink® safety signal. This product is suitable for use in the IEC/EN 62061 applications up to SIL 3.

Attribute	Rating
SIL (IEC/EN 61508)	3
PFD_{avg} Average probability of a dangerous failure on demand (IEC/EN 61508, not in IEC/EN 62061)	1.95E-04
PFHD [/h] average frequency of a dangerous failure per hour	2.88E-09
Mode of operation	High Demand mode
Safety-related subsystems	Type B (use of programmable / complex components)
Hardware fault tolerance, HFT	1
Safe failure fraction, SFF [%]	95.6

The SIL rating of the lock and unlock command with firmware 3.001 or later:

Attribute	Rating
SIL (IEC/EN 61508)	2
PFD_{avg} Average probability of a dangerous failure on demand (IEC/EN 61508, not in IEC/EN 62061)	2.54E-03
PFHD [/h] average frequency of a dangerous failure per hour	2.97E-08
Mode of operation	High Demand mode
Safety-related subsystems	Type B (use of programmable / complex components)
Hardware fault tolerance, HFT	0
Safe failure fraction, SFF [%]	95

Performance Level/ Category

The Performance Level of the safety function is dependent on the structure of all devices that comprise the safety function.

This product can be used in safety systems that meet up to Category 4 and Performance Level PLe in accordance with ISO 13849-1.

Attribute	Rating
Category	4
Performance Level	PLe (1)
$MTTF_d$ [years]	184
Diagnostic Coverage, DC_{avg} [%]	91.3
Days, d_{op} [days/year]	365
Hours, [hours/day]	24
T [years]	20

(1) Applies to GuardLink safety signal only.

The Performance Level rating of the lock and unlock command with firmware 3.001 or later:

Attribute	Rating
Category	2
Performance Level	PLd
$MTTF_d$ [years]	127.6
Diagnostic Coverage, DC_{avg} [%]	90
Days, d_{op} [days/year]	365
Hours, [hours/day]	24
T [years]	20

EMC Directive

This product is designed and tested to meet the European Council Directive 2004/108/EC on Electromagnetic Compatibility (EMC) and the following standards:

- EN 61000-6-4: Generic Standards - Emission Standard for Industrial Environments
- EN 61000-6-2: Generic Standards - Immunity for Industrial Environments

This product is intended for use in an industrial environment.

Notes:

Safety Statements

CIP Safety Devices

When using CIP Safety™ devices, follow these guidelines:

- To replace safety devices, you must properly configure the replacement device and verify the operation of the replacement device.
- If you choose to configure safety connections with a safety configuration ID (SCID)=0, you are responsible for confirming that the originators and targets have the correct configurations.
- Assign SNN numbers for each safety network or safety subnet that are unique system-wide.
- When a safety device is configured directly from a workstation, compare the transferred SCID and configuration data with the SCID and configuration data that is originally viewed in the workstation.
- You must validate all downloads.
- Only after you have tested the signature is it verified (and configuration locked).
- When you configure an originator with connection data and/or target configuration, download the data to the target so you can test and verify the data. Only after this step is complete, confirm SCIDs from the target.
- Test the operation of a device completely before you set the Lock attribute.
- Clear any pre-existing configuration from any safety device before you install the device onto a safety network.
- Commission all safety devices with MAC ID (and communication rate, if necessary) before you install the device onto a safety network.
- When you implement a safety function, carefully consider the implications of mixing different SIL level devices on the network.
- Test safety connection configurations after they are applied in an originator to confirm that the target connection is operating as intended.

ATTENTION:

- Status indicators are not reliable indicators and cannot be guaranteed to provide accurate information. They must only be used for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators as operational indicators.
- Originators with an automatic SNN setting feature must only use that feature when the safety system is not being relied upon.
- If a Type 1 Safety Open configures a device, verify that all originator-configured safety devices have their ownership assignments as part of the final verification process.
- Visually verify that all configuration data was downloaded correctly.

Notes:

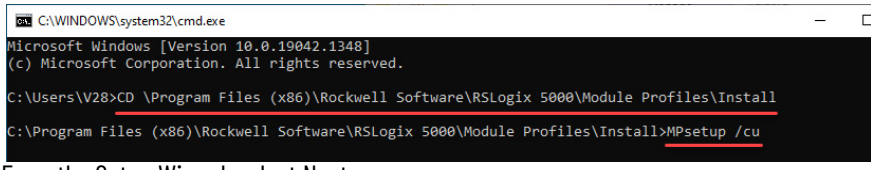
Uninstall the Logix Designer Application Module Profile

Instructions

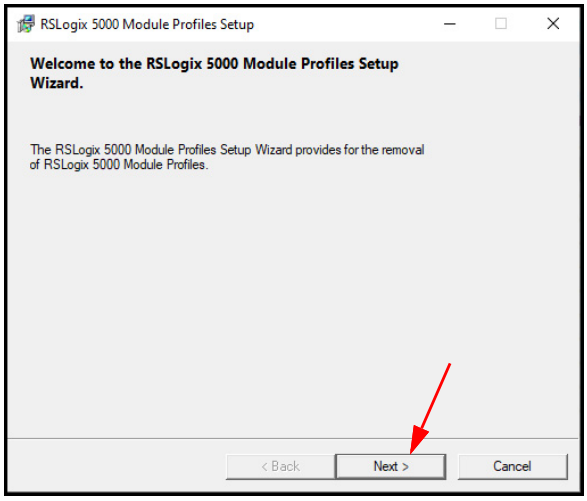
This appendix describes the steps to remove the Module Profile from Studio 5000®.

1. Go to a DoS command prompt.
2. Change the directory to the location of the module profiles. Following is the typical location. Copy and paste this DoS command to the DoS prompt.

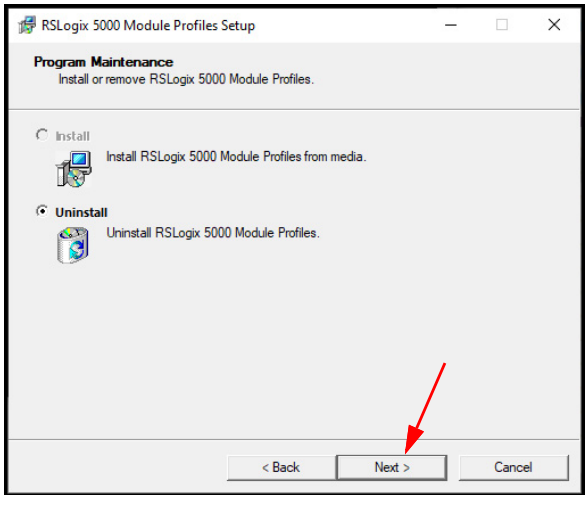
   CD \Program Files (x86)\Rockwell Software\RSLogix 5000\Module Profiles\Install
3. Type the command (MPSetup /cu).



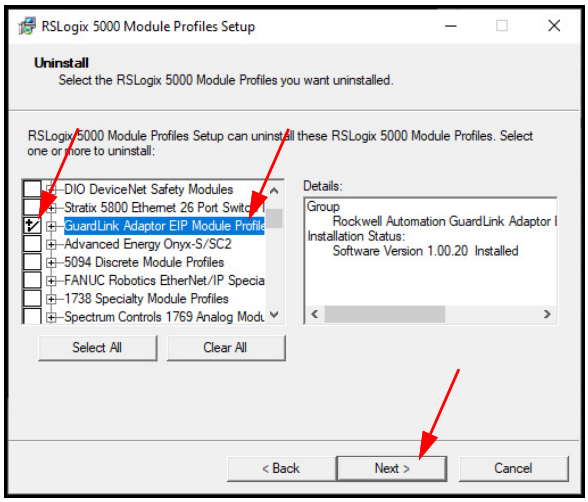
4. From the Setup Wizard, select Next



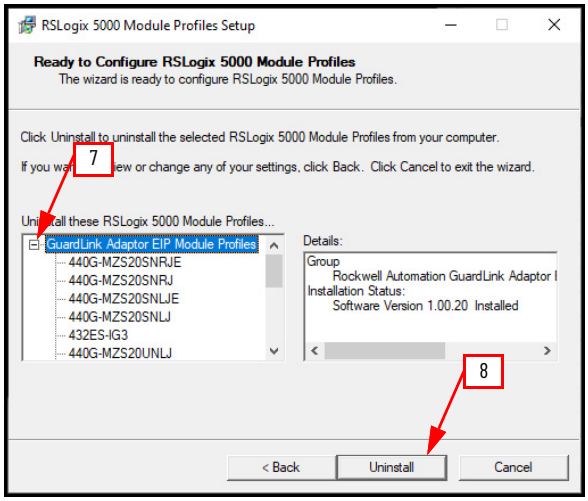
5. Select Next to uninstall.



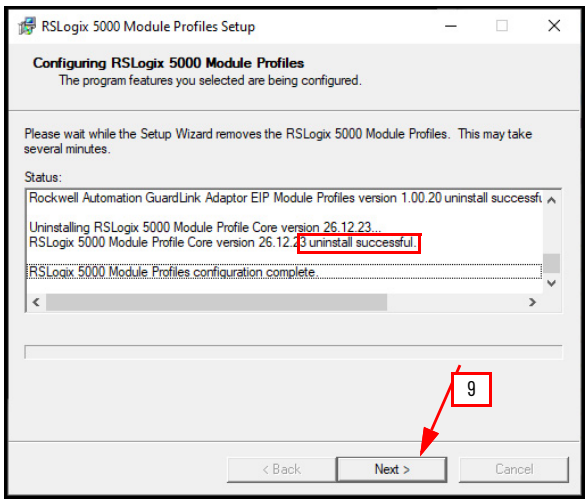
6. Navigate to the GuardLink® Adaptor EIP Module Profile, check the box, and select Next.



7. Expand the GuardLink Adaptor to reveal the list of products to remove. This selection removes the 432ES network interface module and all client devices.
8. Select Uninstall.



9. Uninstall was successful. Select Next.



10. Select Finish in the final window.

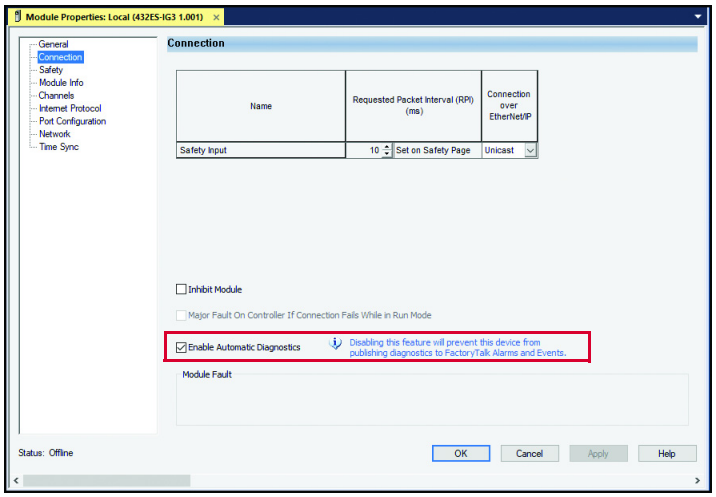
Configure Automatic Diagnostics

On the Controller properties Advanced tab, Enable Automatic Diagnostics is a new feature that was added with the 1756-L8*x* controllers and firmware revision 33. When enabled, it sends analog I/O modules diagnostic information to the Automatic Diagnostics Event Summary object.

If deactivated, you only see Mode changes and loss on communication with controllers in the Automatic Diagnostics Event Summary object.

The automatic diagnostics feature is enabled by default in the Logix Designer application as shown in the following screenshot. The deactivation of automatic diagnostics at the device level deactivates all device-driven diagnostics. You still get device faulted/communication loss diagnostics as the controller drives these diagnostics.

Figure 33 - 432ES Module Properties



Only device Add-on Profiles (AOP) that have been updated with additional diagnostics show the Enable Automatic Diagnostics checkbox (shown in the previous screenshot). You can use this checkbox to verify if the AOP of your device has been updated with additional diagnostics.

IMPORTANT	Application alarms, such as analog input module high/low limit process alarms, are not included.

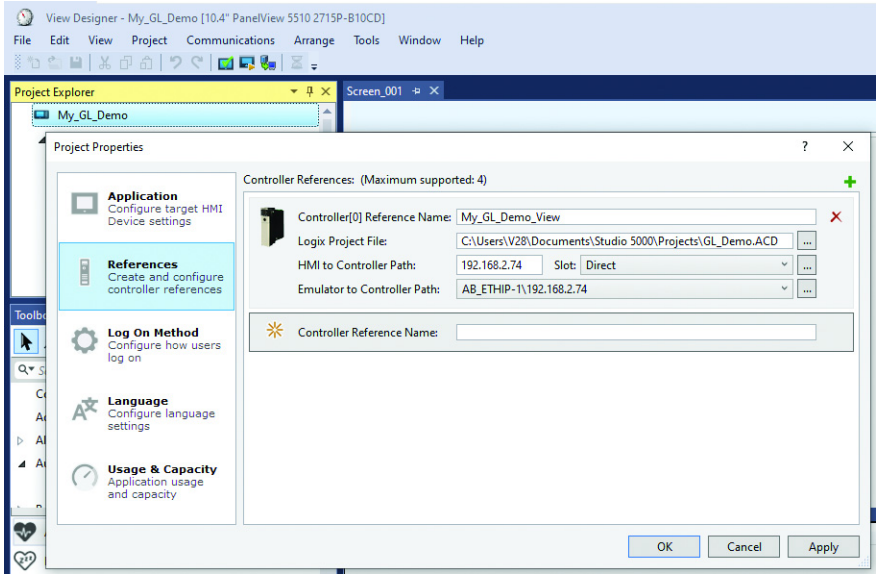
Automatic Diagnostics on PanelView 5000 Display

Automatic diagnostics are enabled by default on all devices. When you use a PanelView™ 5000 display with firmware revision 8 or later, the automatic diagnostic messages from the device display automatically. For more information, see the Automatic Diagnostics chapter in the Studio 5000 View Designer Getting Results Guide, publication 9324-GR001.

When specific events occur, messages automatically report because the controller links to the PanelView 5000 display. In your View Designer project properties, set the Controller References to the controller of the 432ES network interface module (see the following screenshot):

- Logix project File
- HMI to controller
- Emulator to controller path

Figure 34 - Bind Controller to PanelView Project

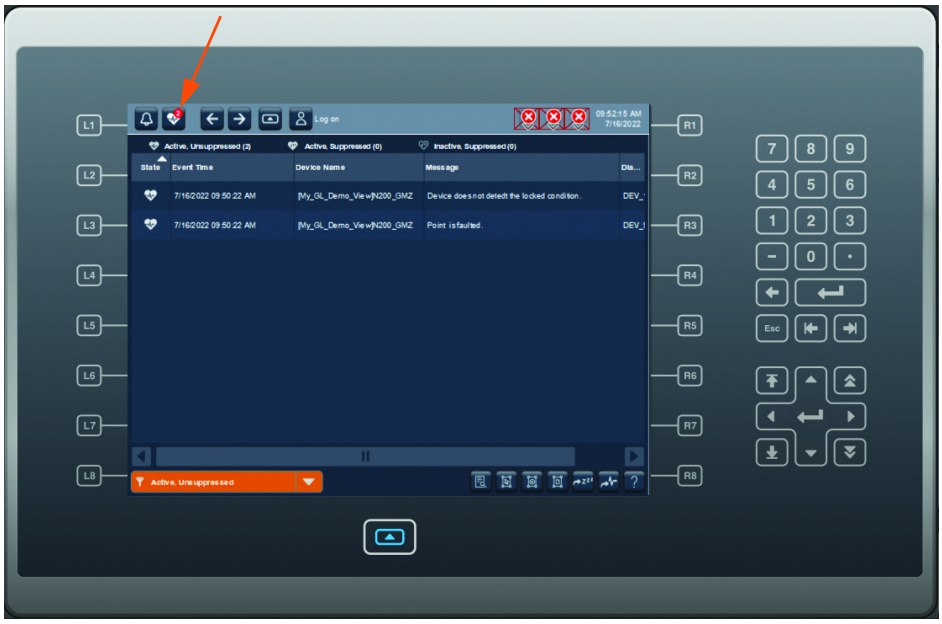


When an event occurs, the diagnostic icon shows the number of active and unsuppressed diagnostic events, as shown in the following screenshot. Each line entry shows:

- State: Active, inactive, or suppressed
- Event Time: Date and time when the event occurred
- Device Name: Path to the device and the device name
- Message: Preprogrammed message for the diagnostic code
- Diagnostic Code: The diagnostic code that applies to the event

IMPORTANT You can rearrange and configure additional columns. See Studio 5000 View Designer® help for more information.

Figure 35 - Diagnostics Page on PanelView 5510



432ES-IG3 network interface modules, Bulletin 440S taps, and 440G-MZ safety switches have unique diagnostic codes that report automatically as shown in the following tables.

Table 13 - 432ES-IG3 Network Interface Module Diagnostics

Display Code	Diagnostic Message
CH-FLT	Channel *x* is faulted.
M-HIPWR	Module has a high system power warning.
M-LOPWR	Module has a low system power warning.
M-IFLT	Module has an internal fault.
CH-TFLT	Channel *x* has a terminator fault.
CH-DEVCNT	Channel *x* exceeds the device count limit.
CH-DEVUNV	Channel *x* has an unverified device.
PORT-FLT	Ethernet port is not connected.

Table 14 - Bulletin 440S Tap and 440G-MZ Safety Switch Diagnostics

Display Code	Diagnostic Message
M-HIPWR	Module has a high system power warning.
M-LOPWR	Module has a low system power warning.
M-IFLT	Module has an internal fault.
M-SHCI	Module has a short circuit or overcurrent condition.
M-ACTFLT	Module has an incorrect actuator inserted.
M-ACTLIM	Module has reached the actuator teach limit.
M-ACTTCH	Module has not completed the teach process with the actuator.
M-LCKDET	Module has a lock detection fault.
M-LCKFLT	Module is unable to lock or unlock as commanded.
M-ACTNDT	Module does not detect the actuator in the closed position.
M-OTMP	Module has an over temperature condition.
M-UTMP	Module has an under temperature condition.
M-DSCFLT	Module has a discrepancy fault.
M-ACTNPR	Module has an actuator not paired condition.
M-SIGFLT	Module has a GuardLink® signal fault.

Notes:

Numerics

A

B

C

D

E

F

G

H

I

K

M

N

O

P

R

S

T

U

W

Notes:

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800

Publication 432ES-UM001D-EN-P - November 2024

Supersedes Publication 432ES-UM001C-EN-P - October 2024