ControlLogix 5580 and GuardLogix 5580 Controllers

Bulletin 1756

Allen-Bradley
by ROCKWELL AUTOMATION

IMPORTANT: This manual links to Logix 5000 Controller and I/O Fault Codes, 1756-RD001; download the spreadsheet now for offline access.

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.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Table of Contents

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.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Preface

This manual provides information to help you design a system, operate a ControlLogix® or GuardLogix®-based controller system, and develop applications.

You must be trained and experienced in the creation, operation, and maintenance of safety systems.

For information on Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012.

The procedures in this manual use the Studio 5000 Logix Designer® application. For information about using FactoryTalk® Design Studio™ software, see the FactoryTalk Design Studio Quick Start, publication FTDS-QS001.

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
Removed CIP Security considerations that do not apply	Manage Controller Communication on page 85
Updated the History of Changes appendix	History of Changes on page 234

Download Firmware, AOP, EDS, and Other Files

You can download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation®. You can view or download publications at rok.auto/literature.

Resource		Description
ControlLogix® 5580 controllers and GuardLogix® 5580 controllers technical documentation.		
Hardware Installation	ControlLogix 5580 Controllers Installation Instructions, publication 1756-IN043	Provides installation instructions for ControlLogix® 5580 controllers.
	GuardLogix 5580 Controllers Installation Instructions, publication 1756-IN048	Provides installation instructions for GuardLogix® 5580 controllers.
	ControlLogix Power Supply Installation Instructions, publication 1756-IN619	Describes how to install standard power supplies.
	ControlLogix Redundant Power Supply Installation Instructions, publication 1756-IN620	Describes how to install redundant power supplies.
	ControlLogix Chassis Installation Instructions, publication 1756-IN621	Describes how to install a ControlLogix® chassis.

Technical Data	1756 ControlLogix Controllers Technical Data, publication 1756-TD001	Provides specifications for ControlLogix® controllers.
	1756 ControlLogix I/O Specifications Technical Data, publication 1756-TD002	Provides specifications for ControlLogix® I/O modules.
	1756 ControlLogix Communications Modules Specifications Technical Data, publication 1756-TD003	Provides specifications for ControlLogix® communications modules.
	1756 ControlLogix Integrated Motion Modules Specifications Technical Data, publication 1756-TD004	Provides specifications for ControlLogix® integrated motion modules.
	1756 ControlLogix Power Supplies Specifications Technical Data, publication 1756-TD005	Provides specifications for ControlLogix® power supplies.
	1756 ControlLogix Chassis Specifications Technical Data, publication 1756-TD006	Provides specifications for a ControlLogix® chassis.
Network	EtherNet/IP Network Devices User Manual, publication ENET-UM006	Describes how to configure and use EtherNet/IP™ devices with a Logix 5000® controller and communicate with various devices on the EtherNet/IP™ network.
Safety application requirements	Logix SIS Safety Reference Manual, publication 1756-RM015	Describes Logix SIS systems, which are type-approved and certified for use in safety applications.
	GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012	Contains detailed requirements to achieve and maintain SIL 2/PLd and SIL 3/PLe with the GuardLogix® 5580 controller system via the Studio 5000 Logix Designer® application.
Design Considerations	Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides information to help design and plan Logix 5000® systems.
	Replacement Guidelines: Logix 5000 Controllers Reference Manual, publication 1756-RM100	Provides information on how to replace earlier generation controllers with controllers in the same family but newer generations, for example, replacing ControlLogix® 5570 controllers with ControlLogix® 5580 controllers.
	High Availability System Reference Manual, publication HIGHAV-RM002	Provides information to help design and plan high availability systems.
	Redundancy System User Manual, publication 1756-UM015	Provides information about how to set up, configure, program, monitor, and troubleshoot high availability systems that use Logix SIS, ControlLogix® 5580, or ControlLogix® 5570 redundancy.
	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.
	OPC UA in 5580 and 5380 Controllers User Manual, publication 1756-UM023	Describes how to implement and use OPC UA communication with ControlLogix® 5580 and GuardLogix® 5580 controllers.
Programming Tasks and Procedures	Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Provides access to the Logix 5000® controllers set of programming manuals. The manuals cover such topics as how to

		manage project files, organize tags, program logic, test routines, faults, and more.
	Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Provides information on the programming instructions available to use in Logix Designer application projects.
	GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information about the GuardLogix® safety application instruction set.
	Advanced Process Control and Drives and Phase and Sequence Instruction Reference Manual, publication 1756-RM006	Provides details about the available General, Motion, Process, and Drives instruction set for a Logix-based controller.
Product Certifications	Product Certifications website, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

Standard and Safety Controller Systems

Standard controllers include:.

Controller Type	Cat. No.
ControlLogix® 5580 controllers	1756-L81E, 1756-L82E, 1756-L83E, 1756-L84E, 1756-L85E
ControlLogix® 5580 controllers with conformal coating	1756-L81EK, 1756-L82EK, 1756-L83EK, 1756-L84EK, 1756-L85EK
ControlLogix® 5580 No Stored Energy (NSE) controllers	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE
ControlLogix-XT™ 5580 controllers	1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT
ControlLogix® 5580 Process controllers	1756-L81EP, 1756-L83EP, 1756-L85EP

Safety controllers include:.

Controller Type	Cat. No.
GuardLogix® 5580 controllers	1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L85ES, 1756-L8SP
GuardLogix-XT™ 5580 controllers	1756-L81EXTS, 1756-L82EXTS, 1756-L83EXTS, 1756-L84EXTS, 1756-L8XTSP
GuardLogix® 5580 controllers with conformal coating	1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8S

Minimum Requirements

The controllers have these minimum requirements:

- ControlLogix® chassis, series C (series B chassis function within a derated temperature range)
- ControlLogix® power supply
- Studio 5000 Logix Designer® software, Linx-based communication software, and ControlFLASH Plus® or ControlFLASH™software

For compatible versions, see the Product Compatibility and Download Center (PCDC).

IMPORTANT:

- If safety components or safety logic are required for your application, then you must use any GuardLogix® controller.
- GuardLogix® project editing requires Studio 5000 Logix Designer® software, Professional, Full Edition, or a licensed GuardLogix® Safety Editor.

IMPORTANT: ControlLogix-XT™ and GuardLogix-XT™ controllers are rated for extreme environmental conditions only when used properly with other system components that share the same extreme-environment ratings. The extreme-environment ratings of ControlLogix-XT™ and GuardLogix-XT™ controllers are nullified when used with other system components that do not share comparable attributes.

EXAMPLE: If the temperature rating found in the Technical Data publication for your GuardLogix-XT™ controller is 70 °C and you pair it with a ControlLogix® chassis that is rated for 60 °C, the system is rated 60 °C

To make sure that your system is equipped for extreme environmental conditions, compare the corrosive atmosphere and temperature ratings in the Technical Data publication for each system component.

IMPORTANT: When a ControlLogix-XT™ or GuardLogix-XT™ controller is used as a replacement for a standard ControlLogix® or GuardLogix® controller, all functional and environmental requirements of the standard controller apply, except for the power output ratings.

Available Controllers

ControlLogix® and GuardLogix® 5580 controllers use Studio 5000 Logix Designer® programming software to establish and maintain control of large industrial automation control systems (IACS).

Working as part of the Integrated Architecture offering, the controllers provide the following:

IMPORTANT: Not all controllers support all of the functionality listed here.

- Support for Integrated Motion over EtherNet/IP™ for high-speed motion applications
- Support for enhanced security, including IEC-62443-4-2 SL 1 certification
- Support for safety solutions
- Support for plantwide process control

ControlLogix-XT and GuardLogix-XT Controllers

The ControlLogix-XT™ and GuardLogix-XT™ controllers function in same way as the traditional ControlLogix® and GuardLogix® controllers, with an extended temperature range, and have the same features as the ControlLogix® standard controllers and GuardLogix® controllers.

The ControlLogix-XT™ and GuardLogix-XT™ controllers are conformal coated to add a layer of protection when exposed to harsh, corrosive environments. While the standard ControlLogix® system can withstand temperatures from 0…60 °C (33…140 °F), the ControlLogix-XT™ system can withstand temperatures from -25…+70 °C (-13…+158 °F).

Process Controllers

The process controller is an extension of the Logix 5000® controller family that focuses on plantwide process control. The process controller comes configured with a default process tasking model and dedicated PlantPAx® process instructions optimized for process applications and that improve design and deployment efforts.

TheControlLogix® process controller hardware is also conformal coated to add a layer of protection when exposed to harsh, corrosive environments, and can be used in temperature extremes from -25…+70 °C (-13…+158 °F) when deployed as part of a Logix-XT system.

ControlLogix No Stored Energy (NSE) Controllers

The NSE controller is intended for use in applications that require the installed controller to deplete its residual stored energy to specific levels before transporting it into or out of your application.

The residual stored energy of the NSE controller depletes to 400 µJ or less in 40 seconds.

If your application requires the NSE controller to deplete its residual stored energy to 400 µJ or less before you transport it into or out of the application, complete these steps before you remove the controller.

1. Turn off power to the chassis.
   After you turn off power, the OK status indicator on the controller transitions from green to solid red to OFF.
2. Wait at least 40 seconds for the residual stored energy to decrease to 400 µJ or less before you remove the controller.
   There is no visual indication of when the 40 seconds has expired. You must track that time period.

IMPORTANT: The Real Time Clock (RTC) does not retain its time and date when power is off.

Some applications require that the installed controller to deplete its residual stored energy to specific levels before transporting it into or out of your application. This requirement can include other devices that also require a wait time before removing them. See the documentation of those products for more information.

Conformal Coated Products

ATTENTION: Conformal Coated Products

Select products that are rated for corrosive atmospheres ship with port plugs, covers, or memory cards installed which provide connectors with a degree of protection in corrosive gas environments. Once the factory packaging seal is broken, plugs or covers must remain installed in all unoccupied ports and memory cards must remain installed for the product to maintain its corrosive atmosphere rating. If temporary access is required, port plugs, covers, memory cards, and so on can be removed, but must be reinstalled after temporary access is complete.

Controller Redundancy

You can use ControlLogix® 5580 controllers in redundant applications with the Studio 5000 Logix Designer® application, version 33 or later.

For information, see these publications:

- High Availability Systems Reference Manual, publication HIGHAV-RM002
- Redundancy Systems User Manual, publication 1756-UM015

ControlLogix 5580 System

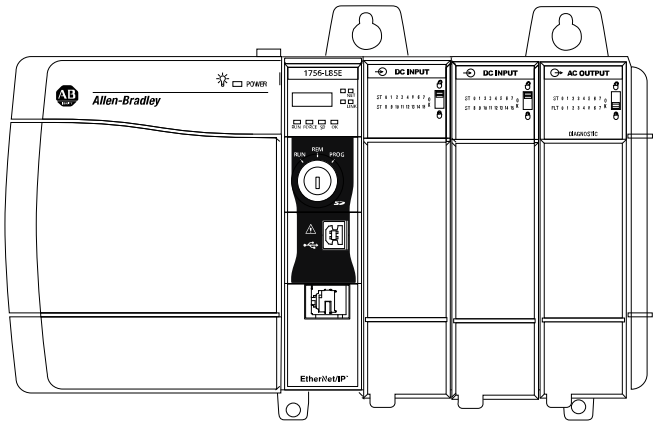
The ControlLogix® system is chassis-based, which provides options for configuring various communications and I/O capabilities. The ControlLogix® controllers support multiple programming languages that enable sequential, process, motion, and drive control.

Various system configuration options are described in the following sections.

Standalone Controller and I/O

One of the simplest controller configurations is a standalone controller with I/O modules residing in one chassis.

Figure 1. Standalone Controller and I/O Modules

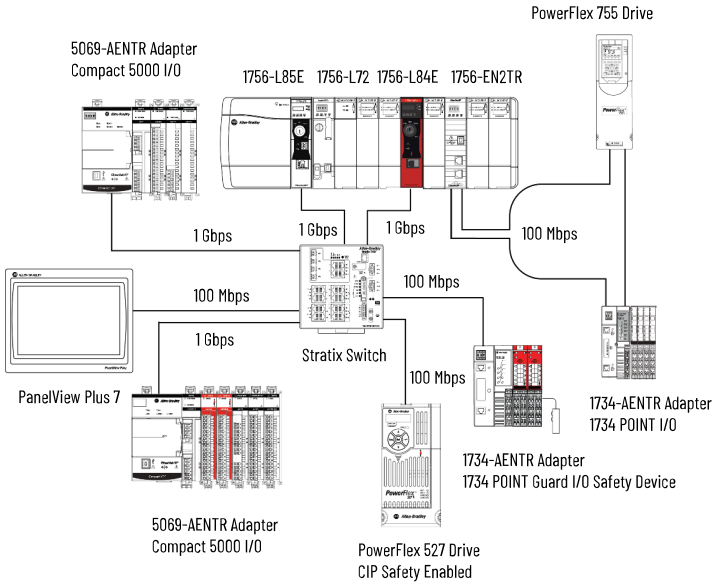


Multiple Controllers in One Chassis

You can use multiple controllers in one ControlLogix® chassis. This example shows the following:

- ControlLogix® 5580 controller (slot 0) connected directly to the EtherNet/IP™ network.
- ControlLogix® 5570 controller (slot 1) connected to the network through a 1756-EN2TR module (slot 7).
- GuardLogix® 5580 controller in a SIL 2/PLd configuration (slot 5) connected directly to the EtherNet/IP™ network.

Figure 2. Multiple Controllers in One Chassis



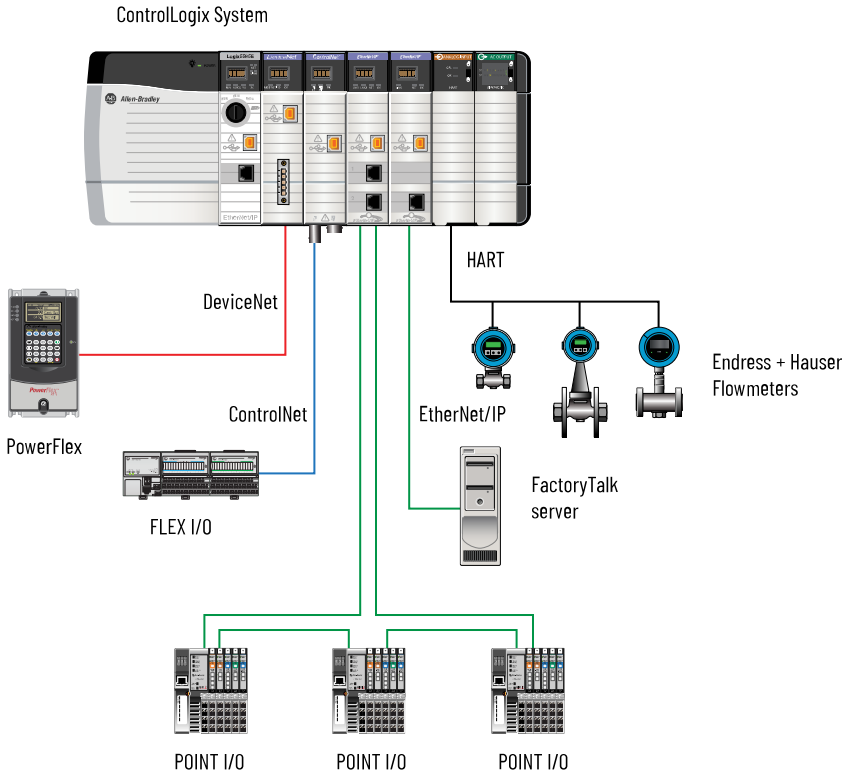
IMPORTANT: You cannot bridge through the Ethernet (front) port of another controller to add remote I/O modules.

Multiple Devices Connected via Multiple Networks

For some applications, various devices can be connected to the ControlLogix® chassis via multiple communication networks. For example, a system can be connected to the following:

- Distributed I/O via an EtherNet/IP™ network •
- A PowerFlex® drive connected via a DeviceNet® network
- Distributed I/O via a ControlNet® network
- Flowmeters that are connected via a HART connection

Figure 3. Multiple Devices Connected Via Multiple Networks



GuardLogix System

The GuardLogix® system can communicate with safety I/O devices via CIP Safety™ over an EtherNet/IP™ network (Guard I/O™ modules, integrated safety drives, integrated safety components).

The GuardLogix® controller, can interface with local standard and safety I/O via the backplane and interface with standard and safety I/O via the front Ethernet port.

For standard tasks, GuardLogix® controllers support:

- Ladder Diagram (LD)
- Structured Text (ST)
- Function Block Diagram (FBD)
- Sequential Function Chart (SFC)

For the safety task, GuardLogix controllers support Ladder Diagram only.

The GuardLogix® system supports up to SIL 3 and PLe safety applications.

- Without a safety partner installed, you can achieve SIL 2/PLd (Category 3) with the use of the safety task and safety I/O.
- With the use of the safety task and a safety partner that is installed, you can achieve SIL 3/PLe (Category 4) capability.

For SIL 3 safety applications, the GuardLogix® system is composed of a primary GuardLogix® controller and a safety partner that function together in a 1oo2 architecture.

- The primary controller is the processor that performs standard and safety functions and communicates with the safety partner for safety-related functions in the GuardLogix® control system.
- The safety partner is a co-processor that provides an isolated second channel for safety-related functions in the system. The safety partner does not have a keyswitch or communication port. The primary controller controls the configuration and operation of the safety partner.
- The safety partner must be installed in the slot immediately to the right of the primary controller. The firmware major and minor revisions of the primary controller and safety partner must match exactly to establish the control partnership that is required for safety applications

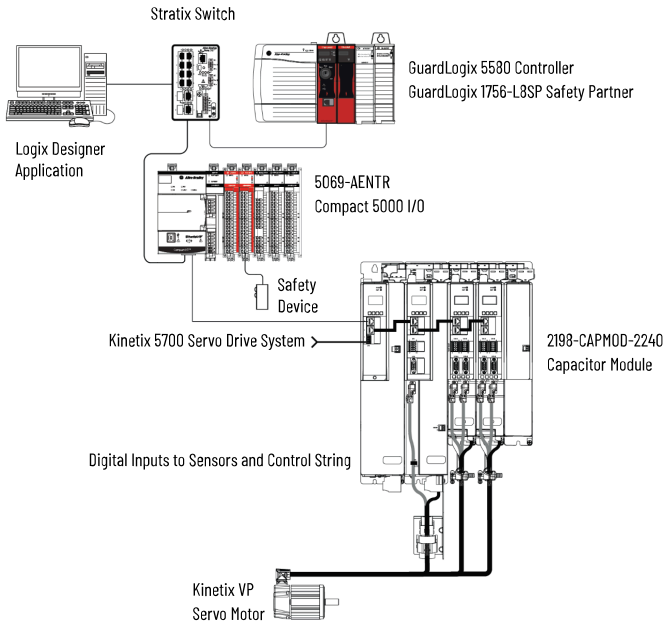
For information on Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements, see the GuardLogix® 5580 and Compact GuardLogix® 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

GuardLogix with Safety I/O and Integrated Safety Drives

In the following example, a GuardLogix® safety controller makes the Motion and Safety connections.

IMPORTANT: If only one controller is used in an application with Motion and Safety connections, it must be a safety controller such as the GuardLogix® 5580 controller.

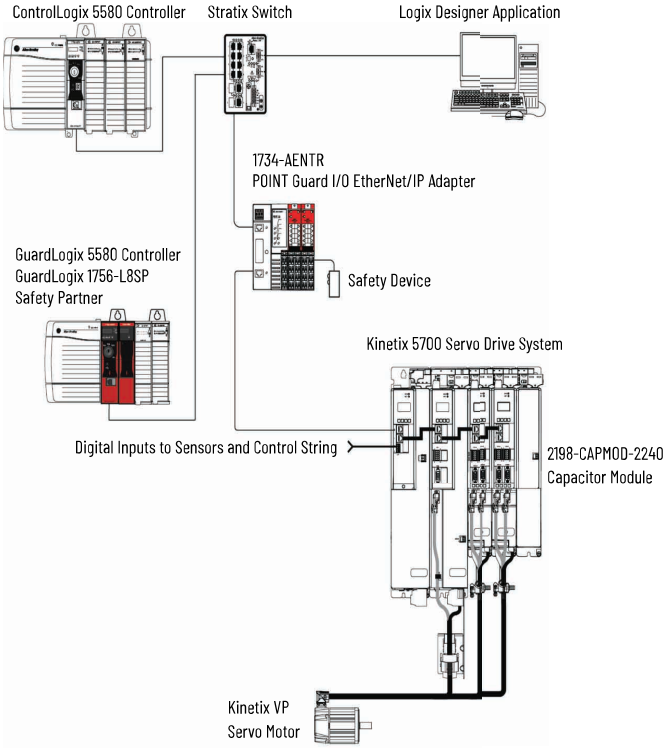
Figure 4. Motion and Safety Configuration (Single Controller)



In the following example, a standard controller makes the motion-only connection and a separate GuardLogix® 5580 controller makes the safety-only connection.

IMPORTANT: If two controllers are used in an application with motion-only and safety-only connections, the safety-only connection must be a GuardLogix® controller while either a standard or safety controller can make the motion-only connection.

Figure 5. Motion and Safety Configuration (Multiple Controllers)



Item	Description
A	Motion program—Module definition configured with Motion Only connection
B	Safety program—Module definition configured with Safety Only connection

Logix SIS

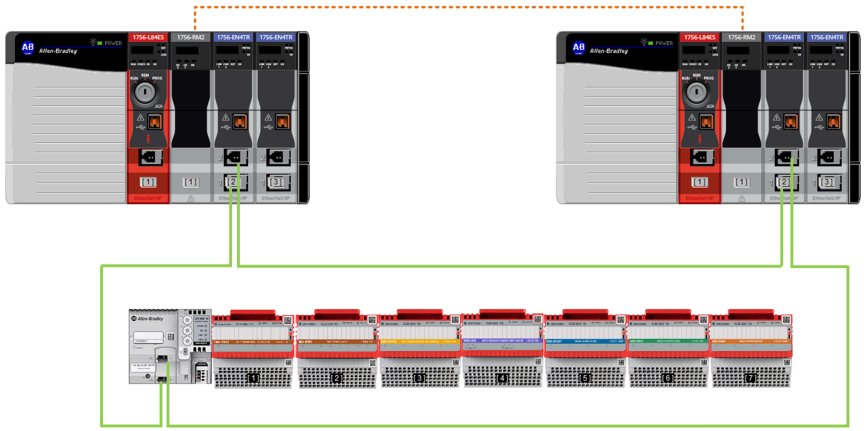
Logix SIS redundancy is designed for safety applications that require high availability. Logix SIS uses redundant safety controllers to provide continuous operation after a single- channel fault. You can also use redundant safety controllers to execute standard tasks with no safety function. Redundancy operation for standard tasks within a safety controller is the same as ControlLogix® redundancy.

In Logix SIS, redundant safety controllers execute tasks as follows:

- Both controllers simultaneously execute the safety task to maintain operation
- Only the primary controller executes standard tasks

For more information, see the Logix SIS Safety Reference Manual, publication 1756-RM015.

Figure 6. Logix SIS Redundancy



SIL 2 and SIL 3 Safety Functions

Logix SIS can achieve SIL 2/3 safety ratings. To support a SIL 3 safety function, redundant SIL 2 controllers must operate together. If one controller fails, the system must be repaired within your mean repair time (MRT).

If redundant operation is interrupted, the primary safety controller operates as a SIL 2, single-channel controller, and the secondary safety controller no longer participates in the safety function. Standard tasks continue to operate.

System Qualification and Synchronization

When the redundant system is first started, the redundancy modules run checks on the chassis. They check if both chassis have the correction modules and firmware. Additionally, they confirm that a safety application exists in the primary safety controller in a safety-protected state.

This stage of checks is referred to as qualification. During qualification, the primary safety controller transfers the safety application and safety signature, if one exists, to the secondary safety controller. After the redundancy modules complete qualification, synchronization takes place between the primary and secondary safety controllers.

Design the System

When you design a a system, there are several system components to consider for your application:

- I/O devices
- Motion control axes and drives
- Communication modules
- Controllers
- Chassis
- Power supplies
- Studio 5000 Logix Designer Application

In addition, safety systems also have components to consider:

- Safety Controller
- Safety Partner (for SIL 3/PLe applications)
- Safety I/O
- Safety Devices

For more information to design and select components for your system, see the following:

- 1756 ControlLogix Controllers Technical Data, publication 1756-TD001
- 1756 ControlLogix I/O Specifications Technical Data, publication 1756-TD002
- GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012

Secure Controller Systems

ControlLogix® 5580 controllers, firmware revision 32.011 or later, and GuardLogix® 5580, firmware revision 37.011 or later, support IEC-62443-4-2 SL 1 requirements. For security features and system requirements, see Develop Secure Applications on page 148.

CIP Security

CIP Security™ is a standard, open-source communication mechanism that helps to provide a secure data transport across an EtherNet/IP™ network. CIP Security™ lets CIP™-connected devices authenticate each other before transmitting and receiving data.

CIP Security™ uses the following security properties to help devices protect themselves from malicious communication:

- Device Identity and Authentication
- Data Integrity and Authentication
- Data Confidentiality

Rockwell Automation uses the following products to implement a CIP Security™ solution:

- FactoryTalk® Policy Manager software (includes FactoryTalk® System Services)
- FactoryTalk® Linx software (lets workstation software communicate securely using CIP Security™)
- Studio 5000 Logix Designer® application (This application required to interface with CIP Security™-enabled Logix controllers. The minimum application version varies by controller product family.)

See the requirements for your products to verify the correct product versions for your solution.

For more information on CIP Security™, for example, a list of CIP Security™-capable products and publications that describe how to use the products, including limitations and considerations, see the following:

- Rockwell Automation Industrial Cybersecurity Solutions
- CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001 (describes the CIP Security™-capable products, minimum software versions and product firmware revisions, and publications that describe how to use the products)

ControlLogix 5580 Controller Features

The following table lists the system, communication, and programming features that are available with ControlLogix® 5580 controllers.

Features	1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP
User Memory	3 MB	5 MB	10 MB	20 MB	40 MB
EtherNet/IP™ nodes supported (A node is an EtherNet/IP™ device that you add directly to the I/O configuration and counts toward the controller node limits.)	60 nodes (Logix Designer application, version 29) 100 nodes (Logix Designer application, version 30 or later)	80 nodes (Logix Designer application, version 29) 175 nodes (Logix Designer application, version 30 or later)	100 nodes (Logix Designer application, versions 28 and 29) 250 nodes (Logix Designer application, version 30 or later)	150 nodes (Logix Designer application, version 29) 250 nodes (Logix Designer application, version 30 or later)	300 nodes (Logix Designer application, version 28 or later)
Communication ports	1 - USB port, 2.0 full-speed, Type B 1 - EtherNet/IP™ port: 10 Mbps, 100 Mbps, 1 Gbps link speeds				
Communication options	• EtherNet/IP™ • ControlNet® • DeviceNet® • DH+™ • Remote I/O • SynchLink™ • Third-party process and device networks				
Controller tasks	• 32 tasks • 1000 programs/task • Event tasks: all event triggers				
Integrated motion	• Integrated Motion on the EtherNet/IP™ network • Sercos interface (Logix Designer application version 31 or later) • Analog options (Logix Designer application version 31 or later.): - Encoder input - Linear displacement transducer (LDT) input - Serial Synchronous Input (SSI)				
Programming languages	• Ladder Diagram (LD) • Structured Text (ST) • Function Block Diagram (FBD) • Sequential Function Chart (SFC)				

GuardLogix 5580 Controller Features

The following table lists the system, communication, and programming features that are available with GuardLogix® 5580 controllers.

Feature	1756-L81ES, 1756-L81ESK, 1756-L81EXTS	1756-L82ES, 1756-L82ESK, 1756-L82EXTS	1756-L83ES, 1756-L83ESK, 1756-L83EXTS	1756-L84ES, 1756-L84ESK, 1756-L84EXTS	1756-L85ES (Supported by Logix Designer application version 36 or later)
User Memory	3 MB	5 MB	10 MB	20 MB	40 MB
Safety Memory	1.5 MB	2.5 MB	5 MB	6 MB	3 MB
EtherNet/IP™ nodes supported (A node is an EtherNet/IP™ device that you add directly to the I/O configuration and counts toward the controller node limits.)	100	175	250	250	300
Communication ports	1 - USB port, 2.0 full-speed, Type B 1 - EtherNet/IP port: 10 Mbps, 100 Mbps, 1 Gbps link speeds				
Communication options	• EtherNet/IP™ (1756-EWEB cannot be used for safety connections) • Support for Network Address Translation (NAT) • ControlNet® • DeviceNet® • DH+™ • Remote I/O • Third-party process and device networks				
Controller tasks	• 31 standard tasks, 1 safety task • 1000 programs/task • Event tasks: all event triggers				
Integrated motion	Integrated motion is supported in standard task only. • Integrated Motion on the EtherNet/IP™ network • Sercos interface • Analog options: - Encoder input - Linear displacement transducer (LDT) input - Serial Synchronous Input (SSI)				
Programming languages	• For the safety task, GuardLogix® controllers support Ladder Diagram only. • For standard tasks, GuardLogix® controllers support: - Ladder Diagram (LD) - Structured Text (ST) - Function Block Diagram (FBD) - Sequential Function Chart (SFC)				
Integrated safety	• Integrated safety on the EtherNet/IP™ network (Kinetix® drives, PowerFlex® drives, safety components) • Distribute and control safety I/O (over EtherNet/IP™ and DeviceNet® networks only) • Produce and consume safety tag data.				
Controller Features	• Data access control • Firmware Supervisor • Secure Digital (SD) card				

Feature	1756-L81ES, 1756-L81ESK, 1756-L81EXTS	1756-L82ES, 1756-L82ESK, 1756-L82EXTS	1756-L83ES, 1756-L83ESK, 1756-L83EXTS	1756-L84ES, 1756-L84ESK, 1756-L84EXTS	1756-L85ES (Supported by Logix Designer application version 36 or later)
	• Safety Connections • Standard Connections				

Features Supported by GuardLogix 550 Controllers via the Safety Task

In the Logix Designer application, version 31 or later, the Safety task supports a subset of features that are supported in the standard task as listed in the following table.

Feature	Studio 5000 Logix Designer®, Version 31 or later	
	Safety Task	Standard Task
Add-on instructions	X	X
Instruction-based alarms and events	–	X
Tag-based alarms	–	X
Controller logging	X	X
Event tasks (While the safety task cannot be an Event task, standard Event tasks can be triggered with the use of the Event instruction in the safety task.)	–	X
Function block diagrams (FBD)	–	X
Integrated motion	X (Limited to the use of Drive Safety Instructions with Kinetix® 5700 ERS4 drives.)	X
Analog motion	–	X
Sercos motion	–	X
Drive Safety Instructions	X	–
Ladder Diagram (LD)	X	X
Language switching	X	X
License-based source protection	–	X
Online import of program components	–	X

Feature	Studio 5000 Logix Designer®, Version 31 or later	
	Safety Task	Standard Task
Online export of program components	X	X
Sequential function chart (SFC) routines	—	X
Structured Text (ST)	—	X

IMPORTANT: Safety Consideration

GuardLogix® 5580 controllers can produce standard tags as unicast or multicast, but they can only produce safety tags as unicast. The controllers can consume safety tags as either unicast or multicast.

When you configure a produced safety tag, you are only allowed to configure unicast connection options. Logix Designer application does not allow you to configure multicast connection options.

When you configure a consumed tag, you must consider the capabilities of the producer:

- If the producer in the I/O tree of this controller is a GuardLogix® 5580 or Compact GuardLogix® 5380 controller, and you are consuming a safety tag, you must configure the consumed tag to use unicast.
- If the producer in the I/O tree of this controller is a GuardLogix® 5570 or 5560, or a Compact GuardLogix® 5370, the safety consumed tag can be configured as either unicast or multicast.
- GuardLogix® 5580 controllers do not produce safety tags to GuardLogix® 5570 (firmware revision 30 or earlier) controllers in the same chassis, because GuardLogix® 5580 controllers can only produce safety tags as unicast, and GuardLogix® 5570 (firmware revision 30 or earlier) controllers cannot configure consumed tags as unicast. This restriction does not apply over EtherNet/IP™, as consumed tags can be configured for unicast.

GuardLogix Functional Safety

The GuardLogix® 5580 controller system is certified for use in safety applications up to and including SIL 2/PLd and SIL 3/PLe where the de-energized state is the safe state:

- For SIL 3/PLe safety applications, the GuardLogix® system is made up of a primary controller and a safety partner that function together in a 1oo2 architecture.
- For SIL 2/PLd and SIL 3/PLe safety system requirements, including functional validation test intervals, system reaction time, and PFD/PFH calculations, see 1756-RM012.

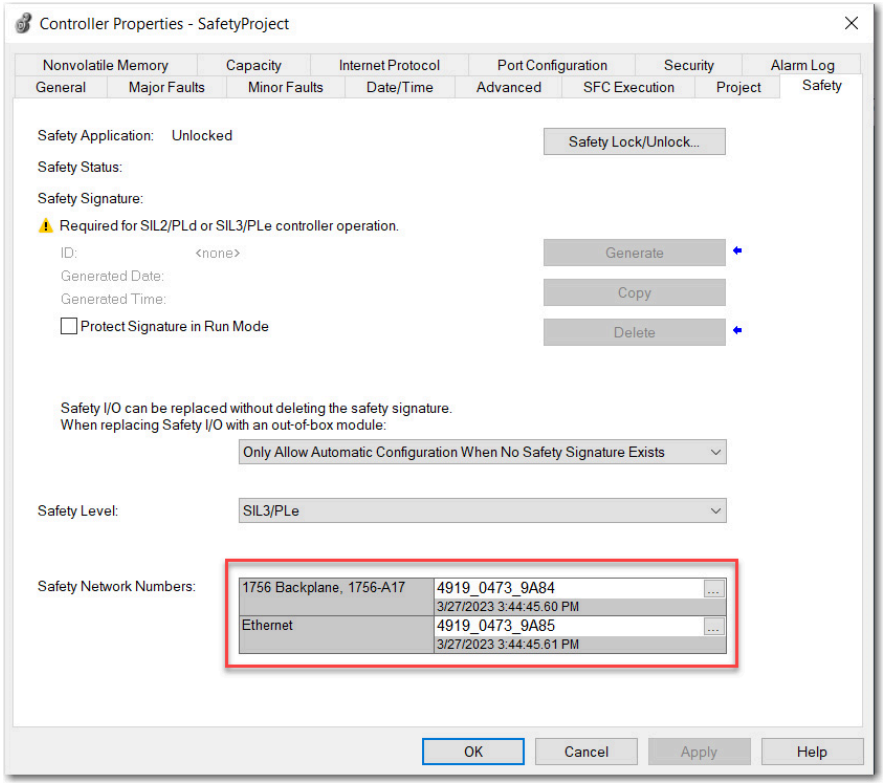
You must read, understand, and fulfill these requirements before you operate a GuardLogix® SIL 2/PLd or SIL 3/PLe safety system.

Safety Network Number

The safety network number (SNN) uniquely identifies CIP Safety™ subnets within a routable safety network. The combination of the SNN + Node Address uniquely identifies each CIP Safety port on each device in the routable safety network. Safety controllers require two SNNs:

- An SNN for the backplane
- An SNN for the Ethernet port

Figure 7. Safety Network Numbers



Safety Network Number Assignment

When you create controller projects, the Studio 5000 Logix Designer® application generates an SNN value automatically whenever it recognizes a new subnet that contains CIP Safety™ devices:

- Each CIP Safety™-capable port on the controller is assigned an SNN. The GuardLogix® 5580 controllers have two safety network numbers: one for the Ethernet port, and one for the backplane.
- If a bridge or adapter device is in the I/O tree and a child CIP Safety™ device is added, the subnet that is created by the bridge or adapter is assigned an SNN.

For typical users, the automatic assignment of a time-based SNN is sufficient. However, manual assignment of the SNN is required if the following is true:

- One or more controller ports are on a CIP Safety™ subnet that already has an established SNN.
- A safety project is copied to another hardware installation within the same routable CIP Safety™ system.

We recommend changing each SNN to the SNN already established for that subnet, if one exists. That way, devices created later in the project are automatically assigned the correct SNN.

For information regarding whether the controller or Ethernet ports are being added to existing subnets, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012.

Each safety network must have a unique safety network number. You must be sure that a unique SNN is assigned to each CIP Safety network that contains safety devices.

Multiple safety network numbers can be assigned to a CIP Safety™ subnet or a ControlBus™ chassis that contains multiple safety devices. However, for simplicity, we recommend that each CIP Safety™ subnet has only one unique SNN.

The SNN can be software-assigned (time-based) or user-assigned (manual).

For more information on time-based assignment, see Automatic Assignment of Time-based Safety Network Number on page 52. For more information on manual assignment, see Manual Assignment of Safety Network Number on page 53.

Safety Signature

A safety signature verifies the integrity of a safety application:

- The safety signature applies to the entire safety portion of the controller project. The ability to create, record, and verify the safety signature is a mandatory part of the safety-application development process. The safety signature must be present to operate as a SIL 2/PLd or SIL 3/PLe safety controller. Nothing in the standard application is included in the safety signature.
- The safety signature is a hierarchy of multiple safety signature elements. For example, the safety task, programs, and routines are examples of safety signature elements. Safety signature elements can help you during impact analysis by identifying the individual changes within a controller project. If your validation plan does not require revalidation of unchanged elements, your certification effort can be reduced.
  All safety signature elements are created at the time that you generate the safety signature for the project. To view all safety signature elements for a project, you can run the Safety Signature report.

The safety signature and each of its elements have the following:

- Safety signature—IDA unique 64-character alphanumeric identification number.
- Time stamp—The date and time that the safety signature was generated. For a safety signature element, the time stamp changes whenever its signature ID changes. The time stamp is based on the local clock of the computer that generated the signature.

Figure 8. Safety Signature

Safety ID	DCA0ACF6 - 4A899D32 - A9ABCAF3 - C2FFA9C0 - 21B47338 - 855266DE - 8D05DB32 - 44DAAE06
Safety Updated	08/23/2023 12:29:41.076 PM

Distinguish between Standard and Safety Components

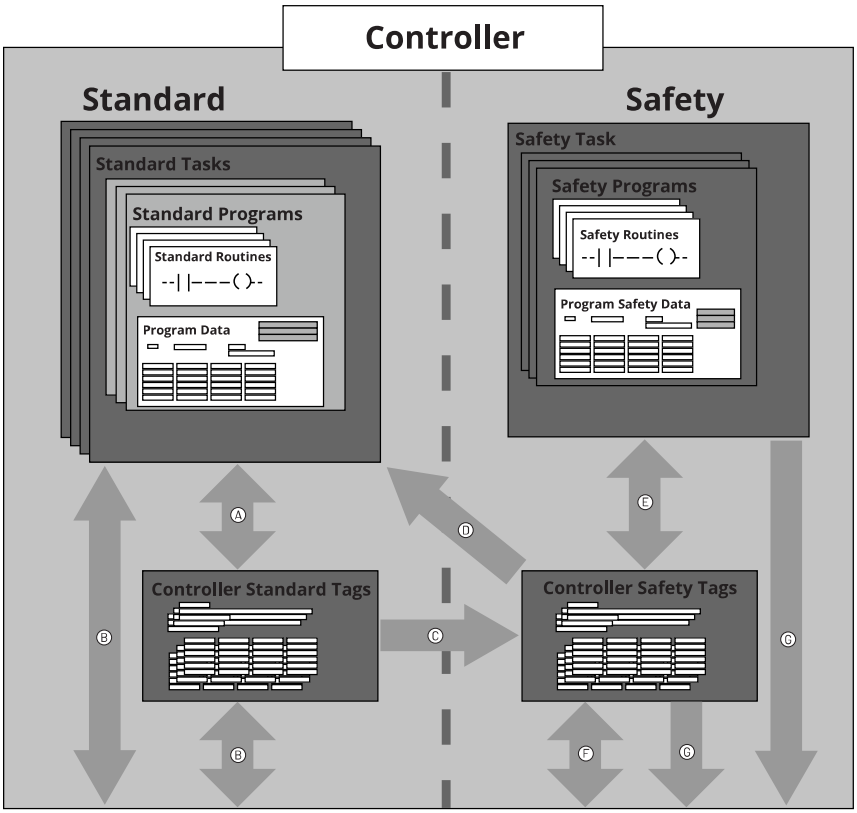
Components of a safety system that are not used by the safety function can be populated with other modules that are certified to the Low Voltage and EMC Directives. See the Rockwell Automation Product Certifications page (rok.auto/certifications) to determine that the modules have the CE certificate.

You must create and document a clear, logical, and visible distinction between the safety and standard portions of the controller project. As part of this distinction, the Studio 5000 Logix Designer® application features safety identification icons to identify the safety task, safety programs, safety routines, and safety components.

In addition, the Logix Designer application uses a safety class attribute that is visible whenever safety task, safety programs, safety routine, safety tag, or safety Add-On Instruction properties are displayed.

Controller Data Flow Capabilities

Figure 9. Controller Data-flow Capabilities



Item	Description
A	Standard tags and logic behave the same way that they do in a standard controller.
B	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.
C	Controllers with safety functions are integrated controllers with the ability to move (map) standard tag data into safety tags for use within the safety task. This is the only way to get standard tag data into the safety task. Safety logic in the safety task cannot read or write the standard tag that is the source in the tag mapping data transfer; it can only reference the safety tag destination of the mapping. But, it can read and write that safety tag. **ATTENTION**: Mapped tag data does not have SIL rated safety integrity. Safety functions requiring a rating of SIL 2 or SIL 3 must use appropriately rated safety inputs.
D	Controller-scoped safety tags can be read directly by standard logic.
E	Safety tags can be read or written by safety logic.
F	Safety tags can be exchanged between safety controllers over Ethernet or ControlNet networks.
G	Safety tag data, program- or controller-scoped, can be read by external devices, such as HMI devices, personal computers, or other standard controllers. External devices cannot write to safety tags (whether the controller is protected or not). Once this data is read, it is considered standard data, not SIL 3/PLe data.

Safety Terminology

This table defines safety terms that are used in this manual.

Table 1. Safety Terms and Definitions

Abbreviation	Full Term	Definition
1oo1	One Out of One	Identifies the programmable electronic controller architecture. 1oo1 is a single-channel system.
1oo2	One Out of Two	Identifies the programmable electronic controller architecture. 1oo2 is a dual-channel system.
CIP Safety	Common Industrial Protocol - Safety Certified	SIL 3/PLe-rated version of CIP™.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.

Table 1. Safety Terms and Definitions (continued)

Abbreviation	Full Term	Definition
SIL	Safety Integrity Level	A relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction.
SIL CL	SIL Claim Limit	The maximum safety integrity level (SIL) that can be achieved.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
UNID	Unique Node ID (also called unique node reference)	The unique node reference is a combination of a safety network number (SNN) and the node address of the node.

Connect to the Controller

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

- The controller has an Ethernet port that supports 10 Mbps, 100 Mbps, or 1 Gbps.
- The controller has a USB port that uses a Type B receptacle. The port is USB 2.0 compatible and runs at 12 Mbps.
- Install and configure a communication module in the chassis with the controller as described in the installation instructions for the communication module.

The EtherNet/IP™ driver:

- Supports runtime communications
- Requires that the workstation and the controller are configured
- Supports communications over longer distances when compared to the USB driver

USB driver:

- Convenient method to connect to an unconfigured controller and configure the Ethernet port
- Convenient method to connect to a controller when the Ethernet port configuration is unknown
- Convenient method to update the controller firmware
- Not intended for runtime connections; it is a temporary-use only connection with a limited cabling distance

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

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

- The controllers ship without an IP address.
- The controller is DHCP-enabled. That is, the controller 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 manually.

To set the IP address, have the following:

- EtherNet/IP™ or USB drivers that are 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

Methods to Set the IP Address

The controller supports the following methods to change the IP address:

- BootP/DHCP EtherNet/IP Commissioning Tool
- FactoryTalk® Linx software
- Studio 5000 Logix Designer®application

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

Duplicate IP Address Detection

The controller verifies that its IP address does not match any other network device IP address when you perform either of these tasks:

- Connect the module to a EtherNet/IP™ network.
- Change the controller IP address.

If the controller IP address matches that of another device on the network, the controller EtherNet/IP™ port transitions to Conflict mode. In Conflict mode, these conditions exist:

- Network (NET) status indicator is steady red.
- The 4-character display indicates the conflict.
  The display scrolls: <IP_address_of_this_module> Duplicate IP

  <Mac_address_of_duplicate_node_detected>

  For example: 192.168.1.1 Duplicate IP - 00:00:BC:02:34:B4

Duplicate IP Address Resolution

When two devices on a network have IP addresses that conflict, the resolution depends on the conditions in which the duplication is detected. This table describes how duplicate IP addresses are resolved.

For more information on how to assign IP addresses, see the EtherNet/IP™ Network Device User Manual, publication ENET-UM006.

Duplicate IP Address Detection Conditions	Resolution Process
• Both devices support duplicate IP address detection. • A second device is added to the network after the first device is operating on the network.	1. The device that began operation first uses the IP address and continues to operate without interruption. 2. The device that begins operation second detects the duplication and enters Conflict mode. To assign a new IP address to the controller and leave Conflict mode, set the network IP address with the BootP/DHCP EtherNet/IP Commissioning Tool.
• Both devices support duplicate IP address detection • Both devices were powered up at approximately the same time.	Both EtherNet/IP devices enter Conflict mode. To resolve this conflict, follow these steps: 1. Assign a new IP address to the controller. Set the network IP address with the BootP/DHCP EtherNet/IP Commissioning Tool. 2. Cycle power to the other device.
One device supports duplicate IP address detection and a second device does not	1. Regardless of which device obtained the IP address first, the device that does not support IP address detection uses the IP address and continues to operate without interruption. 2. The device that supports duplicate IP address detection detects the duplication and enters Conflict mode. To assign a new IP address to the controller and leave Conflict mode, set the network IP address with the BootP/DHCP EtherNet/IP Commissioning Tool.

DNS Addressing

You can also use DNS addressing to specify a host name for a controller, a domain name, and DNS servers. DNS addressing makes it possible to configure similar network structures and IP address sequences under different domains.

IMPORTANT: Safety Considerations

Safety connections are not allowed to use host names (this requires DNS lookup, which is not allowed for Safety I/O).

- Safety devices on EtherNet/IP™ networks (such as a safety-enabled controller in a safety project) do not present the host name parameter.
- Standard devices (not safety enabled) do present the host name parameter, regardless of whether the project is safety or standard. When used in a standard project, the only connections are standard consumed tags, so the controller presents the host name parameter.

DNS addressing is necessary only if you refer to the controller by host name, such as in path descriptions in MSG instructions.

To use DNS addressing, follow these steps.

1. Assign a host name to the controller.
   A network administrator can assign a host name. Valid host names must be IEC-1131-3 compliant.
2. Configure the controller parameters.
3. Configure the IP address, subnet mask, gateway address, a host name for the controller, domain name, and primary/secondary DNS server addresses.
   In the DNS server, the host name must match the IP address of the controller.
4. In the Logix Designer application, add the controller to the I/O configuration tree.

   IMPORTANT: Remember the following:
   - If a child module resides in the same domain as its parent module, type the host name. If the domain of the child module differs from the domain of its parent module, type the host name and the domain name (hostname.domainname).
   - You can also use DNS addressing in a module profile in the I/O configuration tree or in a message path. If the domain name of the destination module differs from the domain name of the source module, then use a fully qualified DNS name (hostname.domainname). For example, to send a message from EN2T1.location1.companyA to EN2T1.location2.companyA, the host names match, but the domains differ. Without the entry of a fully qualified DNS name, the module adds the default domain name to the specified host name.

Firmware Upgrade Guidelines for Safety Controllers

IMPORTANT: You cannot update a controller that is safety-locked.

The IEC 61508 functional safety standard requires impact analysis before you upgrade or modify components in a certified, functional safety system. This section provides high-level guidance on how you can perform the impact analysis for safety controller hardware/firmware upgrades. Reference the standard to make sure you fulfill all requirements as they relate to your application.

When you upgrade controller firmware to a newer version, consider the following:

- All major and minor firmware releases for safety controller systems are certified for use in safety applications. As part of the certification process, Rockwell Automation® tests the safety-related firmware functions, such as the CIP Safety™ communication subsystems, embedded safety instruction execution, and safety-related diagnostic functions. The firmware release notes identify changes to safety-related functions.

- Perform an impact analysis of the planned firmware update:
  - Review of the firmware release notes for changes in safety-related functionality.
  - Review of hardware and firmware compatibility in the Product Compatibility and Download site to identify potential compatibility conflicts.
  - Any modification or enhancement of your validated software must be planned and analyzed for any impact to the functional safety system as described in the 'Edit Your Safety Application' section in the safety reference manual for your controller.
- You must remove and regenerate the safety signature as part of the firmware update process.

IMPORTANT: When updating firmware revisions, the safety logic compiler can change. You must validate that the application compiles correctly when making firmware revisions.

For product change management guidelines and product version management definitions, see System Security Design Guidelines Reference Manual, publication SECURE-RM001.

For example:

1. From the Product Compatibility and Download Center;
   a. Review all firmware release notes, starting with the original firmware revision through the new firmware revision, to identify any changes that impact the safety- related implementation of the application.
   b. Review hardware and firmware compatibility to identify any restrictions between the original system components and the new system components.
2. Perform a hazard and risk assessment for any changes that are identified during the impact analysis and determine what additional testing is necessary.
3. Perform the online and offline edit process that is described in the safety reference manual for your controller. You can restrict the 'Test the Application' block to the testing identified by the hazard and risk assessment.

Controller Firmware and Logix Designer Application Compatibility

In Logix 5000® control systems, the controller firmware and the Studio 5000 Logix Designer® application must be of the same major revision level. For example, if the controller firmware revision is 38.xxx, you must use the Logix Designer application, version 38.

There are minimum software version requirements for the software applications that you use in your system.

Compatible builds of software have been tested together to verify they work properly. Versions of software that are not identified as being compatible with each other have not been tested together and are not guaranteed to work.

For more information on controller firmware revisions and software application minimum requirements, go to the Product Compatibility and Download Center (PCDC) at rok.auto/pcdc.

In the PCDC:

- The Download section has the firmware for your controller.
- The Compare section has software compatibility information for software applications that are used in a control system.

IMPORTANT: The controller must be in Remote Program or Program mode and all major recoverable faults must be cleared to accept updates.

The controller ships with firmware revision 1.xxx installed. You must update the firmware revision before you can use it in a Logix Designer application project.

IMPORTANT: Safety Consideration

For a safety system that includes a Safety Partner (SIL 3/PLe only), the firmware on the primary controller and safety partner must match. When you update the firmware on the primary controller, the safety partner updates automatically.

Obtain Controller Firmware

You can obtain controller firmware in these ways:

- Install the Studio 5000 Logix Designer® application and use the packaged firmware.

IMPORTANT: The firmware that is packaged with the software installation is the initial release of the controller firmware. Subsequent firmware revisions to address anomalies can be released during the life of a product.

We recommend that you check the Product Compatibility and Download Center (PCDC) to determine if later revisions of the controller firmware are available

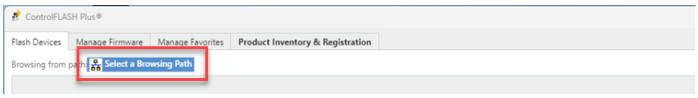
- From the PCDC, download revisions of controller firmware, and download controller firmware, associated files, and product release notes.
  ControlFLASH Plus® software version 2.00.00 or later provides integration with PCDC for an enhanced experience while you browse for firmware revisions, downloads, release notes, and access to important notices.

Visit the Product Compatibility and Download Center (PCDC) at rok.auto/pcdc.

Use ControlFLASH Plus Software to Update Firmware

Use ControlFLASH Plus® software to flash firmware revisions on one or more devices. You browse to the devices from the Flash Devices tab and select the network path.

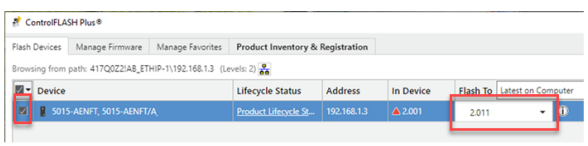
- Click Select a Browsing Path button to set up the browsing path on the network.
- If a path is already established, click Select Browsing from Path.



The network browser shows the devices in your system.

The following steps show how to select devices and firmware.

1. In ControlFLASH Plus® software, select the device, select the firmware revision as shown in the following example, and click Next to confirm.



If a firmware revision needs to be downloaded from the Product Compatibility and Download Center, the Download Center License Agreement dialog box opens, and you follow the prompts to download the firmware revision.

2. If the updated screen shows the correct selections, click Flash.
3. When a dialog box prompts you to confirm whether to trust the publisher of a DMK during the update, you must trust it to continue.
4. When the operation completes, click Close.
   If necessary, click Retry to flash devices whose flash operations have failed or were canceled.

NOTE: For more details on how to use ControlFLASH Plus®, see the online help or ControlFLASH Plus Quick Start, CFP-QS001

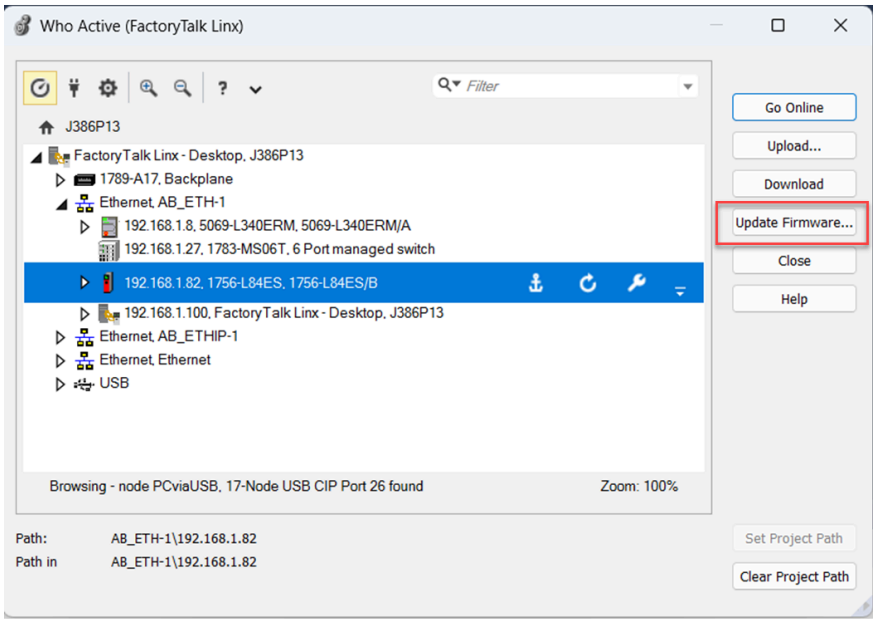
Use AutoFlash to Update Firmware

To update your controller firmware with the AutoFlash feature, complete these steps.

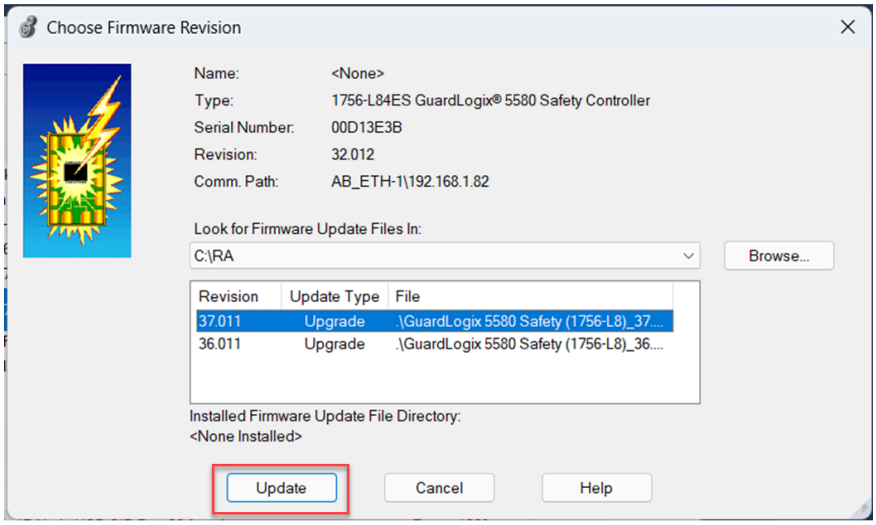
IMPORTANT: If the Secure Digital Card is locked and set to load on power-up, then this update can be overwritten by firmware on the SD card.

1. Verify that the network connection is made and your network driver is configured in Linx-based communication software.
2. On the Path bar in the programming software, click Who Active.

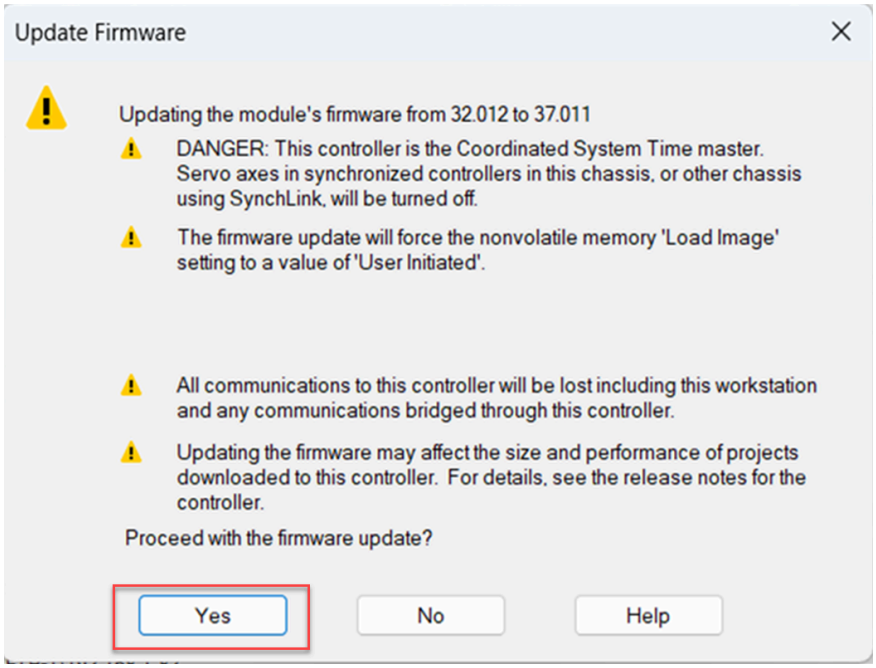
3. On the Who Active dialog box, select your controller under the communication driver you want to use, and click Update Firmware.



4. On the Choose Firmware Revision dialog box, browse to the location of the firmware files.
5. Select the firmware revision, and click Update.



6. On the Confirmation dialog box, click Yes.



7. When the memory card warning appears on the the ControlFLASH Attention dialog box, click OK.
   The firmware update begins.
   Allow the firmware update to complete without interruption. When the firmware update is complete, the process dialog box closes.

Communication Networks

Several communication networks are available. This table describes typical application features that are used with ControlLogix® and GuardLogix® systems, and lists the networks available to support such application features.

Table 2. Applications and Supported Networks

Application Features	Networks for Standard Communication	Networks for CIP Safety™ Communication
Integrated Motion, analog, or SERCOS motion interfaces	EtherNet/IP™	EtherNet/IP™
Time synchronization	EtherNet/IP™	EtherNet/IP™
Control of distributed I/O	• EtherNet/IP™ • DeviceNet® • ControlNet® • Foundation Fieldbus • HART • Universal remote I/O	Time synchronization does not use the safety protocol.
Produce/consume data between controllers	• EtherNet/IP™ • ControlNet®	• EtherNet/IP™ • ControlNet®
Messaging to and from other devices, including access to the controller via the Studio 5000 Logix Designer® application	• EtherNet/IP™ • ControlNet® • DeviceNet® (only to devices) • Data Highway Plus™ (DH+™) • DH-485	Messaging does not use the safety protocol.

EtherNet/IP Network Communication

The EtherNet/IP™ network offers control, configuration, and data collection services by layering the Common Industrial Protocol (CIP™) over the standard Internet protocols, such as TCP/IP and UDP. This combination of standards provides full support for information data exchange and control applications.

IMPORTANT: You cannot bridge through the Ethernet front port of another controller to add remote I/O.

The controller supports 10 Mbps/100 Mbps/1 Gbps port speeds and provides double data rate (DDR) capability across the ControlLogix®backplane.

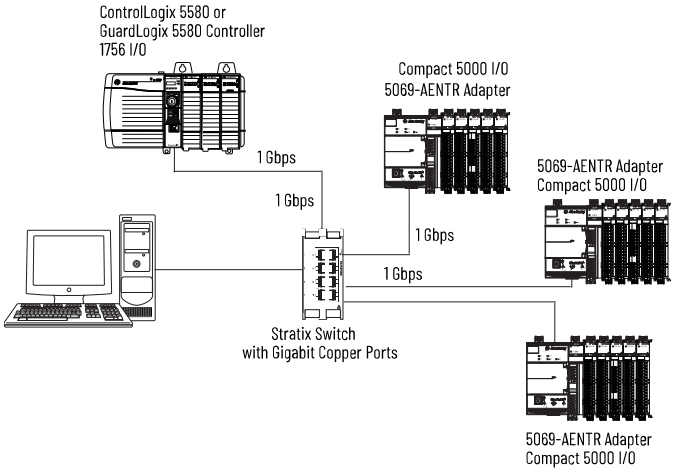
Network performance in the controller system is optimal if the 1 Gbps speed is used. However, legacy Ethernet devices do not support the 1 Gbps speed. Instead, they support a maximum rate of 100 Mbps.

The difference in maximum link speeds impacts your controller system and, in some applications, restricts you from using the 1 Gbps link speeds on a controller.

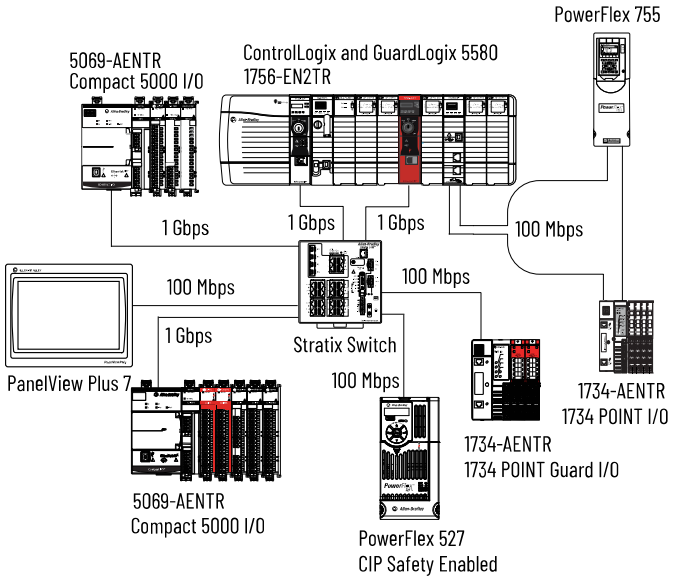
When you design a controller system and consider using the 1 Gbps rate on the controller, remember the following:

- You can use the 1 Gbps speed on the controller port when all network devices support 1 Gbps, for example, 5069-AEN2TR adapters with Compact 5000® I/O modules.

  When switches are used in a star topology, configure the controller ports to use Auto Negotiate.



- You can use the 1 Gbps speed on the controller port when some network devices support a maximum link speed of 100 Mbps. However, the controller must be connected to those devices through a managed switch.



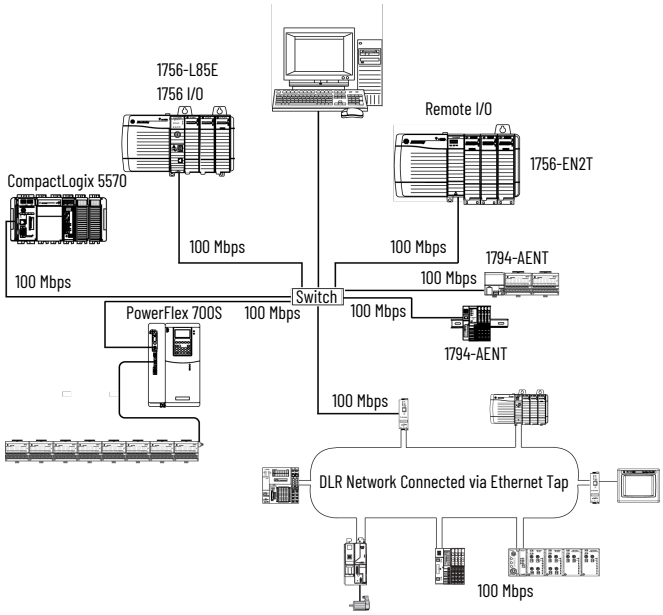
- Do not mix 1 Gbps and 100 Mbps port speeds within one DLR network or linear network.

IMPORTANT: Do not use different speeds on device ports in the same EtherNet/IP™ network without a managed switch.

If you use two or more of these components with a legacy Ethernet device in a ring or linear topology, set all devices to a fixed speed of 100 Mbps and full-duplex:

- ControlLogix® or GuardLogix® controllers
- Compact GuardLogix® 5380 controllers
- 5069 communication adapters
- 5094 communication adapters

This can help prevent bursts of traffic and DLR traffic reversal due to a ring break from causing issues.



EtherNet/IP Communication Modules

ControlLogix® 5580 and GuardLogix® 5580 controllers feature one or more front Ethernet ports that can be used for these purposes:

- Directly connect the controller to an EtherNet/IP™ network without requiring a bridge.
- Communicate with distributed I/O modules and other EtherNet/IP™ devices.
- Bridge messages over an EtherNet/IP™ network.
- Support 10 Mbps, 100 Mbps, 1 Gbps port speeds.

You can use the following communication modules for network communication.

Table 3. EtherNet/IP Communication Modules

Communication Module	Description
1756-EN2T, 1756-EN2TK, 1756-EN2TXT	• Directly connects the controller to an EtherNet/IP™ network without requiring a bridge. • Communicates with distributed I/O modules and other EtherNet/IP™ devices. • Bridges messages over an EtherNet/IP™ network. • 1756-EN2TXT operates in extreme environments with -25…+70 °C (-13…+158 °F) temperatures.
1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT	• Performs the same functions as the 1756-EN2T modules. • Supports communication for a single-fault tolerant Device Level Ring (DLR) network. • Supports a linear topology. • 1756-EN2TRXT operates in extreme environments with -25…+70 °C (-13…+158 °F) temperatures.
1756-EN2F, 1756-EN2FK	• Performs the same functions as the 1756-EN2T modules. • Connects fiber media by an LC fiber connector on the module.
1756-EN2TP, 1756-EN2TPK	• Performs the same functions as the 1756-EN2T modules. • Supports Parallel Redundancy Protocol (PRP).
1756-EN3TR, 1756-EN3TRK	• Performs the same functions as the 1756-EN2TR modules. • Extended Integrated Motion on EtherNet/IP™ network. • Supports as many as 128 motion axes.
1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT	• Performs the same functions as the 1756-EN3TR modules. • Supports as many as 256 motion axes.

Table 3. EtherNet/IP Communication Modules (continued)

Communication Module	Description
	• Supports a 1 Gbps communication rate. • Helps to secure access to a control system from within the plant network.
1756-ENBT, 1756-ENBTK	• Directly connects the controller to an EtherNet/IP™ network without requiring a bridge. • Communicates with distributed I/O modules and other EtherNet/IP™ devices. • Bridges messages over anEtherNet/IP™ network.
1756-EN2TSC	• Performs the same functions as a 1756-ENBT module with twice the capacity for more demanding applications. • Helps to secure access to a control system from within the plant network.
1756-EWEB, 1756-EWEBK	• Performs the same functions as the 1756-ENBT modules. • Provides remote access via an Internet browser to tags in a local ControlLogix® controller. This module does not provide support for I/O or produced/consumed tags. This module does not support CIP Safety™.

ControlNet Network Communication

The ControlNet® network is a real-time control network that provides high-speed transport of time-critical I/O and interlocking data and messaging data. This includes the upload and download of program and configuration data on one physical-media link.

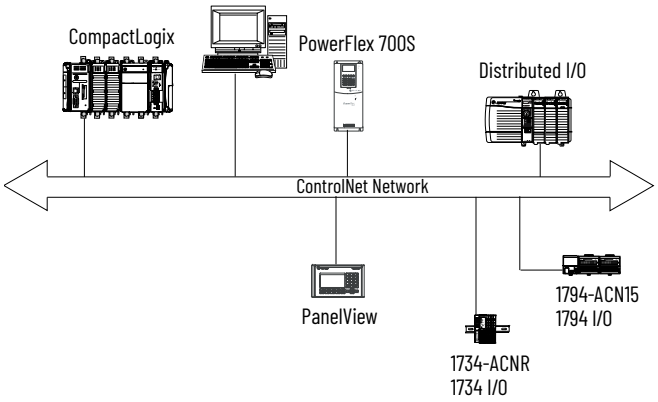
The ControlNet® network is highly deterministic and repeatable and is unaffected when devices are connected or disconnected from the network. This quality results in synchronized and coordinated real-time performance.

The ControlNet® network often functions as the following:

- A substitute/replacement for the remote I/O (RIO) network because the ControlNet® network adeptly handles large numbers of I/O points
- A backbone for multiple distributed DeviceNet® networks
- A peer interlocking network

In the following example, these actions occur on the ControlNet® network:

- The controllers produce and consume tags.
- The controllers initiate MSG instructions that do the following:
  - Send and receive data.
  - Configure devices.
- The workstation is used to do the following:
  - Configure the ControlNet® devices and the ControlNet® network.
  - Download and upload projects from the controllers.



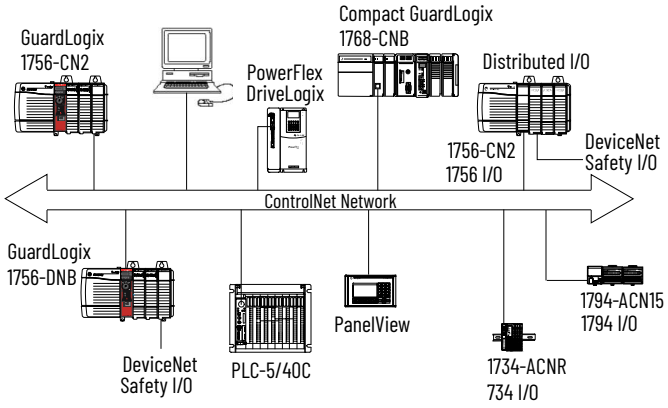
GuardLogix Controllers in a ControlNet Network

ControlNet® communication modules provide the following:

- Support for messaging, produced/consumed safety and standard tags, and distributed standard I/O
- Support the use of coax and fiber repeaters for isolation and increased distance

This example illustrates the following:

- GuardLogix® controllers can produce and consume standard or safety tags between each other.
- GuardLogix® controllers can initiate MSG instructions that send/receive standard data or configure devices. GuardLogix® controllers do not support MSG instructions for safety data.
- The 1756-CN2 module can be used as a bridge, letting the GuardLogix® controller produce and consume standard and safety data to and from I/O devices.



The 1734-ACN adapter does not support POINTGuard I/O™ Safety modules.

ControlNet Communication Modules

This table lists the available ControlNet® modules and their primary features.

Table 4. ControlNet Modules

Module	System	Description
1756-CN2 1756-CN2K	ControlLogix® GuardLogix®	• Performs the same functions as a 1756-CNB module. • Provides twice the capacity for more demanding applications.
1756-CN2R 1756-CN2RK 1756-CN2RXT	ControlLogix® GuardLogix®	• Performs the same functions as a 1756-CN2 module. • Supports redundant ControlLogix® media. • 1756-CN2RXT operates in extreme environments with -25…+70 °C (-13…+158 °F) temperatures.
	ControlLogix®	• Controls I/O modules. • Communicates with other ControlLogix® devices (messages). • Shares data with other Logix 5000© series controllers (produce/consume). • Bridges ControlLogix® links to route messages to devices on other networks. • Standard connections only.
	ControlLogix®	• Performs the same functions as a 1756-CNB module. • Supports redundant ControlNet media. • Standard connections only.

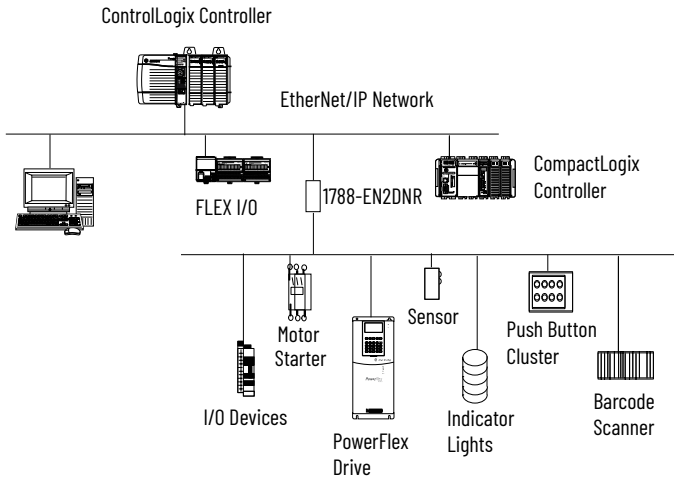
DeviceNet Network Communication

The DeviceNet® network uses the Common Industrial Protocol (CIP™) to provide the control, configuration, and data collection capabilities for industrial devices. You can connect devices directly to plant-floor controllers without having to hard-wire each device into an I/O module.

In the following example, a ControlLogix® controller is connected to the DeviceNet® network and devices via the 1788-EN2DNR linking device.

For more information about DeviceNet® modules and devices, see DeviceNet Modules in Logix 5000 Control Systems User Manual, publication DNET-UM004.

Figure 10. DeviceNet Network



DeviceNet Communication Devices

This table lists the available DeviceNet® bridge and linking devices that can be used with the DeviceNet® network.

Table 5. DeviceNet Communication Modules and Capabilities

Module	System	Description
1756-DNB, 1756-DNBK	ControlLogix® GuardLogix®	• Controls I/O modules. • Communicates with other DeviceNet® devices via messages.
1788-EN2DNR	ControlLogix®	Links an EtherNet/IP™ network to a DeviceNet® network.
1788-CN2DN	ControlLogix®	Links a ControlNet® network to a DeviceNet® network.

A ControlLogix controller requires two connections for each 1756-DNB module:

- One connection for module status and configuration
- One rack-optimized connection for device data

Data Highway Plus (DH+) Network Communication

For DH+™ network communication, you have two module options for use in the ControlLogix® chassis. This table lists the DH+™ modules and capabilities.

Table 6. DH+ Modules and Capabilities

RIO Module	Description
1756-DHRIO, 1756-DHRIOK	• Function as a remote I/O (RIO) scanner. • Support 32 logical rack connections or 16 block transfer connections per channel. • Establish connections between controllers and I/O adapters. • Distribute control so that each controller has its own I/O. • Use for standard communications only.
1756-DHRIOXT	• Performs the same functions as a1756-DHRIO module. • Operates in extreme environments with -25...+70 °C (-13...+158 °F) temperatures. • Use for standard communications only.

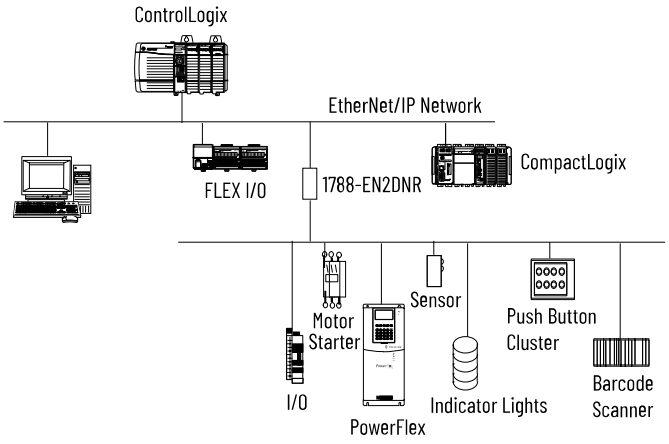
For DH+™ network communication, use a 1756-DHRIO or 1756-DHRIOXT module in theControlLogix® chassis to exchange information between these controllers:

- PLC and SLC™ controllers
- ControlLogix® controllers and PLC or SLC™ controllers
- ControlLogix® controllers

You can connect a maximum of 32 stations to one DH+™ link:

- Channel A supports 57.6 Kbps, 115.2 Kbps, and 230.4 Kbps.
- Channel B supports 57.6 Kbps and 115.2 Kbps.

Figure 11. DH+ Network



Communicate Over a DH+ Network

For the controller to communicate to a workstation or other device over a DH+™ network, use Linx-based communication software to do the following:

- Specify a unique link ID for each ControlLogix® backplane and additional network in the communication path.
- Configure the routing table for the 1756-DHRIO or 1756-DHRIOXT module.

The 1756-DHRIO or 1756-DHRIOXT module can route a message through up to four communication networks and three chassis. This limit applies only to the routing of a message and not to the total number of networks or chassis in a system.

Universal Remote I/O (RIO) Communication

For communication in a Universal RIO network, you have three module options for use in the ControlLogix® chassis. This table lists the RIO modules and capabilities.

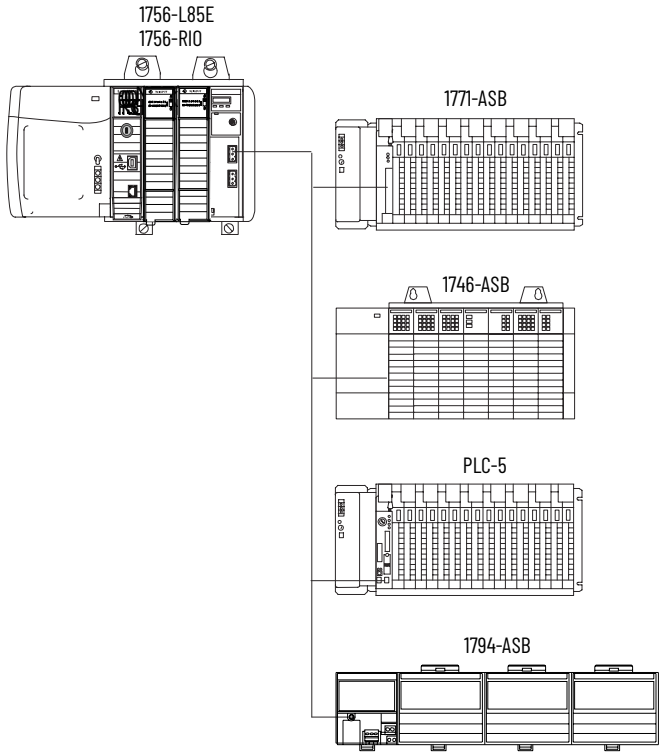
Table 7. RIO Modules and Capabilities

Module	Description
1756-RIO, 1756-RIOK	• Functions as an RIO scanner and adapter. • Supports connections to 32 racks in any combination of rack size or block transfers. • Updates data to the ControlLogix® controller by using scheduled connections. • Supports only standard communication.
1756-DHRIO, 1756-DHRIOK	• Functions as an RIO scanner. • Supports 32 logical rack connections or 16 block transfer connections per channel. • Establishes connections between controllers and I/O adapters. • Distributes control so that each controller has its own I/O. • Supports only standard communication.
756-DHRIOXT	• Performs the same functions as a 1756-DHRIO module. • Operates in extreme environments with -25...+70 °C (-13...+158 °F) temperatures. • Supports only standard communication.

When a channel on the 1756-DHRIO or 1756-DHRIOXT module is configured for Universal RIO communication, the module acts as a scanner for the network. The controller communicates to the module to send and receive the I/O data on the Universal RIO network.

The 1756-RIO module can act as a scanner or adapter on a Universal RIO network. The 1756-RIO module transfers digital, block transfer, analog, and specialty data without message instructions.

Figure 12. Universal RIO Network



Communicate Over a Universal RIO Network

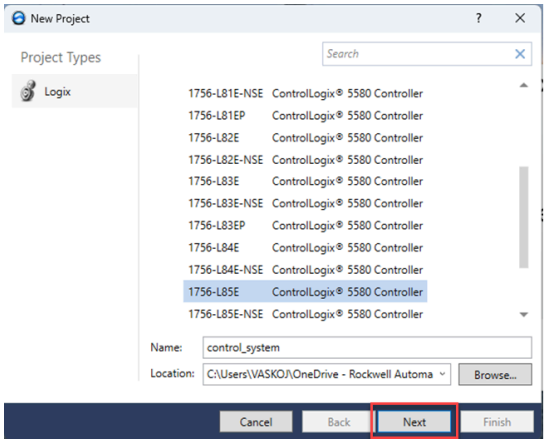
As you design your Universal RIO network, remember the following:

- All devices that are connected to a Universal RIO network must communicate with the same communication rate. Available rates include the following:
  - 57.6 Kbps
  - 115.2 Kbps
  - 230.4 Kbps
- You must assign unique partial and full racks to each channel used in Remote I/O Scanner mode. Both channels of a 1756-DHRIO or 1756-DHRIOXT module cannot scan the same partial or full rack address. Both module channels can communicate to 00...37 octal or 40...77 octal, but each channel can communicate only with one address at a time in whichever of these two ranges it falls.

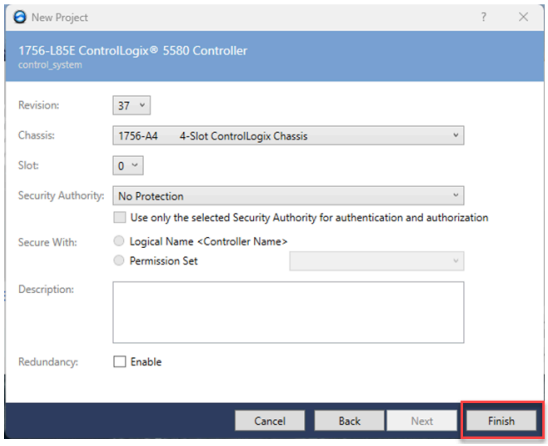
Create a Controller Project

To create a controller project, use the Studio 5000 Logix Designer® application.

1. Open the Logix Designer application and click New Project.
2. Choose the controller catalog number, name the controller, and click Next.



3. Define the properties of the controller, and click Finish:



Safety Project Configuration

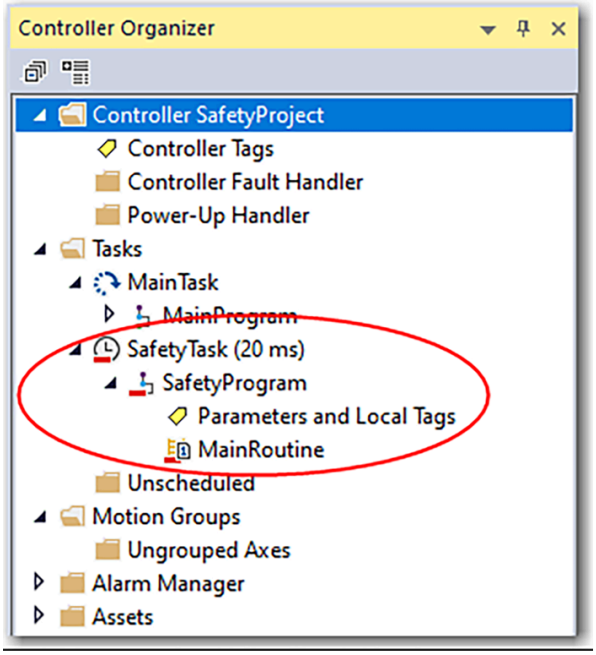
NOTE: The safety configuration descriptions only apply when you are using a GuardLogix® 5580 controller.

Safety projects require additional configuration after you create the project. These topics describe how to configure your controller.

For a safety-enabled controller, the programming software creates a safety task and a safety program. A main Ladder Diagram safety routine that is called MainRoutine is also created within the safety program.

A red bar under the icon distinguishes safety programs and routines from standard project components in the Controller Organizer.

Figure 13. Safety Components



Set the Safety Level

The safety level declares the intent of the safety application. The safety level indicates whether the project is at safety level SIL 2/PLd or SIL 3/PLe.

- The safety level that is required for an application is based on a required risk assessment that you must perform.
- The safety level that is achieved is determined by conformance to Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements.

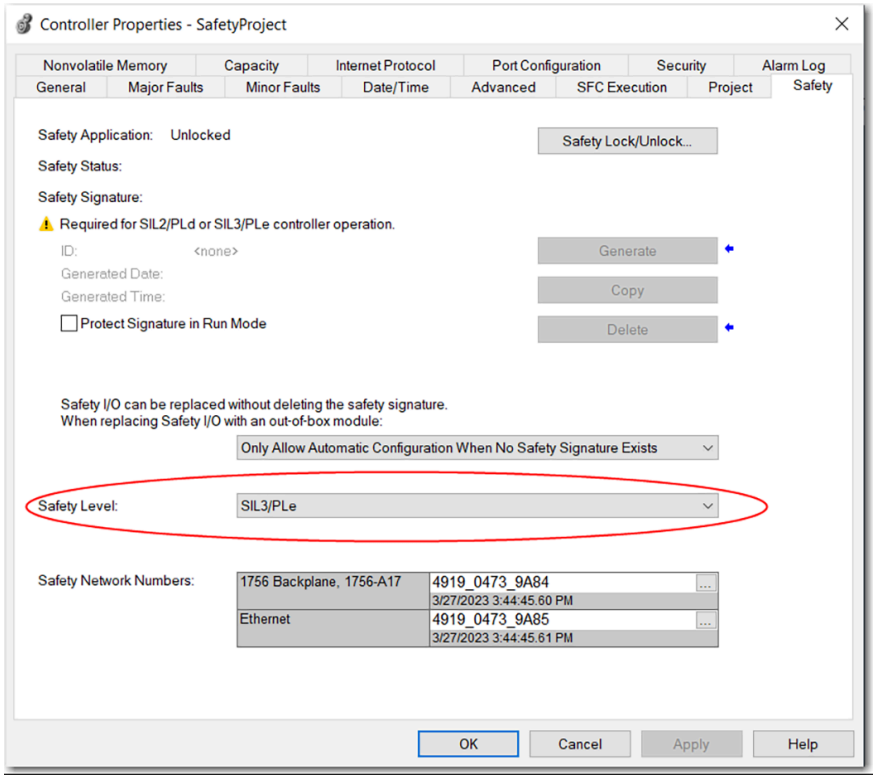
You must specify the safety level:

- The default setting is SIL 2/PLd.
- You can only modify the setting offline, when the safety application is in the Unlocked state and no safety signature exists.
- For SIL 3/PLe, you must have a 1756-L8SP safety partner that is installed to the right of the primary controller. If you select SIL 3/PLe, a safety partner appears in the Controller Organizer I/O tree. If you change the value back to SIL 2/PLd, the safety partner disappears from the I/O tree.

Perform these tasks to set the safety level.

1. On the Online toolbar, click the Controller Properties icon.
2. On the Controller Properties dialog box, click the Safety tab.
3. On the Safety tab, select the Safety Level.

4. Click Apply and then OK.



Passwords for Safety-locking and Unlocking

Safety-locking the controller helps to protect safety control components from modification. Only safety components, such as the safety task, safety programs, safety routines, safety tags, and safety signature are affected. Standard components are unaffected. You can safety-lock or -unlock the controller project when online or offline.

The safety-lock and -unlock feature uses two separate passwords. Passwords are optional.

IMPORTANT: Rockwell Automation does not provide any form of password or security override services. When products and passwords are configured, Rockwell Automation encourages customers to follow good security practices and to plan accordingly for password management.

Protect the Safety Signature in Run Mode

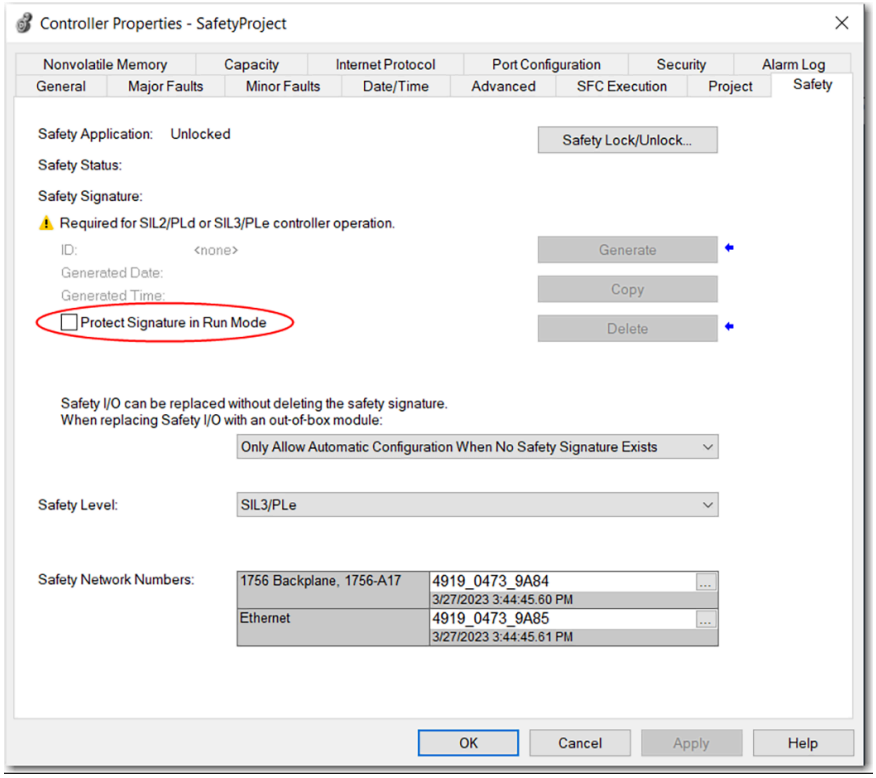
You can help prevent the safety signature from being deleted while the controller is in Remote Run mode, regardless of whether the safety application is locked or unlocked.

IMPORTANT: You must complete these steps before you create a safety signature or safety-lock the controller. Once a safety signature exists, or the application is safety-locked, the Protect Signature in Run Mode checkbox is not editable.

With Studio 5000 Logix Designer® software, version 38 and later, if no signature exists and the Protect Signature in Run Mode box is checked, the user will still be able to generate a new signature while in Remote Run or Test mode. Once created, the new signature will not be able to be deleted while the checkbox is checked and the controller is in Run Mode.

Follow these steps to protect the safety signature.

1. Open the Controller Properties dialog box.
2. Click the Safety tab.
3. Check Protect Signature in Run Mode, and click OK.



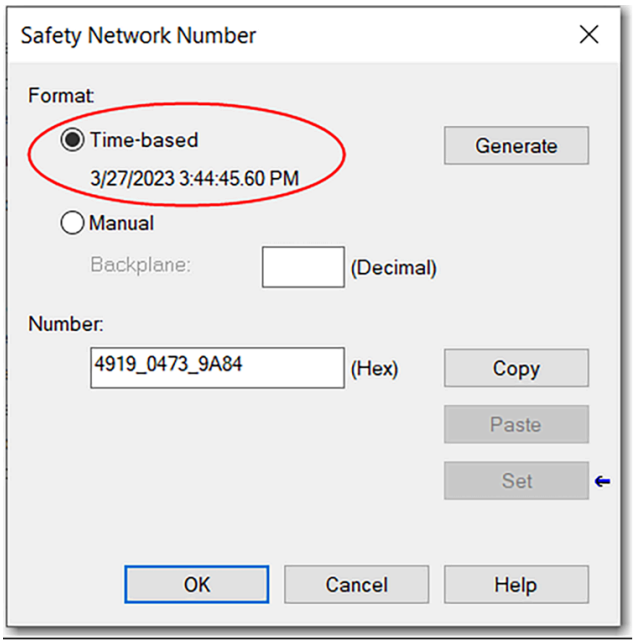
Automatic Assignment of Time-based Safety Network Number

When a new controller or device is created, a time-based SNN is automatically assigned.

- Devices that are created directly under the controller port default to having the same SNN as that port on the controller.
- For devices not directly under a controller port, subsequent new safety device additions to the same CIP Safety™ network are assigned the same SNN defined within the lowest address on that CIP Safety™ network.

The time-based format sets the SNN value as the date and time when the number was generated, according to the computer running the configuration software.

Figure 14. Time-based Format



Manual Assignment of Safety Network Number

Manual assignment is useful if you lay out your network and put the SNNs on your network diagram. It may be easier to read SNNs from a diagram than it is to copy and paste them from multiple projects.

Manual assignment of the SNN is required if the following is true:

- One or more controller ports are on a CIP Safety™ subnet that already has an established SNN.
- A safety project is copied to another hardware installation within the same routable CIP™ Safety system.

IMPORTANT: If you assign an SNN automatically or manually, make sure that system expansion does not result in a duplication of SNN and unique node reference combinations.

A warning appears if your project contains duplicate SNN and unique node reference combinations. You can still verify the project, but Rockwell Automation recommends that you resolve the duplicate combinations.

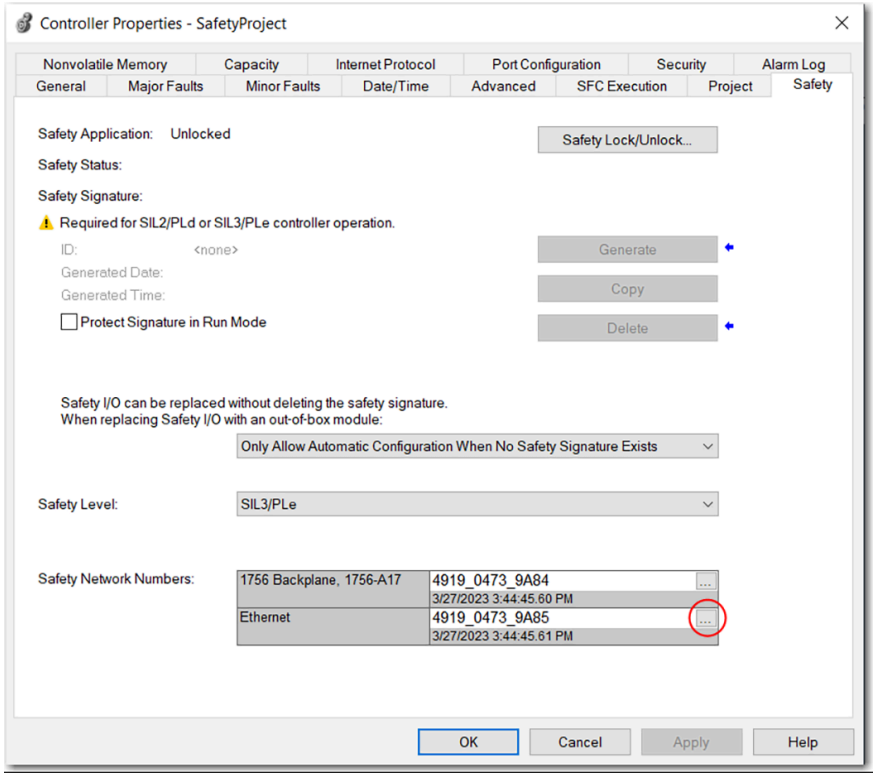
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

If two different devices have the same node references, the safety system cannot detect a packet received by one device that was intended for the other device.

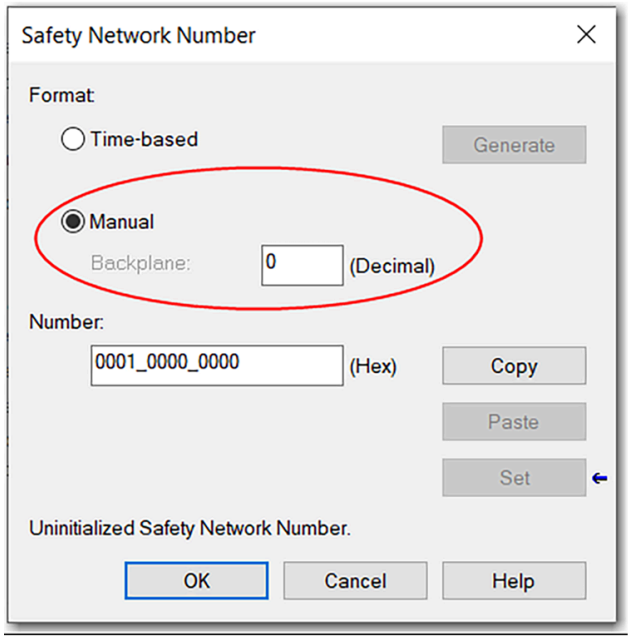
If there are duplicate unique node references, as the system user, you are responsible for proving that an unsafe condition cannot result.

Follow these steps to change the controller SNNs to manual assignments.

1. On the Online toolbar, click the Controller Properties icon.
2. On the Controller Properties dialog box, click the Safety tab.
3. On the Safety tab, click the ellipse button to the right of the safety network number for the port that you want to change.



4. On the Safety Network Number dialog box, select Manual.
5. Enter the SNN as a value from 1...9999 (decimal) and then click OK.

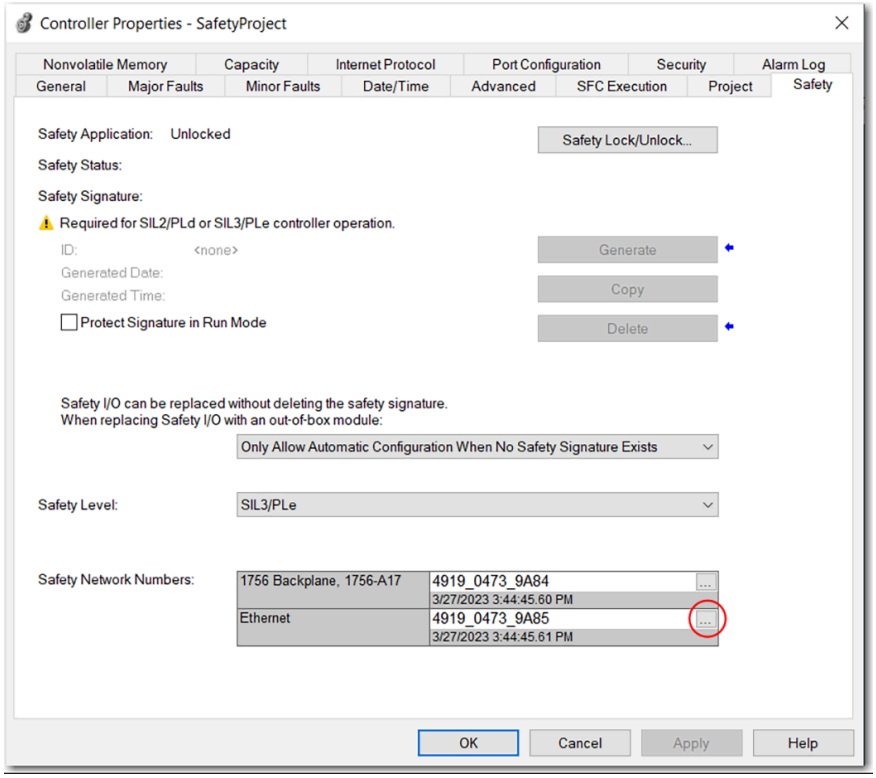


Copy a Safety Network Number

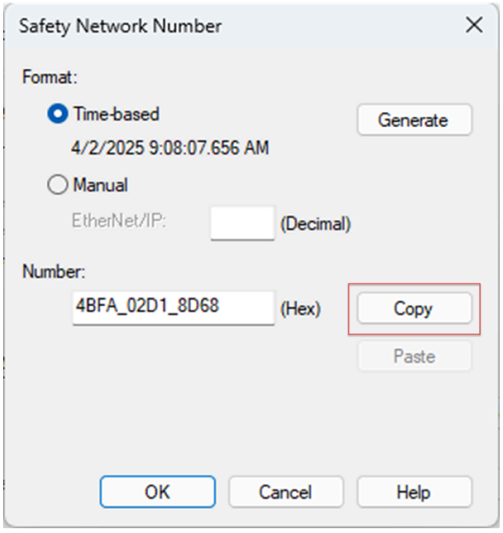
If you must apply a Safety Network Number to other controllers, you can copy and paste the SNN.

To copy a Safety Network Number, complete the following steps.

1. On the Online toolbar, click the Controller Properties icon.
2. On the Controller Properties dialog box, click the Safety tab.
3. Of the Safety tab, click the ellipse to the right of the Safety Network Number.



4. On the Safety Network Number dialog box, click Copy and then OK.



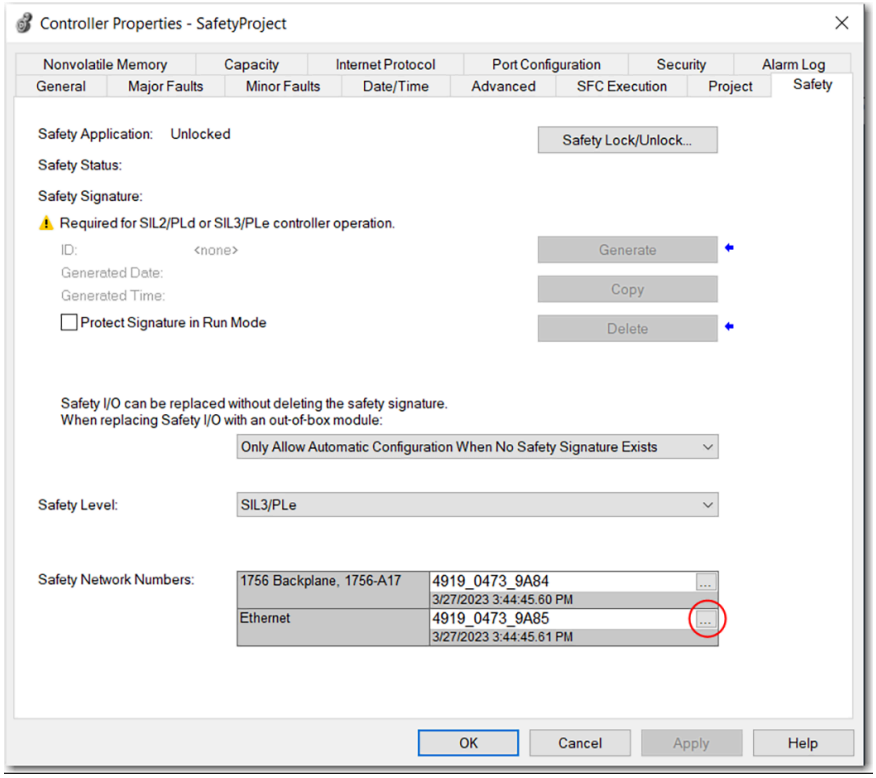
5. On the Controller Properties dialog box, click OK.

Paste a Safety Network Number

If you must apply a Safety Network Number to other controllers, you can copy and paste the SNN.

To paste a Safety Network Number, complete the following steps.

1. On the Online toolbar, click the Controller Properties icon.
2. On the Controller Properties dialog box, click the Safety tab.
3. On the Safety tab, click the ellipse to the right of the Safety Network Number.



4. On the Safety Network Number dialog box, click Paste and then OK.
5. On the Controller Properties dialog box, click OK.

Use Who Active or the Network Browser to Go Online with the Controller

To go online with the controller, you must first specify a communication path in the Studio 5000 Logix Designer® application.

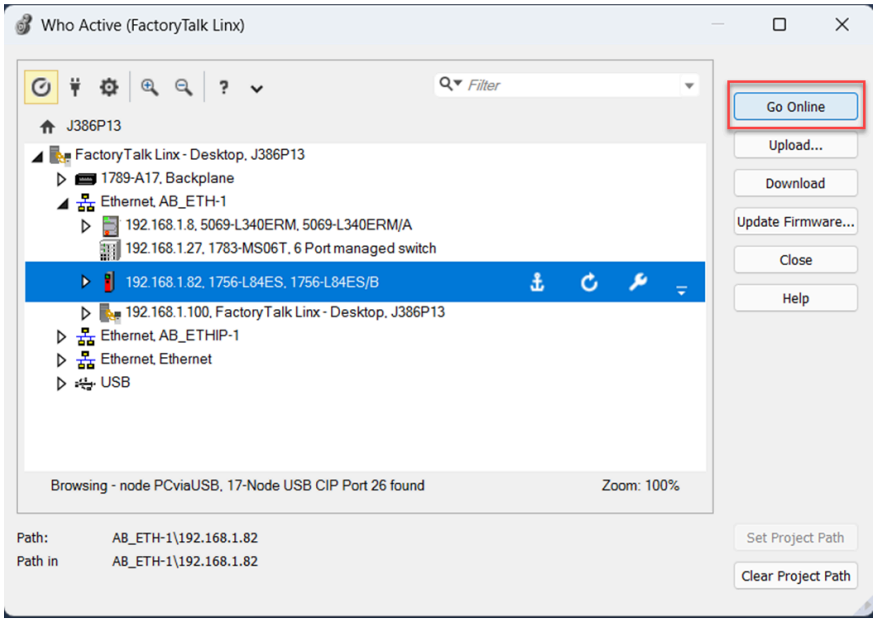
IMPORTANT: With the Studio 5000 Logix Designer® application version 38.00.00 and later, RSWho/Who Active has changed to Network Browser.

1. Open or create a Logix Designer application project.
2. In the application, click Who Active or the Network Browser.

3. Expand the communication path and select the controller.
4. To store the path in the project file, click Set Project Path.

If you store the project path in the project, then you do not have to choose the path each time you go online.

5. After choosing the communication path, click Go Online.



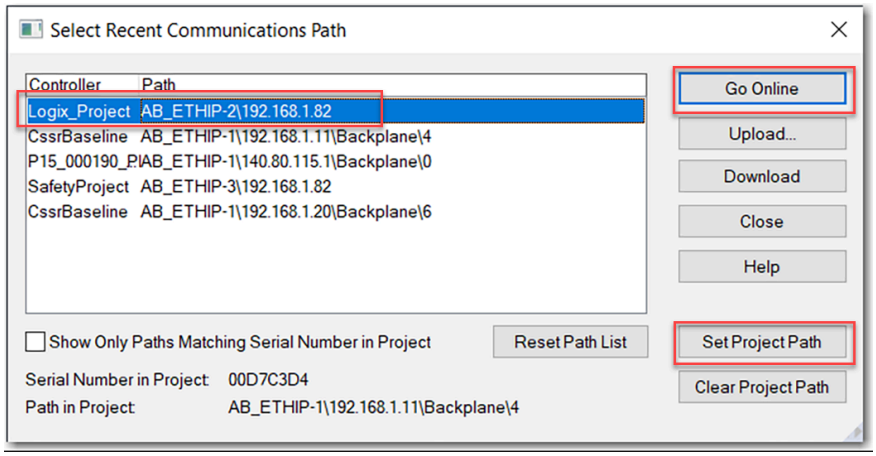
Go Online uses the highlighted node in the tree, regardless of the setting for Path in Project.

Use a Recent Communication Path to Go Online with the Controller

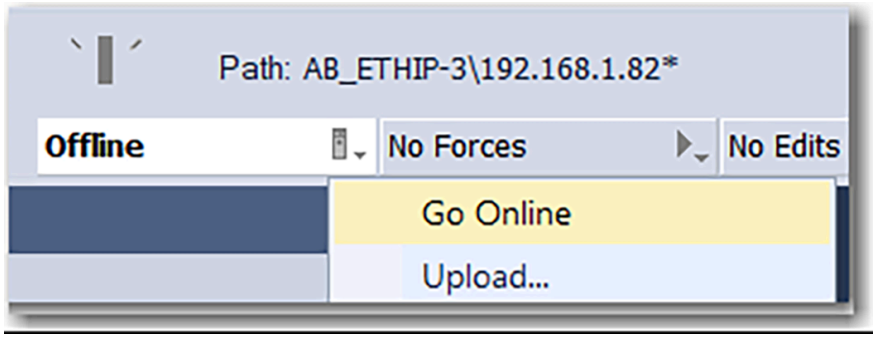
You can also select a recent communications path and go online or apply it to your project.

1. In the application, click the arrow that is on the Path bar.

2. On the Select Recent Communications Path dialog box, choose the path.
3. To store the path in your project, click Set Project Path.
4. Click Go Online.



5. Once you establish a communication path, you can choose Go Online from the Controller Status menu.



Considerations for Going Online with the Controller

The programming software determines whether you can go online with a target controller based on whether the offline project is new or whether changes occurred in the offline project.

- If the project is new, you must first download the project to the controller.
- If changes occurred to the project, you are prompted to upload or download.
- If no changes occurred, you can go online to monitor the execution of the project.

A number of factors affect these processes, including Match Project to Controller and Firmware Revision Matching feature.

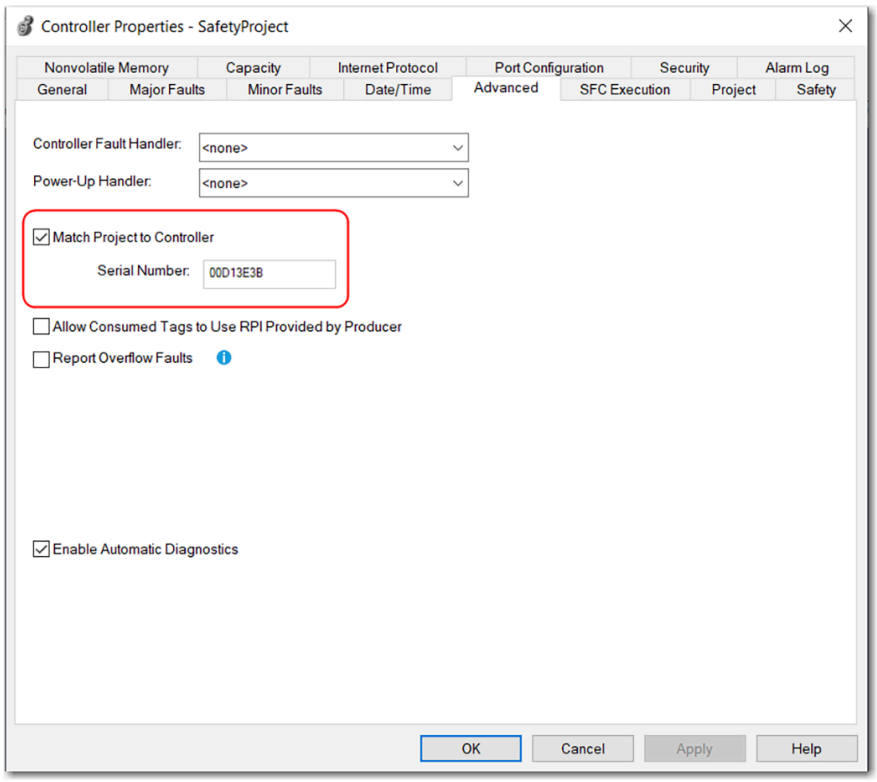
For safety controllers, additional considerations include the safety status and faults, the existence of a safety signature, and the safety-lock/-unlock status of the project and the controller.

Match Project to Controller

The Match Project to Controller feature affects the download, upload, and go online processes of standard and safety projects. This feature is on the Advanced tab of the Controller Properties dialog box.

If the Match Project to Controller feature is enabled in the offline project, the Logix Designer application compares the serial number of the controller in the offline project to that of the connected controller. If they do not match, you must cancel the download/upload, connect to the correct controller, or confirm that you are connected to the correct controller that updates the serial number in the project to match the target controller.

Figure 15. Match Project to Controller



Firmware Revision Matching

Firmware revision matching affects the download process. If the revision of the controller does not match the revision of the project, you are prompted to update the firmware of the controller. The Logix Designer application lets you update the firmware as part of the download sequence.

IMPORTANT: To update the firmware of the controller, first install a firmware update kit.

You can download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc .

You can also upgrade the firmware by choosing ControlFLASH Plus® from the Tools menu in the Logix Designer application.

Considerations for Going Online with a Safety Project

The programming software determines whether you can go online with a target controller based on whether the offline project is new or whether changes occurred in the offline project.

- If the project is new, you must first download the project to the controller.
- If changes occurred to the project, you are prompted to upload or download.
- If no changes occurred, you can go online to monitor the execution of the project.

A number of factors affect these processes, including Match Project to Controller feature and Firmware Revision Matching. For more information on these features, see Considerations for Going Online with the Controller on page 58.

Additional considerations include the safety status and faults, the existence of a safety signature, the safety-lock/-unlock status of the project and the controller, and the configured safety level disagreeing with the presence or absence of a partner in the chassis.

Safety Status/Faults

Uploading program logic and going online is allowed regardless of safety status. Safety status and faults only affect the download process.

You can view the safety status via the Safety tab on the Controller Properties dialog box.

Safety Signature and Safety-locked and -unlocked Status

The existence of a safety signature and the safety-locked or -unlocked status of the controller affect both the upload and download processes.

The safety signature and the safety-lock status are uploaded with the project. For example, if the project in the controller was safety-unlocked, the offline project remains safety-unlocked following the upload, even if it was locked before the upload.

Following an upload, the safety signature in the offline project matches the controller's safety signature.

The safety-lock status always uploads with the project, even when there is no safety signature.

The existence of a safety signature, and the controller's safety-lock status determines whether a download can proceed.

Table 8. Effect of Safety-lock and Safety Signature on Download Functionality

Controller Status	Safety Signature Status	Download Functionality
Safety-unlocked	Safety signature in the offline project matches the safety signature in the controller.	• All standard project components download. • Safety-lock status matches the status in the offline project. The safety signature does not change.
	Safety signatures do not match.	• If the controller had a safety signature, it is automatically deleted, and the entire project is downloaded. • Safety-lock status matches the status in the offline project.
Safety-locked	Safety signatures match.	• If the offline project and the controller are safety-locked, all standard project components are downloaded. • If the offline project is not safety-locked, but the controller is, the download is blocked and you must first unlock the controller to allow the download to proceed.
	Safety signatures do not match.	• You must first safety-unlock the controller to allow the download to proceed. • If the controller had a safety signature, it is automatically deleted, and the entire project is downloaded. • Safety-lock status matches the status in the offline project.

Checks for Going Online with a Safety Project

For a safety project, the programming software checks for the following:

- If Match Project to Controller is selected, do the offline project and controller serial numbers match?
- Does the offline project contain changes that are not in the controller project?
- Do the revisions of the offline project and controller firmware match?
- Are either the offline project or the controller safety-locked?
- Do the offline project and the controller have compatible safety signatures?

Table 9. Connect to the Controller with a Safety Project

Software Indicates	Action
Unable to connect to controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller, select another project file, or choose the Update project serial number checkbox and choose Go Online... to connect to the controller and update the offline project serial number to match the controller.
Unable to connect to controller. The revision of the offline project and the controller's firmware are not compatible.	Choose one of the following options: • Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection. **IMPORTANT:** The online project is deleted. • To preserve the online project, cancel the online process and install a version of the Studio 5000© environment that is compatible with the firmware revision of your controller.
You need to upload or download to go online by using the open project.	Choose one of the following options: • Upload to update the offline project. • Download to update the controller project. • Choose File to select another offline project.
Unable to connect in a manner that preserves safety signature. The firmware minor revision on the controller is not compatible with safety signature in offline project.	• To preserve the safety signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller. • To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to connect to controller. Incompatible safety signature cannot be deleted while project is safety-locked.	Cancel the online process. You must safety-unlock the offline project before attempting to go online.

When the controller and the Logix Designer application are online, the safety-locked status and safety signature of the controller match the controller's project. The safety-lock status and safety signature of the offline project are overwritten by the controller. If you do not want the changes to the offline project to be permanent, do not save the project file following the go online process.

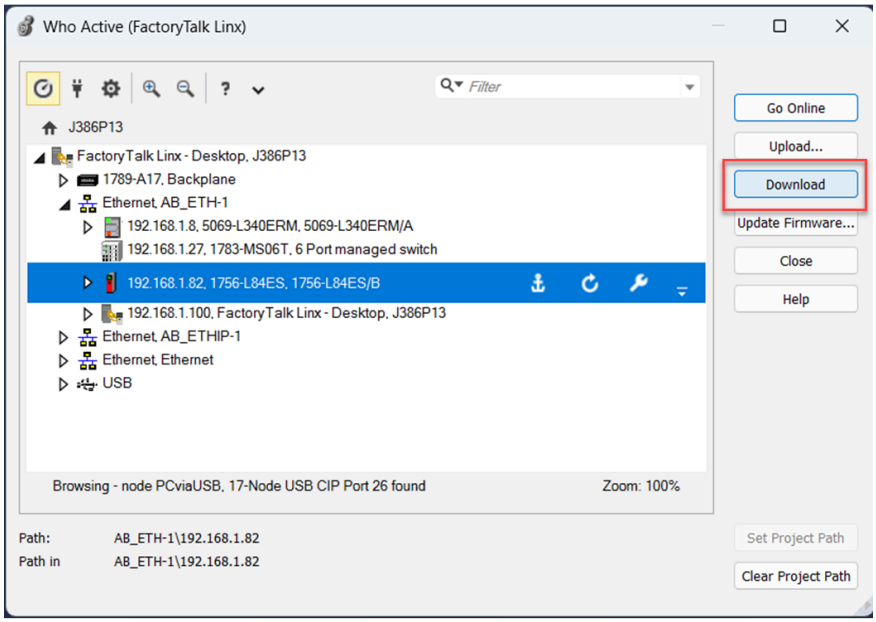
Use Who Active or the Network Browser to Download to the Controller

When you download a project to the controller, it copies the project from the programming software to the controller.

You can use the features of the Who Active or Network Browser dialog box to download to your controller after you have set the communication path. Complete these steps to download to the controller.

IMPORTANT: Studio 5000 Logix Designer® application version 38.00.00 and later, RSWho/Who Active has changed to Network Browser.

1. After you set the communication path, click Download.



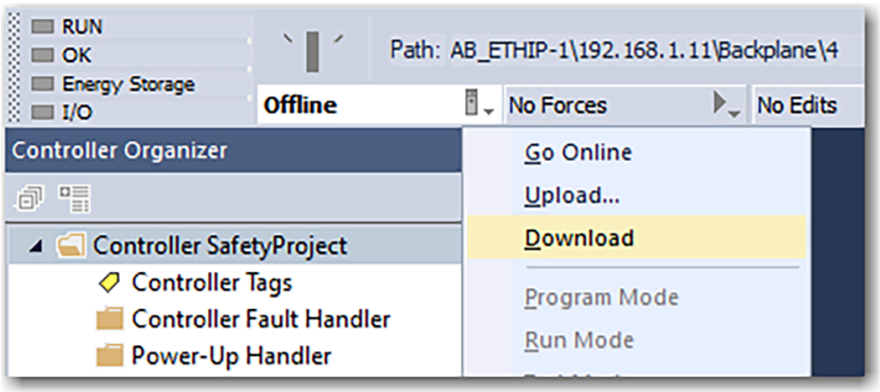
2. After reading the warning in the Download dialog box, click Download.

Use the Controller Status Menu to Download to the Controller

After you select a communication path in the Logix Designer application, you can use the Controller Status menu to download to the controller.

From the Controller Status menu, choose Download. After the download completes, the project name appears on the scrolling status display.

Figure 16. Download via the Controller Status Menu



Download Considerations for a Safety Project

For a safety project, the programming software compares the following information in the offline project and the safety controller:

- Controller serial number (if Match Project to Controller is selected)
- Firmware major and minor revisions
- Safety status
- Safety signature (if one exists)
- Safety-lock status
- Safety partner (if one exists) - The programming software does not allow the download of a project configured for SIL 2 if a safety partner is to the right of the primary controller.

After the checks all pass, a download confirmation dialog box appears. Click Download.

The programming software displays status messages in the download dialog, progress screen, and the Errors window.

Table 10. Status Messages

Software Message	Action
Unable to download to the controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller or verify that this is the correct controller. If it is the correct controller, check the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number.
Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible.	Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.
Unable to download a SIL 2 application, Safety Partner is Present.	Remove the safety partner.
Unable to download to controller. The safety partner is missing or unavailable.	Cancel the download process. Install a compatible safety partner before attempting to download.
Unable to download to controller. The firmware revision of the safety partner is not compatible with the primary controller.	Update the firmware revision of the safety partner. Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.
Unable to download to controller. Safety partnership has not been established.	Cancel this download process and attempt a new download.
Unable to download to controller. Incompatible safety signature cannot be deleted while the project is safety-locked.	Cancel the download. To download the project, you must safety-unlock the offline project, delete the safety signature, and download the project. **IMPORTANT:** The safety system requires revalidation.
Cannot download in a manner that preserves the safety signature. Controller's firmware minor revision is not compatible with safety signature in offline project.	• If the firmware minor revision is incompatible, to preserve the safety signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project. • To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to download to controller. Controller is locked. Controller and offline project safety signatures do not match.	Choose Unlock. The Safety Unlock for Download dialog box appears. If the Delete Signature checkbox is selected and you choose Unlock, click Yes to confirm the deletion.

Table 10. Status Messages (continued)

Software Message	Action
Downloading safety signature...	The safety signature is present in the offline project and is downloading.

Following a successful download, the safety-locked status and safety signature of the controller match the project that was downloaded. Safety data is initialized to the values that existed when the safety signature was created.

Use Who Active or the Network Browser to Upload from the Controller

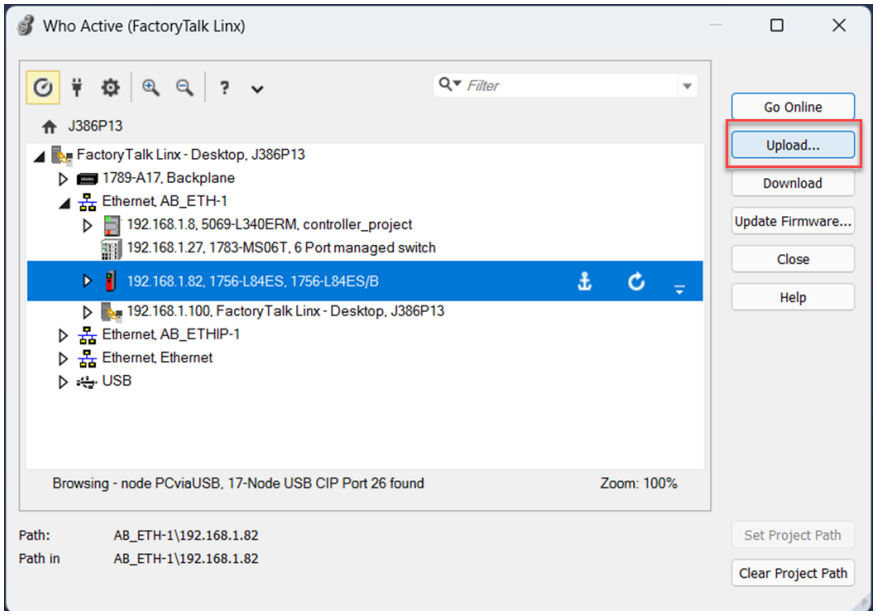
When you upload a project from the controller, it copies the project from the controller to the Studio 5000 Logix Designer® application.

You can use the features of the Who Active or Network Browser dialog box to upload from your controller after you have set the communication path.

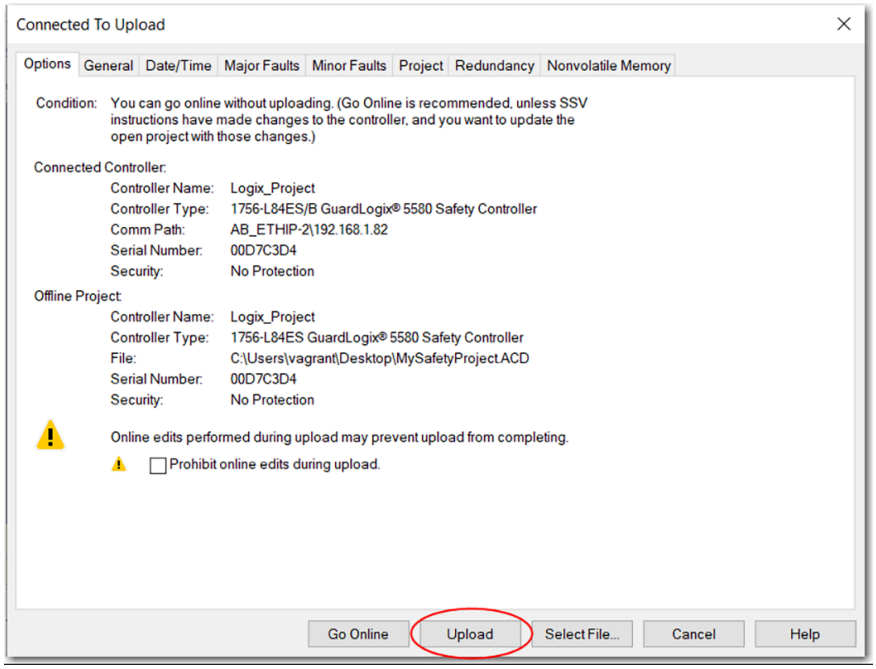
IMPORTANT: With the Studio 5000 Logix Designer® application version 38.00.00 and later, RSWho/Who Active has changed to Network Browser.

Complete these steps to upload from the controller.

1. After choosing the communication path, click Upload.



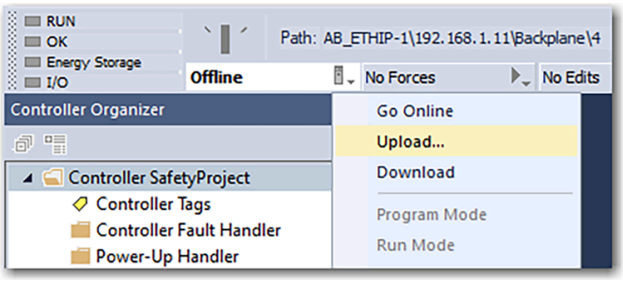
2. On the Connected to Upload dialog box, verify the project to upload and click Upload.



Use the Controller Status Menu to Upload from the Controller

After you chose a communication path, you can use the Controller Status menu to upload from the controller.

1. From the Controller Status menu, choose Upload.



2. On the Connected to Upload dialog box, verify the project to upload and click Upload.

Considerations for Upload from a Safety Controller

For a safety project, the Studio 5000 Logix Designer® application compares the following information in the project and the controller:

- Controller serial number (if project to controller match is selected)
- Open project to the controller project
- Firmware major and minor revisions
- Safety signature (if one exists)

IMPORTANT: An upload is allowed regardless of the Safety status and the safety-locked state of the offline project and controller. The locked status follows the state of the uploaded project.

Upload Behavior	Response
If the project to controller match is enabled, the Logix Designer application checks whether the serial number of the open project and the serial number of the controller match.	• Connect to the correct controller or verify that this is the correct controller. • Select a new project to upload into or select another project by choosing Select File. • If it is the correct controller, select the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number.
The Logix Designer application checks whether the open project matches the controller project.	• If the projects do not match, you must select a matching file or cancel the upload process. • If the projects match, the software checks for changes in the offline (open) project.
The Logix Designer application checks for changes in the offline project.	• If there are no changes in the offline project, you can go online without uploading. Click Go Online. • If there are changes in the open project that are not present in the controller, you can choose to upload the project, cancel the upload, or select another file.
Uploading safety signature...	This message appears during the upload only if a safety signature matching the one in the controller does not exist in the offline project.

If you choose Upload, the standard and safety applications are uploaded. If a safety signature exists, it is also uploaded. The safety-lock status of the project reflects the original status of the online (controller) project.

Before the upload, if an offline safety signature exists, or the offline project is safety-locked but the controller is safety-unlocked or has no safety signature, the offline safety signature and safety-locked state are replaced by the online values (safety-unlocked with no safety signature). If you do not want to make these changes permanent, do not save the offline project following the upload.

Controller Operation Modes

The controller operates in the following modes:

- Run
- Remote Run
- Remote Program
- Remote Test
- Program

Run Mode

In Run mode, the controller is actively controlling the process or machine. You cannot edit projects when the controller is in Run mode.

ATTENTION: Only use Run mode when all conditions are safe.

The controller can perform these functions in Run mode:

- Turn outputs to the state commanded by the logic of the project
- Execute (scan) tasks
- Send messages
- Send and receive data in response to a message from another controller
- Produce and consume tags

The controller **cannot** perform these functions in Run mode:

- Turn outputs to their configured state for Program mode
- Change the mode of the controller via the programming software
- Download a project
- Schedule a ControlNet® network
- While online, edit the project

Remote Run Mode

Remote Run mode is identical to Run mode except you can edit the project online, and change the controller mode through the Logix Designer application.

ATTENTION: You are able to modify a project file online in Remote Run mode. Be sure to control outputs with care to avoid injury to personnel and damage to equipment.

The controller can perform these functions in Remote Run mode:

- Turn outputs to the state commanded by the logic of the project
- Execute (scan) tasks
- Change the mode of the controller via the programming software
- While online, edit the project
- Send messages
- Send and receive data in response to a message from another controller
- Produce and consume tags
- Generate a safety signature

The controller **cannot** perform these functions in Remote Run mode:

- Turn outputs to their configured state for Program mode
- Download a project
- Schedule a ControlNet® network

Remote Program Mode

Remote Program mode functions like Program mode, except you can change the controller mode through the Logix Designer application.

ATTENTION: Outputs are commanded to their Program mode state, which can cause a dangerous situation.

The controller can perform these functions in Remote Program mode:

- Turn outputs to their configured state commanded for Program mode
- Change the mode of the controller via the programming software
- Download a project

- Schedule a ControlNet® network
- While online, edit the project
- Send and receive data in response to a message from another controller
- Produce and consume tags
- Generate a safety signature

The controller **cannot** perform these functions in Remote Program mode:

- Turn outputs to the state commanded by the logic of the project
- Execute tasks

Remote Test Mode

Remote Test mode executes code, but I/O is not controlled. You can edit the project online and change the controller mode through the Logix Designer application.

ATTENTION: Outputs are commanded to their Program mode state, which can cause a dangerous situation.

The controller can perform these functions in Remote Test mode:

- Turn outputs to their configured state commanded for Program mode
- Execute tasks
- Change the mode of the controller via the programming software
- While online, edit the project
- Send messages
- Send and receive data in response to a message from another controller
- Produce and consume tags

The controller **cannot** perform these functions in Remote Test mode:

- Turn outputs to the state commanded by the logic of the project
- Download a project
- Schedule a ControlNet® network
- Send messages

Program Mode

Program mode does not execute code or control I/O, but editing is available. Controller modes cannot be changed through the Logix Designer application.

ATTENTION: Do not use Program mode as an emergency stop (E-stop). Program mode is not a safety device.

Outputs are commanded to their Program mode state, which can cause a dangerous situation.

The controller can perform these functions in Program mode:

- Turn outputs to their configured state commanded for Program mode
- Download a project
- Schedule a ControlNet® network
- While online, edit the project
- Send and receive data in response to a message from another controller
- Produce and consume tags

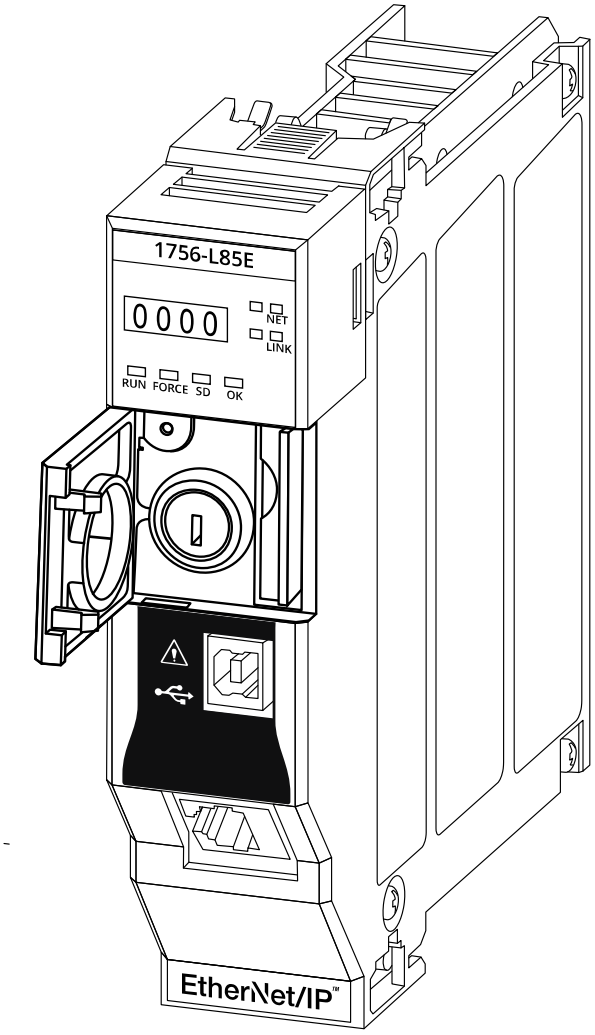
The controller **cannot** perform these functions in Program mode:

- Turn outputs to the state commanded by the logic of the project
- Execute tasks
- Change the mode of the controller via the programming software
- Send messages

Change the Operation Mode

You can use the keyswitch on the front of the controller to change the operation mode.

Figure 17. Controller Keyswitch



To change the operation mode, you must physically change the position of the keyswitch to correspond with the desired operation mode, as described in the following table.

Table 11. Controller Keyswitch Positions and Operation Modes

Keyswitch Position	Operation Mode
RUN	Run mode
REM	• Remote Run mode • Remote Program mode • Remote Test mode
PROG	Program mode

When the keyswitch is in the REM position, there are three possible modes:

- To activate Remote Run mode, move the keyswitch from RUN to REM.
- To activate Remote Program mode, move the keyswitch from PROG to REM.
- To activate Remote Test mode, use the Logix Designer application along with the REM keyswitch position.

When the mode keyswitch on the controller is set to RUN mode, features like online editing, program downloads, and firmware updates are prohibited. For a list of prohibited features, see Controller Operation Modes on page 66.

The keyswitch provides a mechanical means to enhance controller and control system security. The physical switch can complement other authorization and authentication methods that similarly control user-access to the controller, such as the FactoryTalk® Security service.

IMPORTANT: During runtime, we recommend that you place the controller keyswitch in RUN mode and remove the key from the switch. By removing the key, you discourage unauthorized access to the controller or potential tampering with the program of the controller, configuration, or firmware.

Place the keyswitch in REM or PROG mode during controller commissioning and maintenance and whenever access is needed to change the program, configuration, or firmware.

Use the Logix Designer Application to Change the Operation Mode

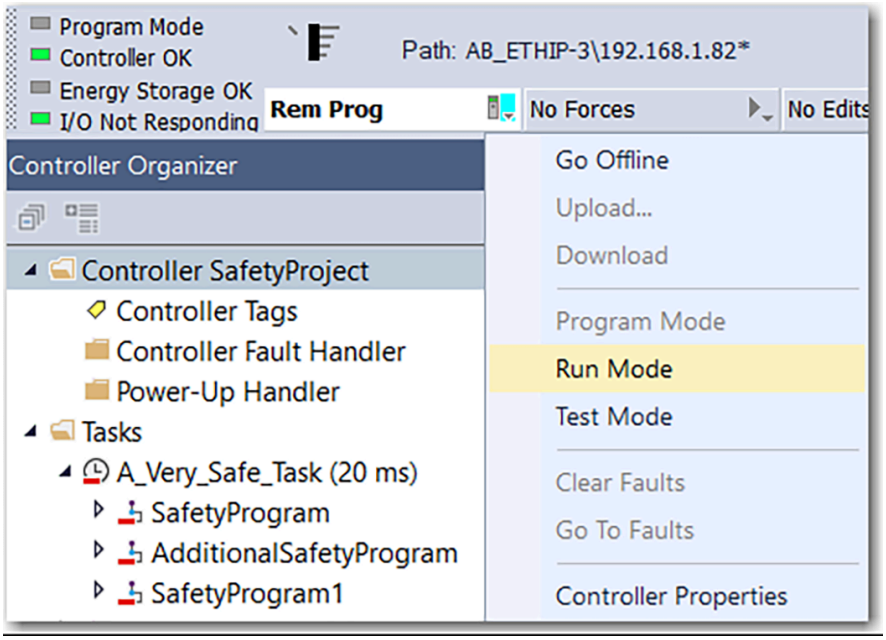
When you are online with the controller, and the switch position is set to REM, then you can use the Logix Designer application to change the operation mode.

The Controller Status menu lets you specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

From the Controller Status pulldown menu, choose the operation mode.

Figure 18. Operation Modes in Logix Designer



Reset Button

You can reset the controllers or the safety partner with the reset button. The reset button is only read during a power-up or restart. If you press the reset button at another time, it has no effect.

For a safety controller, the Safety Locked status or safety signature does not prevent you from performing a controller reset. Because the application is cleared from the controller during a reset, the safety level of the controller is cleared also. When you download a safety project to the controller, the safety level is set to the level specified in the project.

A controller has two stages of reset:

- A Stage 1 reset clears the application program and memory, but retains the IP address and all network settings. A stage 1 reset occurs only if the controller contains a user application.
- A Stage 2 reset returns the controller to factory settings, including firmware, and clears all network settings. A stage 2 reset occurs only if the controller does not contain a user application, and the current controller firmware is not a 1.x version.

The Safety Partner reset returns the safety partner to out-of-box settings, including firmware.

IMPORTANT: Because port enable/disable status is associated with the application program, the controller Ethernet port becomes enabled after a Stage 1 or Stage 2 reset.

WARNING: When you press the reset button while power is on, an Electric Arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Figure 19. Controller Reset Button

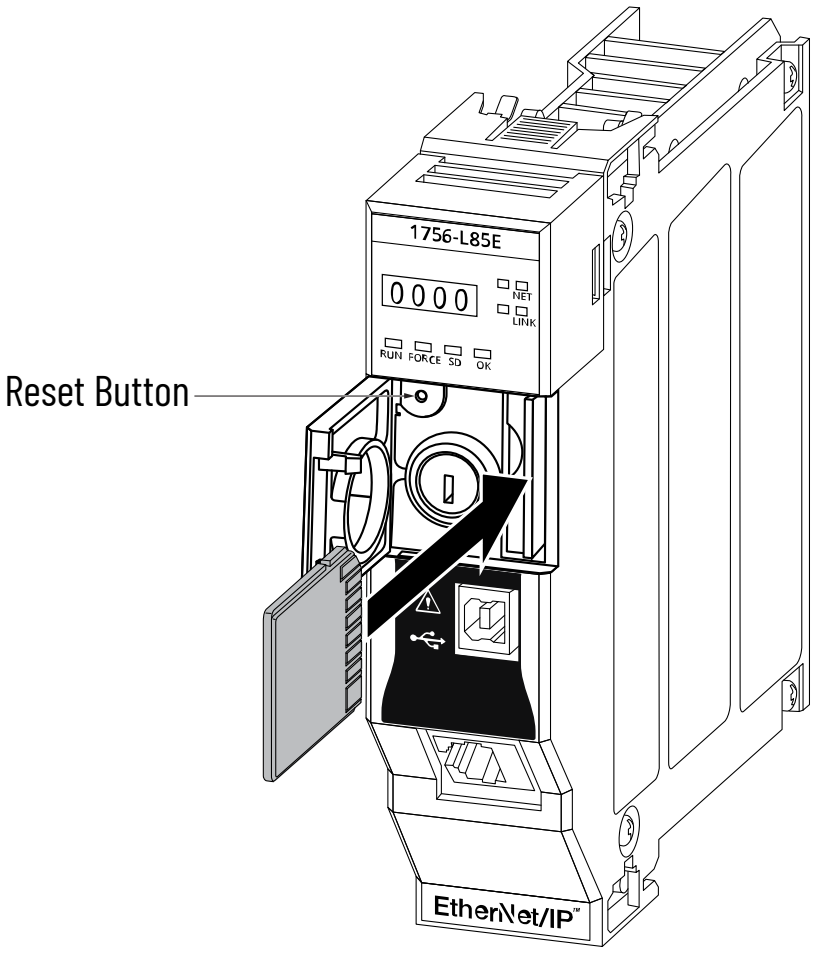
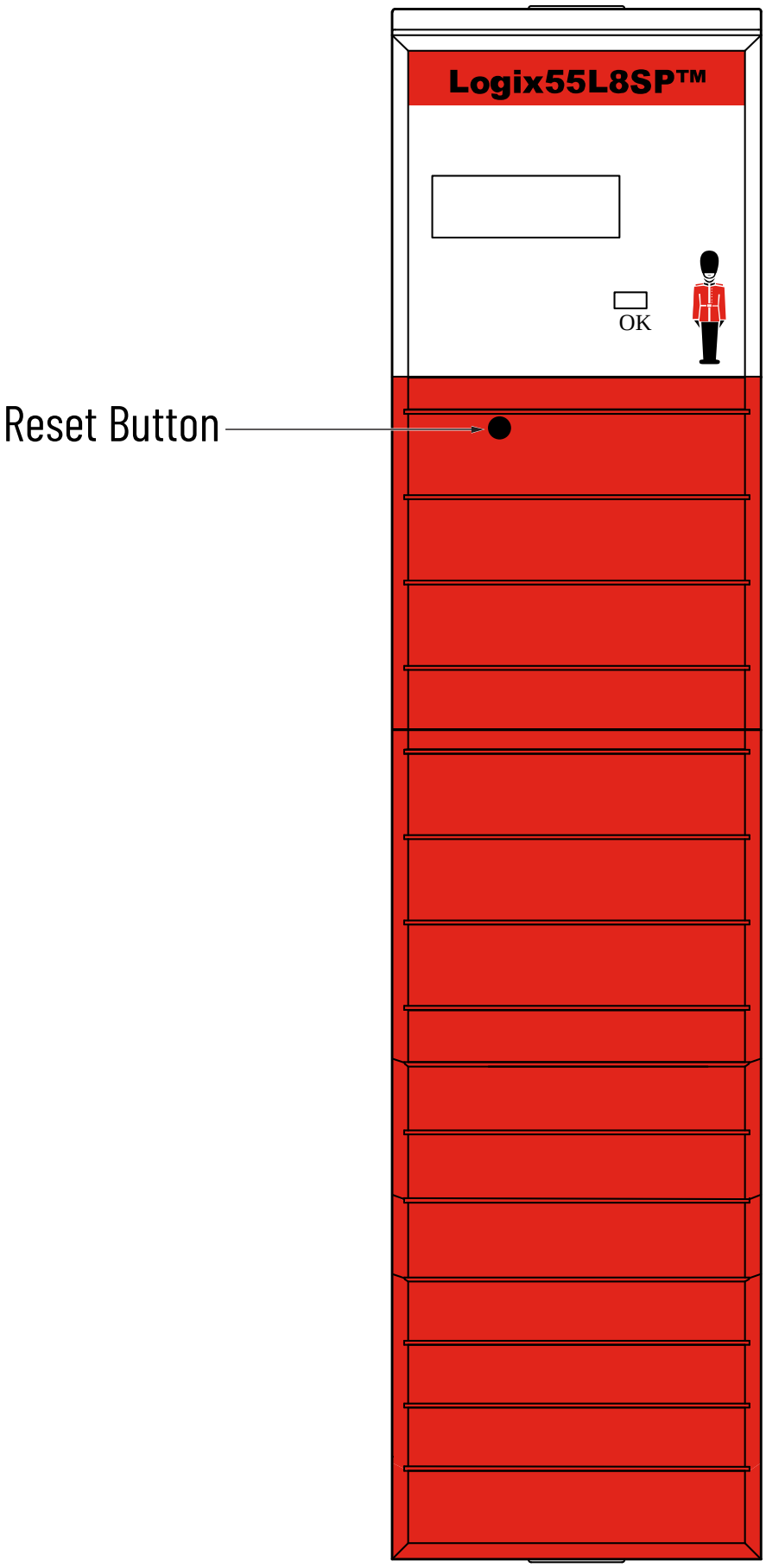


Figure 20. Safety Partner Reset Button



Stage 1 Reset

The stage 1 reset does the following:

- Clears the application program.
- Retains the network settings for the embedded Ethernet port.
- Retains APR (motion position) information.
- Retains non-volatile configuration parameters for PTP (Precision Time Protocol)/CIP Sync time synchronization.
- Resets WallClockTime to default parameters.
- Resets the controller to begin the controller startup process.
- Helps to prevent the controller from loading firmware or software from the memory card on first start up after the reset, regardless of the setting on the memory card and without modifying the memory card contents (the write-protect setting is irrelevant). A memory card will reload on subsequent powerup situations.
- Enables the Ethernet port, if it was previously disabled.

To perform a Stage 1 reset, complete these steps. This process assumes that a memory card is installed in the controller.

1. Power down the controller.
2. Remove the key from the keyswitch.
3. Open the front door on the controller.
4. Use a small tool with a diameter of a paper clip, to press and hold the reset button. The button is recessed behind the panel.
5. While holding in the reset button, power up the controller.
6. Continue to hold the reset button while the 4-character display cycles through CLR, 4, 3, 2, 1, Project Cleared.
7. After Project Cleared appears, release the reset button.

IMPORTANT: If you release the reset button before Project Cleared scrolls across the display, the controller continues with powerup and does not reset.

After a Stage 1 reset is performed, load a Studio 5000 Logix Designer® application project to the controller in these ways:

- Download the project from the Logix Designer application.
- Cycle power on the controller to load a project from the SD card.
  This option works only if the project stored on the SD card is configured to load the project on powerup.

Stage 2 Reset

The stage 2 reset does the following:

- Returns the module to revision 1.x firmware (out-of-box firmware revision).
- Clears all user settings to the out-of-box values including network and time synchronization settings.
- Resets the controller to begin the controller startup process.
- There will be no entries in the controller log after a Stage 2 reset, but saved logs on the memory card remain.

To perform a Stage 1 reset, complete these steps. This process assumes that a memory card is installed in the controller.

1. Power down the controller.
2. Remove the key from the keyswitch.

3. Open the front door on the controller.
4. Remove the memory card.
5. Use a small tool with a diameter of a paper clip, to press and hold the reset button. The button is recessed behind the panel.
6. While holding in the reset button, power up the controller.
7. Continue to hold the reset button while the 4-character display cycles through DFLT, 4, 3, 2, 1, Project Cleared.
8. After Project Cleared appears, release the reset button.
9. On your workstation, delete all files on the memory card.
10. Power down the controller.
11. Reinstall the memory card.
12. Powerup the controller.
13. Verify that the controller is at firmware revision 1.x, and the controller is set to DHCP.
14. After a Stage 2 reset is performed, you must complete these tasks to use the controller again:
    a. Configure the Ethernet ports, set the desired EtherNet/IP™ mode, and set the controller IP address configuration.
    b. Update the firmware revision.
    c. Download a Studio 5000 Logix Designer® application project to the controller in one of these ways:
    - Download the project from the Logix Designer application.
    - Cycle power on the controller to load a project from the memory card. This option works only if the project stored on the memory card is configured to load the project on powerup.

Safety Partner Reset

Follow these steps to perform a safety partner reset.

1. Power down the safety partner.
2. Use a small tool with a diameter of a paper clip to press and hold the reset button. This button is recessed 5 mm (0.19 in.) behind the panel.
3. While holding in the reset button, power up the safety partner.
4. Continue to hold the reset button while the 4-character display cycles through DFLT, 4, 3, 2, 1, Factory Default.
5. After Factory Default appears, release the reset button

Use the Memory Card

The controllers ship with a memory card installed.

The safety partners ship with a memory card installed. This card is used internally by the product to automatically capture the module error log should a fault occur.

We recommend that you leave the memory card installed, so if a fault occurs, diagnostic data is automatically written to the card. Rockwell Automation can then use the data to help investigate the cause of the fault.

We recommend that you use the memory cards available from Rockwell Automation®. For information on what memory cards are compatible with the controllers, see 1756 ControlLogix and GuardLogix Controllers Technical Data, 1756-TD001.

While other memory cards can be used with the controller, Rockwell Automation® has not tested the use of those cards with the controller and you could experience data corruption or loss.

Memory cards that are not provided by Rockwell Automation® can have different industrial, environmental, and certification ratings as those cards that are available from Rockwell Automation®. These cards can have difficulty with survival in the same industrial environments as the industrially rated versions available from Rockwell Automation®.

The memory card that is compatible with your controller is used to load or store the contents of user memory for the controller.

When you use the Store feature, the project that is stored on the memory card matches the project in the controller memory then. Changes that you make after you store the project are not reflected in the project on the memory card.

If you change the project in the controller memory but do not store those changes, the next time that you load the project from the memory card to the controller, you overwrite the changes.

IMPORTANT: Do not remove the memory card while the controller is reading from, or writing to, the card. If you remove the card during either activity, the data on the card or controller can become corrupt.

Additionally, the controller firmware at the time when the card is removed can become corrupted. Leave the card in the controller until the OK status indicator turns steady green.

If a memory card is installed, you can see the contents of the card on the Nonvolatile Memory tab of the Controller Properties dialog box. If a safety application is stored on the card, the safety-lock status and the safety signature are shown.

The project must be online to see the contents of the memory card.

Remember the following:

- A memory card slot is on the front of the controller behind the door.
- If the memory card is installed and a fault occurs, diagnostic data is automatically written to the card. Diagnostic data helps the investigation and correction of the fault cause.
- The controller detects the presence of a memory card at power-up or if a card is inserted during controller operation.
- The memory card can store all configuration data that is stored in nonvolatile memory.
- The memory card can store the back-up program.

IMPORTANT: We recommend that you back up your controller project to a memory card regularly. If a major non-recoverable fault occurs that removes the program from the controller memory, the backup copy on the memory card can be automatically restored to the controller and quickly resume normal controller operation.

For detailed information on how to use nonvolatile memory, refer to the Logix 5000 Controllers Nonvolatile Memory Programming Manual, publication 1756-PM017.

Safety Project Considerations

You cannot store a safety project if the safety task status is Safety Task Inoperable. When you store a safety project, the controller firmware is also stored to the memory card.

If no application project exists in the controller, you can save only the firmware of the controller if a valid partnership exists, you can only save the firmware of the internal safety partner.

A firmware-only load does not clear a Safety Task Inoperable condition.

If a safety signature exists when you store a project, the following occurs:

- Both safety and standard tags are stored with their current values.
- The current safety signature is saved.

When you store a safety application project on a memory card, we recommend that you select Program (Remote Only) as the Load mode, that is, the mode that the controller enters after a project is loaded from the memory card.

IMPORTANT: To help prevent the firmware that is stored on the memory card from overwriting newly updated firmware:

- The update process first checks the load option on the memory card and changes the load option to User Initiated if necessary.
- The firmware update process.
- The controller resets.
- The load option remains set to User Initiated.

If the memory card is locked, the load option does not change, and the firmware that is stored on the memory card can overwrite the newly updated firmware.

Store to the Memory Card

We recommend that you back up your controller project to a memory card regularly. If a major nonrecoverable fault occurs that removes the program from the controller memory, the backup copy on the memory card can be automatically restored to the controller to resume normal controller operation.

To store a project to the memory card, complete these steps.

1. Make sure that the controller is online in Program mode or Remote Program mode.
2. In the Controller Organizer, double-click the controller to open the Controller Properties dialog box.
3. Click the Nonvolatile Memory tab.
4. On the right side of the Nonvolatile Memory tab, click Load/Store.

   If Load/Store is dimmed, verify the following:

   - The controller is in Program mode or Remote Program mode.
   - You specified the correct communication path.

- The memory card is installed.
- The memory card is unlocked. The locked status appears in the bottom-left corner of the Nonvolatile memory/Load Store dialog box.

If the memory card is not installed, a message in the lower-left corner of the Nonvolatile Memory tab indicates the missing card.

5. In the Load Image field, select a setting according to your application requirements described in the following table.

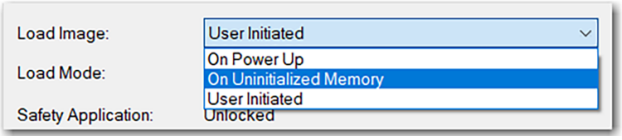


Table 12. Choose a Load Image Setting

Application Requirement	Load Image Setting	Description	Safety Considerations
Load image when you turn on or cycle power	On Power Up	- During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory. - The controller loads the stored project and firmware at every powerup regardless of the firmware or application project on the controller. - You can always use the Logix Designer application to load the project.	For a safety project, On Power Up loads whether the controller is safety-locked or there is a safety signature.
Load image when there is no project in the controller and you turn on or cycle chassis power	On Uninitialized Memory	- If the project has been cleared from memory, this option loads the project back into the controller on powerup. - The controller updates the firmware on the controller, if necessary. The application project that is stored in nonvolatile memory	The controller also updates the firmware on the safety partner, if necessary.

Application Requirement	Load Image Setting	Description	Safety Considerations
		is also loaded and the controller enters the selected mode, either Program or Run. - You can always use the Logix Designer application to load the project.	
Load image only from the Controller Properties dialog in the Logix Designer application	User Initiated	If the controller type and the major and minor revisions of the project in nonvolatile memory match the controller type and major and minor revisions of the controller, you can initiate a load.	- You can initiate a load, regardless of the Safety Task status. - You can load a project to a safety-locked controller only when the safety signature of the project that is stored in nonvolatile memory matches the project on the controller. - If the signatures do not match or the controller is safety-locked without a safety signature, you are prompted to first unlock the controller. When you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety signature are set to the values contained in nonvolatile memory once the load is complete. - If the firmware on the primary controller matches the revision in nonvolatile memory, the safety partner firmware is updated, if necessary, the application that is stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the Program mode.

IMPORTANT: To help prevent the firmware that is stored on the memory card from overwriting newly updated firmware:

- The update process first checks the load option on the memory card and changes the load option to User Initiated if necessary.
- The firmware update proceeds.
- The controller resets.
- The load option remains set to User Initiated.

If the memory card is locked, the load option does not change, and the firmware that is stored on the memory card can overwrite the newly updated firmware.

6. In the Load Mode field, choose the mode that you want the controller to go to after loading:
   - Program (Remote Only)
   - Run (Remote Only)

IMPORTANT: Safety Consideration

We recommend that you use Program (Remote Only), when you set the Load Mode for a safety application project

7. According to your application requirements, set the Automatic Firmware Update properties for I/O devices in the configuration tree of the controller. The Automatic Firmware Update property is also referred to as the Firmware Supervisor feature.

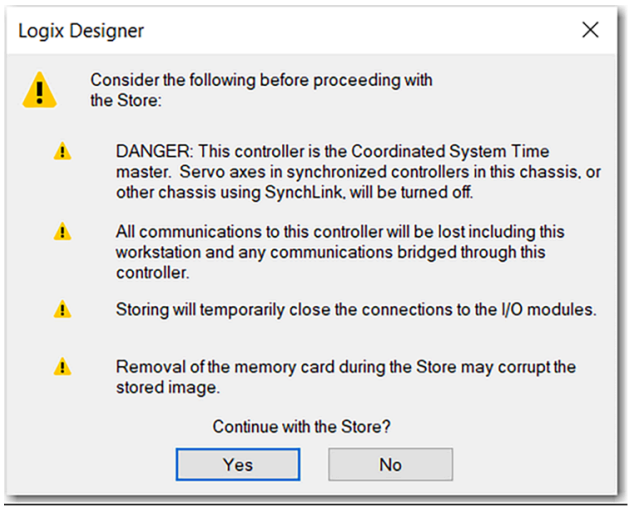
IMPORTANT: Safety Consideration

Some Safety I/O devices do not support the Firmware Supervisor feature.

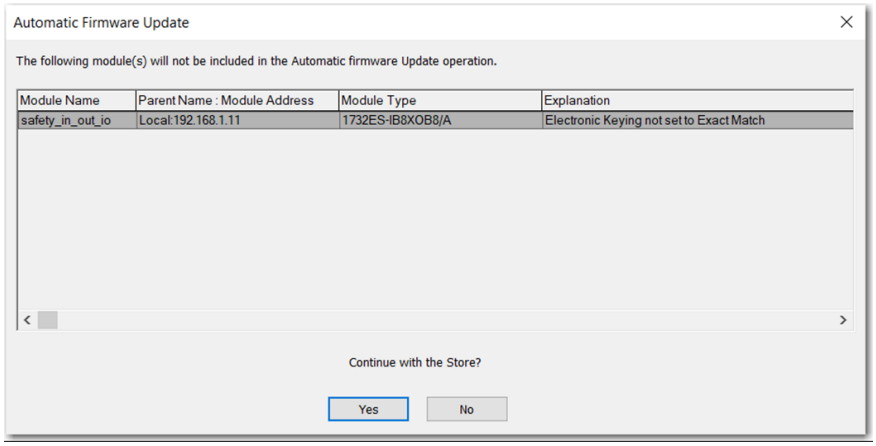
This table describes the Automatic Firmware Update options for I/O devices.

Setting	Description
Disable	- Disables any automatic firmware updates. - This item only appears in the menu when you initially save the image.
Enable and Store Files to Image	- Enables automatic firmware updates for I/O devices in the configuration tree of the controller. - Saves I/O device firmware and controller firmware to the image. - Only I/O devices that are configured for Exact Match Keying participate in the Automatic Firmware Update process. The devices that are used with this option must support the revision of firmware being updated to.
Disable and Delete Files from Image	- Disables automatic firmware updates for I/O devices in the configuration tree of the controller. - Removes I/O device firmware from the image but does not remove controller firmware from the image. - This item only appears in the menu on subsequent saves of the image.

8. Click Store.
9. Click Yes in the confirmation dialog box that appears.



If you enabled Automatic Firmware Update, then a dialog box appears to inform you which modules are not included in the Automatic Firmware Update operation.



IMPORTANT: Do not remove the memory card while the controller is reading from or writing to the card.

If you remove the card during either activity, the data on the card or controller can become corrupt.

Also, the controller firmware at the time when the card is removed can become corrupt. Leave the card in the controller until the OK status indicator turns steady green.

10. On the Automatic Firmware Update dialog box, click Yes.
The project is saved to the memory card as indicated by the controller status indicators. While the store is in progress, the following occurs:
    - OK indicator is flashing green.
    - Memory card is flashing green.
    - Saving...Do Not Remove SD Card is shown on the status display.
    - A dialog box in the Logix Designer application indicates that the store is in progress.
    - Controller resets.
    - SAVE is shown on the status display.

When the store is complete, the controller resets.

IMPORTANT: Allow the store to complete without interruption. If you interrupt the store, data corruption or loss can occur.

Load from the Memory Card

After you set the communication path, are online with the controller, and changed the controller to Program mode, you can load a project to the controller from the memory card.

IMPORTANT: With the memory card and new, out-of-box controllers:

- If you insert a memory card with an image into a new, out-of-box controller (firmware 1.x), then at powerup, the controller automatically updates the firmware up to the version of firmware that is stored on the memory card. The update happens regardless of the Load Image setting in the image on the memory card (User Initiated, On Power Up, or On Uninitialized Memory).
- If the image was created with either On Power Up or On Uninitialized Memory settings, then the controller both updates the firmware and loads in the controller application.

You can load from a memory card to a controller in one of the following ways:

- Controller powerup
- User-initiated action

Controller Powerup

This table shows what happens at powerup when you insert a memory card that contains an image into a controller.

Image Setting	Controller is in out-of-box condition (v1.x firmware)	Firmware > 1.x and internal nonvolatile memory is not valid ("Valid" includes the No Project condition)	Firmware > 1.x and internal nonvolatile memory is valid ("Valid" includes the No Project condition)
User Initiated	Loads Firmware Only (firmware is only loaded on the controller, not the safety partner)	Does Nothing	Does Nothing
On Power Up	Loads both Firmware and Application	• Loads Firmware if there is a revision mismatch • Loads Application	• Loads Firmware if there is a revision mismatch • Loads Application
On Uninitialized Memory	Loads both Firmware and Application	• Loads Firmware if there is a revision mismatch • Loads Application	Does Nothing

User-initiated Action

IMPORTANT: For an out-of-box controller that uses firmware revision 1.xx, you must manually update the controller to the required firmware revision before you can load a project on the controller.

You must complete the following before you can load a project to the controller from the memory card when the controller is already powered-up:

- Make sure that the controller has a working firmware revision.
- Establish the communication path.
- Go online with the controller.
- Make sure that the controller is in Program mode.

To load a project to the controller from the memory card, complete these steps.

1. In the Controller Organizer, double-click the controller to open the Controller Properties dialog box.
2. Click the Nonvolatile Memory tab.
3. Under Image in Nonvolatile Memory, verify that the name of the controller project that is listed is the correct one.

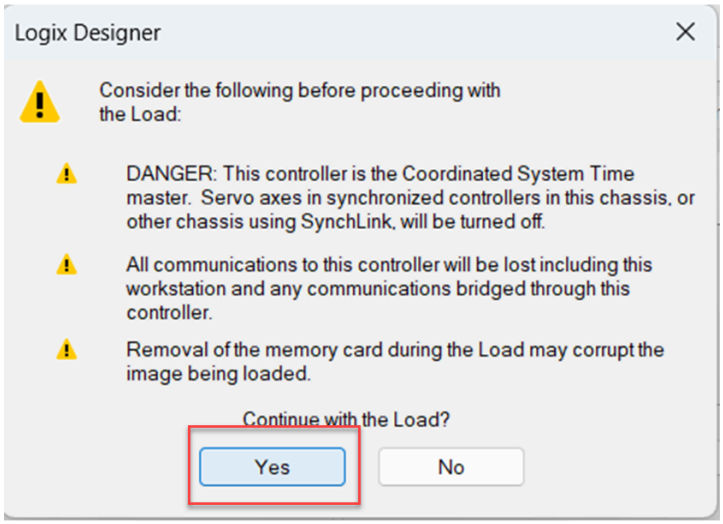
   If no project is stored on the memory card, a message on the Nonvolatile Memory tab indicates that an image (or project) is not available.

   For information on how to change the project that is available to load from nonvolatile memory, see the Logix 5000 Controllers Nonvolatile Memory Programming Manual, publication 1756-PM017.

4. On the right side of the Nonvolatile Memory tab, click Load/Store.

   If Load/Store is dimmed (unavailable), verify the following:
   - You have specified the correct communication path and are online with the controller.
   - The SD card is installed.
   - The controller is not in Run Mode.

5. On the bottom of the Nonvolatile Memory tab, click Load.
6. Click Yes on the confirmation dialog box that appears.



After you click Yes, the project is loaded to the controller as indicated by the controller status indicators. A dialog box in the Logix Designer application also indicates that the store is in progress.

Table 13. Controller Status Indicators

Controller	SD Indicator	OK Indicator	4-character Display Message
Controller when restoring firmware or project	Flashing Green	Steady Red	"LOAD", then followed by "UPDT"
SIL 2 controller when restoring firmware or project	Flashing Green	Steady Red	"LOAD", then followed by "UPDT"
SIL 3 controller during primary controller firmware update	Flashing Green	Steady Green	"Updating Firmware...Do Not Remove SD Card"
SIL 3 controller during Safety Partner firmware update	Flashing Green	Steady Green	"Updating Firmware...Do Not Remove SD Card"
SIL 3 controller when loading project	Flashing Green	Steady Green	"Loading...Do Not Remove SD Card"

When the load is complete, the controller reboots.

Other Memory Card Tasks

You can perform these tasks with the memory card:

- Change the image that is loaded from the card
- Check for a load that was completed
- Clear an image from the card
- Store an empty image
- Change load parameters
- Read/write application data to the card
- View safety-lock status and safety signatures on the Nonvolatile Memory tab

For more information on how to complete any of these tasks, see the Logix 5000 Controllers Memory Card Programming Manual, publication 1756-PM017.

Manage Controller Communication

The controller provides connection resources whenever communication is established between two devices.

Connections are used when the system contains the following conditions or activities:

- I/O modules, communication modules, and adapters are present in the I/O configuration of the user project.
- Produced or consumed tags are configured in the user project.
- Connected Messages are executed in the user application.
- External devices, programming terminals, or HMIs communicate with the controller.

When configuring your control system, you must account for the number of EtherNet/IP™ nodes you include in the I/O configuration tree in your project. The following table shows the maximum number of EtherNet/IP™ nodes that are supported for each controller.

Table 14. Maximum EtherNet/IP Nodes Supported for ControlLogix

Cat. No.	Version 28	Version 29	Version 30	Version 31 or later	Version 36 or later
1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	–	60	100	100	100
1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	–	80	175	175	175
1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	100	100	250	250	250
1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	–	150	250	250	250
1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP	300	300	300	300	300
1756-L81ES, 1756-L81ESK, 1756-L81EXTS	–	–	–	100	100

Table 14. Maximum EtherNet/IP Nodes Supported for ControlLogix (continued)

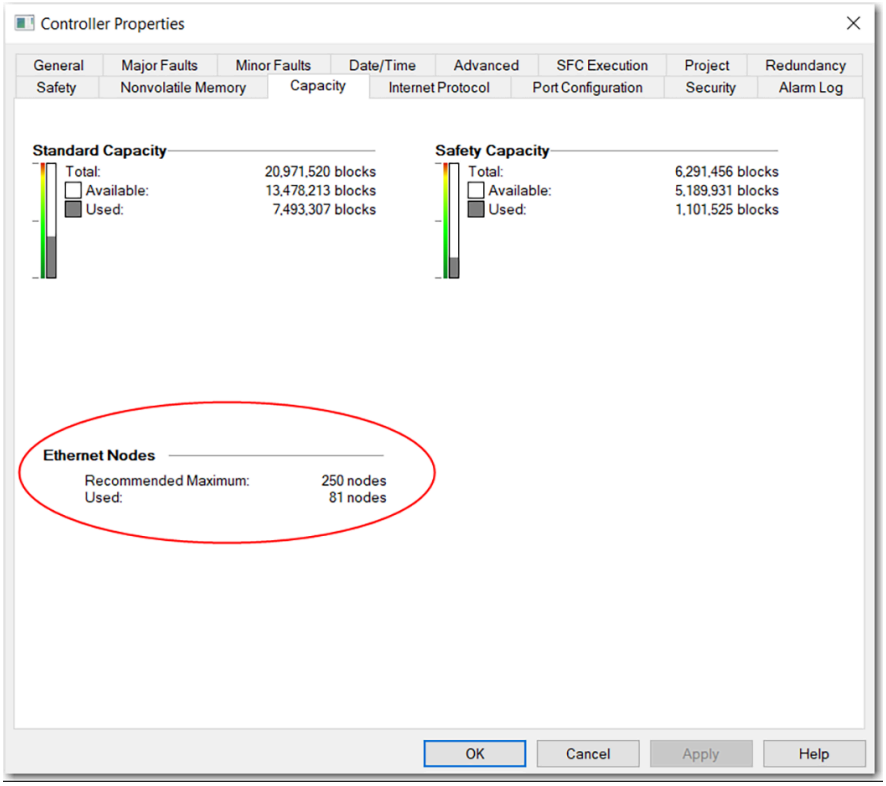
Cat. No.	Version 28	Version 29	Version 30	Version 31 or later	Version 36 or later
1756-L82ES, 1756-L82ESK, 1756-L82EXTS	–	–	–	175	175
1756-L83ES, 1756-L83ESK, 1756-L83EXTS	–	–	–	250	250
1756-L84ES, 1756-L84ESK, 1756-L84EXTS	–	–	–	250	250
1756-L85ES	–	–	–	–	300

Table 15. Maximum EtherNet/IP Nodes Supported for GuardLogix

Cat. No.	Version 28	Version 29	Version 30	Version 31 or later	Version 36 or later
1756-L81ES, 1756-L81ESK, 1756-L81EXTS	–	–	–	100	100
1756-L82ES, 1756-L82ESK, 17 56-L82EXTS	–	–	–	175	175
1756-L83ES, 1756-L83ESK, 1756-L83EXTS	–	–	–	250	250
1756-L84ES, 1756-L84ESK, 1756-L84EXTS	–	–	–	250	250
1756-L85ES	–	–	–	–	300

With firmware revision 29 or later, the Capacity tab on the Controllers Properties dialog box keeps a running count as you add nodes to the I/O configuration tree.

Figure 21. Maximum Number of Ethernet Nodes



Devices Included in the Node Count

Any EtherNet/IP™ devices that you add to the I/O configuration section are counted toward the controller node limits. The following are examples of devices that must be counted:

- Remote communication adapters
- Remote controllers
- Devices with an embedded EtherNet/IP port
- EtherNet/IP™ devices that connect to a communication module in the local chassis, even though the communication module in the local chassis does not count as a node
- HMI devices that are included in the I/O configuration section
- Third-party devices that are directly connected to the EtherNet/IP™ network

Devices Excluded from the Node Count

When considering the EtherNet/IP™ node limitation of a ControlLogix® 5580 controller, you do not count Ethernet devices that exist on the EtherNet/IP™ network but are not added to the I/O configuration section of the project.

The following devices are not added to the I/O configuration section in your project and are not counted among the total number of nodes:

- Computer
- Communication modules in the local chassis
- HMIs that are not added to the I/O configuration section
- Devices that are the target of MSG Instructions
- Standard Ethernet devices with which the controller communicates via a socket interface

The following example shows four nodes in the I/O tree.

Figure 22. Ethernet Nodes Example

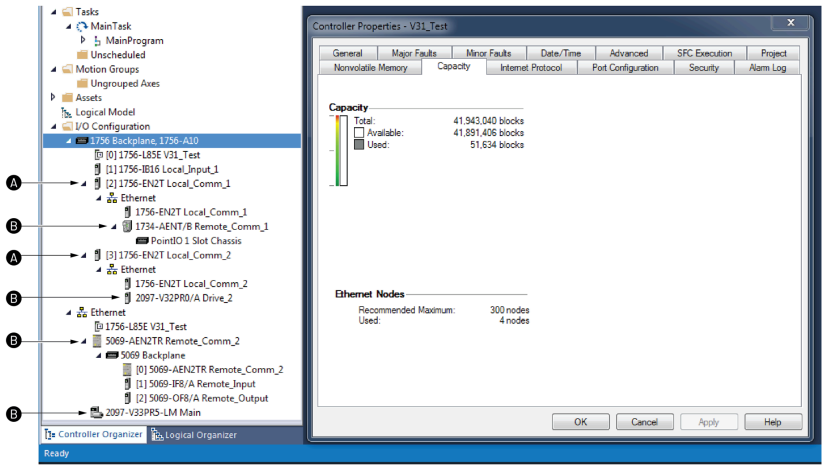


Table 16. Item Description

Item	Description
A	Not a node. Module is in the local chassis.
B	Node

Controller Communication Interaction with Control Data

The controller runs the communication task separately from the application code. The controller runs communication asynchronously to the application. Therefore, it is important to make sure that communication that is delivered to the controller is complete before the application executes on the newly delivered data. This applies to data that is coming into the controller and data that is going out from the controller.

For example, if an HMI device writes a large block of recipe data to the controller, the application code can start to execute on that data before the data is written. This action results in half of the current recipe and half of the last recipe in the application space.

You can use the following methods to control the effects of asynchronous communication. Blocking access helps to prevent source data values from changing by communication during application execution. Allowing access means that communication can change source data values during application execution.

Table 17. Controller Behavior

Application Construct	Tag Access					
	HMI	MSG	I/O Update	Produce/Consume	Other User Tasks	Motion Planner
UID/UIE	Allows	Allows	Allows	Allows	Blocks	Allows
CPS	Blocks	Blocks	Blocks	Blocks	Allows	Allows
Periodic Task	Allows	Allows	Allows	Allows	Allows	Allows

These options rely on controlling when the main core can switch tasks. As a result, the communication task cannot change data when the control task is using it. Because the controller processes communication on an independent CPU core, these methods are no longer effective in all cases.

Because the controllers have 32-bit data integrity, this only applies to data structures larger than 32 bits. If word-level integrity is your primary concern, the 32-bit data integrity does not impact your data use.

Good programming practice dictates the use of two unique words at the beginning and the end of data. The controller validates the words to assure the entire structure has data integrity. We recommend that the handshake data is changed and the application code validates it every transaction before the controller application code or higher-level system reading controller data acts on it.

The following table shows that two data elements added to a structure for data integrity checking: Start Data and End Data. We recommend that the controller validates the Start Data value and the End Data value match before the controller acts on My_Recipe1.

If the Start Data and End Data values do not match, it is likely that communication is in the process of filling the structure. The same applies to higher-level systems that are receiving data from the controller.

Table 18. Data Elements

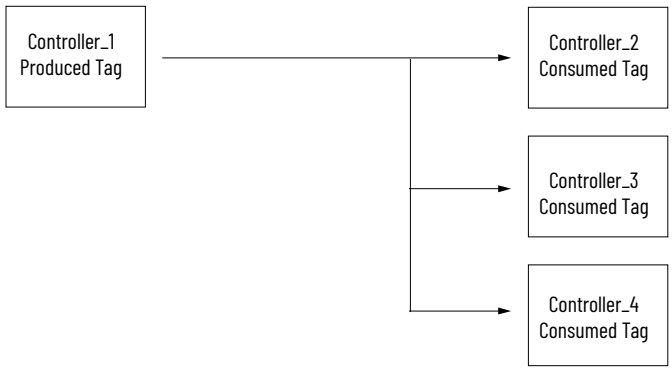
Structure	My_Recipe1	My_Recipe2	My_Recipe3
Start Data	101	102	103
Sugar	3	4	8
Flour	4	3	9
Chocolate	2	2	4
Oil	6	7	2
End Data	101	102	103

We recommend that you perform this test on a buffered copy of the data and not the actual data element being written to by the communication core. If you use buffered data, you help prevent the risk of the communication core changing data after you have passed the data valid test.

Produce and Consume (Interlock) Data

The controllers let you produce (transmit) and consume (receive) controller-scoped tags. Logix 5000® controllers produce the same standard tag through both the Ethernet port and the backplane, and consumer counts apply to the total consumers from both ports.

Figure 23. Illustration of Produced and Consumed Tags



The following table describes the system-shared tags.

Table 19. Produced and Consumed Tag Definitions

Tag	Definition
Produced tag	A tag that a controller makes available for use by other controllers. Multiple controllers can simultaneously consume (receive) the data. A produced tag sends its data to one or more consumed tags (consumers) without using logic.
Consumed tag	A tag that receives the data of a produced tag. The data type of the consumed tag must match the data type (including any array dimensions) of the produced tag. The RPI of the consumed tag determines the period at which the data updates.

For two controllers to share produced or consumed tags, the controllers must be attached to the same network. You cannot bridge produced and consumed tags over two networks.

Produced and consumed tags use the connections of the controller and communication modules.

Safety controllers can also use produced and consumed safety tags.

For more information on how to use them, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

For a ControlNet® network, produced and consumed tags use scheduled connections.

Requested Packet Interval (RPI) of Multicast Tags

The first consumer of a multicast produced tag on any communication port establishes the RPI value for that port. All subsequent consumers using the same port must request the same RPI value as the first consumer, otherwise they fail to connect. Controllers with backplane and Ethernet ports can produce data at an independent RPI value on each port.

For more information about produced/consumed tags, see the Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011.

Send and Receive Messages

Messages transfer standard or safety data to other devices, such as other controllers or operator interfaces. The MSG instruction is a ladder logic output instruction that asynchronously

reads or writes a block of data to or from another module over the backplane or a network. The size of the instruction depends on the data types and message command that you program.

Messages use connection resources to send or receive data. Messages can leave the connection open (cached) or can close the connection when the message is done transmitting.

Messages can be either unconnected or connected. Unconnected messages are dependent upon the availability of unconnected buffers in all devices through which the message passes. Connected messages begin with a request to allocate connection buffers in all of those devices, before sending the actual message. Choosing to cache a connected message instructs the controller to keep the connection open after the message has been completed - this improves efficiency if the message is intended to be sent repeatedly.

Connected messages use connection resources. If the connected message is uncached, the resources are used temporarily each time the message is triggered. As long as a cached connected message remains in the cache, the resources remain allocated and are not available for other messages. Messages can get pushed from the cache if the application exceeds the cache capacity of the controller.

Each message uses one connection out of the controller, regardless of how many devices are in the message path. You can connect CIP™ generic messages. However, for most applications we recommend that you leave CIP™ generic messages unconnected. Connected messages that occur more frequently than once every 60 seconds should be cached if possible.

Table 20. Message Types

Message Type	Communication Method	Connected Message	Message Can Be Cached
CIP™ data table read or write	N/A	Configurable	Yes
PLC-2®, PLC-3®, PLC-5®, or SLC™(all types)	CIP™	No	No
	CIP™ with Source ID	No	No
	DH+™	Yes	Yes
CIP™ generic	N/A	Optional	Yes
Block-transfer read or write	N/A	Yes	Yes

For more information about how to use messages, see the Logix 5000 Controllers Messages Programming Manual, publication 1756-PM012.

Cache Message Connections

When you configure an MSG instruction, you can choose whether to cache the connection. Cached connections transfer data faster than uncached connections. The controllers can cache 256 messages and trigger 256 messages simultaneously.

The following table describes the options for caching connections.

Table 21. Options for Caching Connections

Frequency of Message Execution	Action
Repeatedly	Cache the connection. This keeps the connection open and optimizes execution time. Opening a connection each time the message executes increases execution time.
Infrequently	Do not cache the connection. This closes the connection upon completion of the message, which frees up that connection for other uses.

Socket Interface

The controller can use socket interfaces to communicate with Ethernet devices that do not support theEtherNet/IP™ application protocol. The socket interface is implemented via the socket object. The controller communicates with the socket object via MSG instructions.

MSG instructions that configure and operate the socket interface must be configured as Unconnected and use the Message to Self path. To communicate with another device, you must understand the application protocol of the other device.

IMPORTANT: Keep these in mind when you use sockets with the controllers:

- Use unconnected MSG instructions for socket servers. When you configure a MSG instruction, make sure that the Connected checkbox on the Message Configuration dialog box is cleared.
- When a controller operates in Dual-IP mode and uses a socket object, you can use an IP address with a Socket_Create service type.

These devices support as many as 32 socket instances each:

- Controllers, firmware revision 35.011 or later
- 1756-EN4TR modules, firmware revision 5.001 or later

For more information on the socket interface, see the EtherNet/IP Socket Interface Application Technique, publication ENET-AT002.

TLS Support

The secure socket option adds support for Transport Layer Security (TLS) to the socket object.

HTTP(S) REST API Client Support

You can develop your application to send HTTP REST API requests and implement HTTPS via the socket interface with TLS. For more information, see the documentation for these objects in the Common Application Library available from the Product Compatibility and Download Center at rok.auto/pcdc:

- raC_Impl_HTTPClient
- raC_Impl_HTTPCmdGET
- raC_Impl_HTTPCmdPOST
- raC_Impl_HTTPCmdPUT

Use a CIP Generic MSG to Enable SNMP on the Controller

Simple Network Management Protocol (SNMP) enables the controller to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. SNMP is disabled on the controller by default. If the port is disabled, you can enable SNMP on the controller with a CIP Generic MSG (firmware revision 32 or later).
For more information about SNMP, see the Ethernet Reference Manual, publication ENET-RM002.

1. Add an MSG instruction to your program.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in RUN mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.

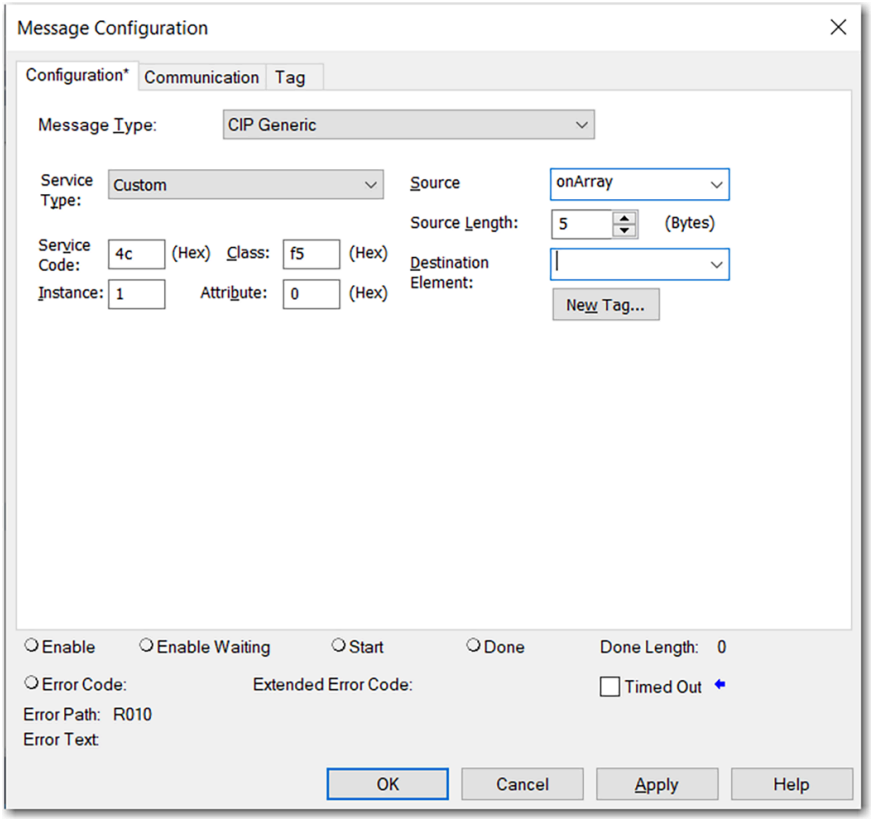
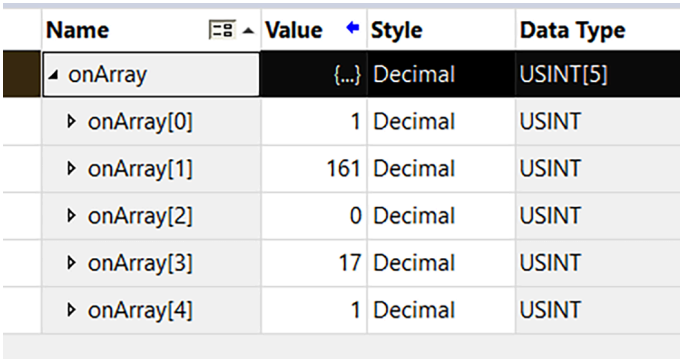


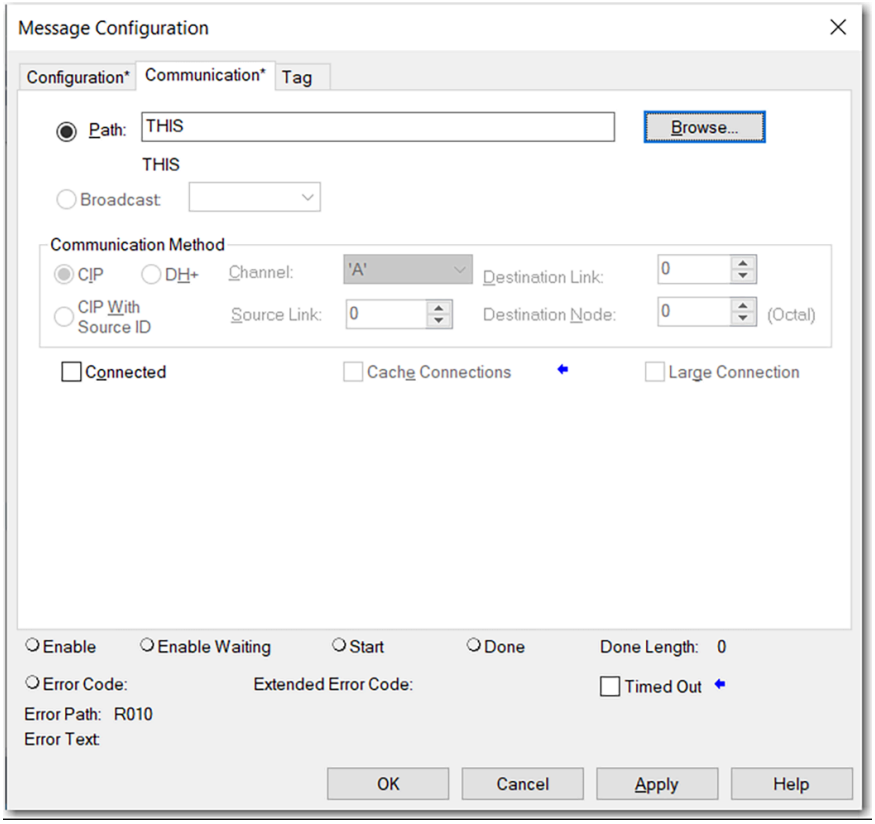
Table 22. Enable SNMP

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 = controller with single Ethernet port or configured for Linear/DLR mode 2 = controller configured for Dual-IP mode

Field	Description
Class	f5
Attribute	0
Source Element	Controller tag of USINT[5] data type. In this example, the controller tag is named onArray and must match the following graphic.  **IMPORTANT**: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP will not be enabled.
Source Length	5

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



Use a CIP Generic MSG to Disable SNMP on the Controller

Simple Network Management Protocol (SNMP) enables the controller to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. SNMP is disabled on the controller by default. If the port is enabled, you can disable SNMP on the controller with a CIP Generic MSG (firmware revision 32 or later).
For more information about SNMP, see the Ethernet Reference Manual, publication ENET-RM002.

1. Add an MSG instruction to your program.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in RUN mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.

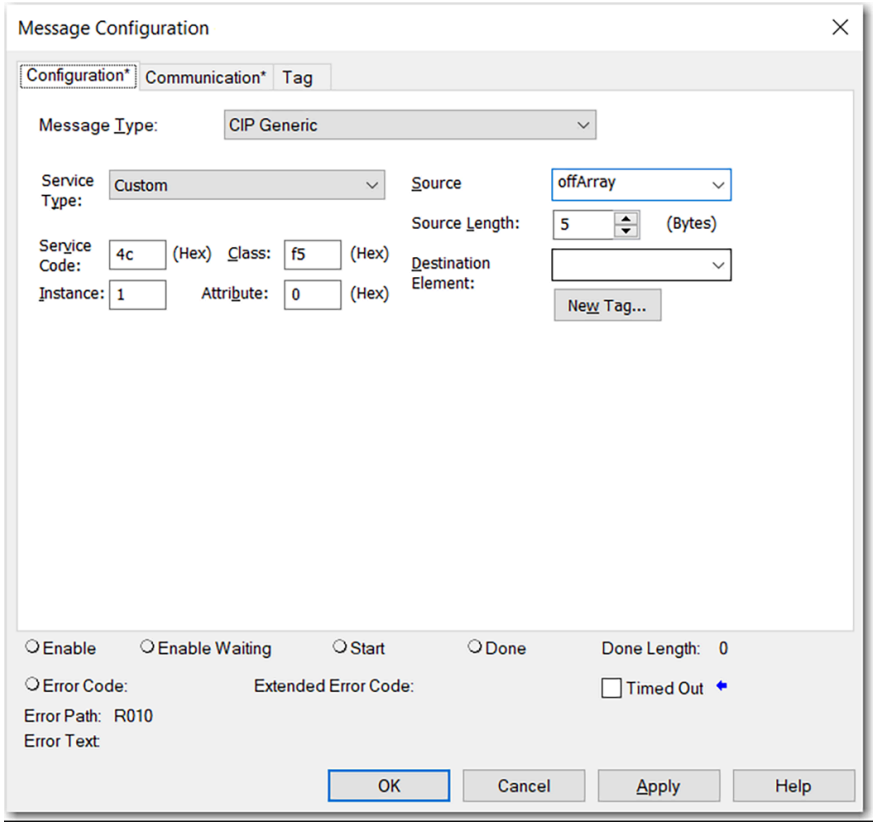
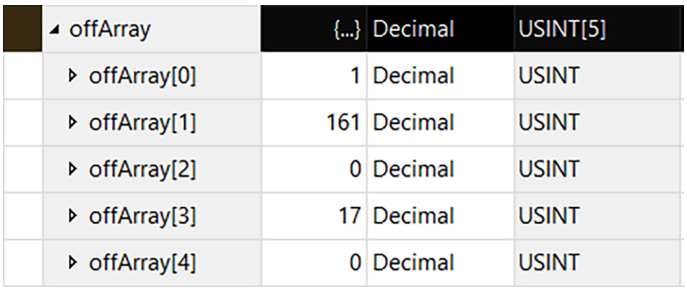


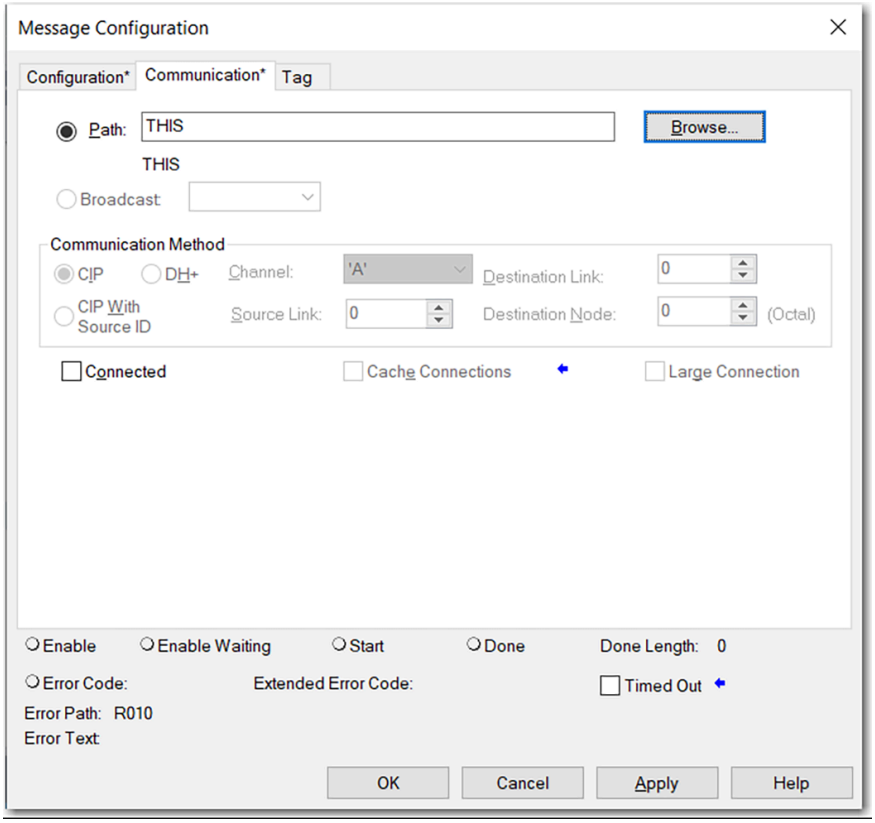
Table 23. Enable SNMP

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 = controller with single Ethernet port or configured for Linear/DLR mode 2 = controller configured for Dual-IP mode
Class	f5
Attribute	0
Source Element	Controller tag of USINT[5] data type. In this example, the controller tag is named offArray and must match the following graphic.

Field	Description
	 **IMPORTANT**: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP is not disabled.
Source Length	5

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



Trusted Slots on the Controller

Trusted slots help maintain network segmentation when a controller front Ethernet port is disabled, such as in redundant control systems. Trusted slots restrict communication paths through which certain operations are performed on the controller.

IMPORTANT: Trusted slots and CIP Security™ are not compatible on the same device. If both features are used on the same device, programming through the controller front Ethernet port is disabled and you are locked out of programming the controller until you perform a physical reset.

To meet IEC-62443-4-2 SL 1 certification requirements, you must not configure Trusted slots on the controller and instead use CIP Bridging Control on page 156.

Trusted slots help maintain network segmentation when the controller front Ethernet port is disabled, such as in redundant control systems. Trusted slots restrict communication paths through which certain operations are performed on the controller.

The following rules apply to Trusted slots:

- The firmware revisions of the physical modules in the Trusted slots must be compatible with the firmware revisions and electronic keying options that are configured in the I/O tree of the project. For compatibility, see Electronic Keying on page 100.
- All communication is Trusted from the module as long as there is not a fault or keying mismatch.
- If no module is configured in the I/O tree for the respective Trusted slot, then all communication is Trusted regardless of which module is physically present.

You configure Trusted slots with the parameters on the Security tab of the Controller Properties dialog box.

Restrict Communication Except Through Selected Slots

Select this checkbox to restrict communication through any slot in the chassis that is not Trusted. Clear the checkbox to allow the controller to communicate without communication restrictions.

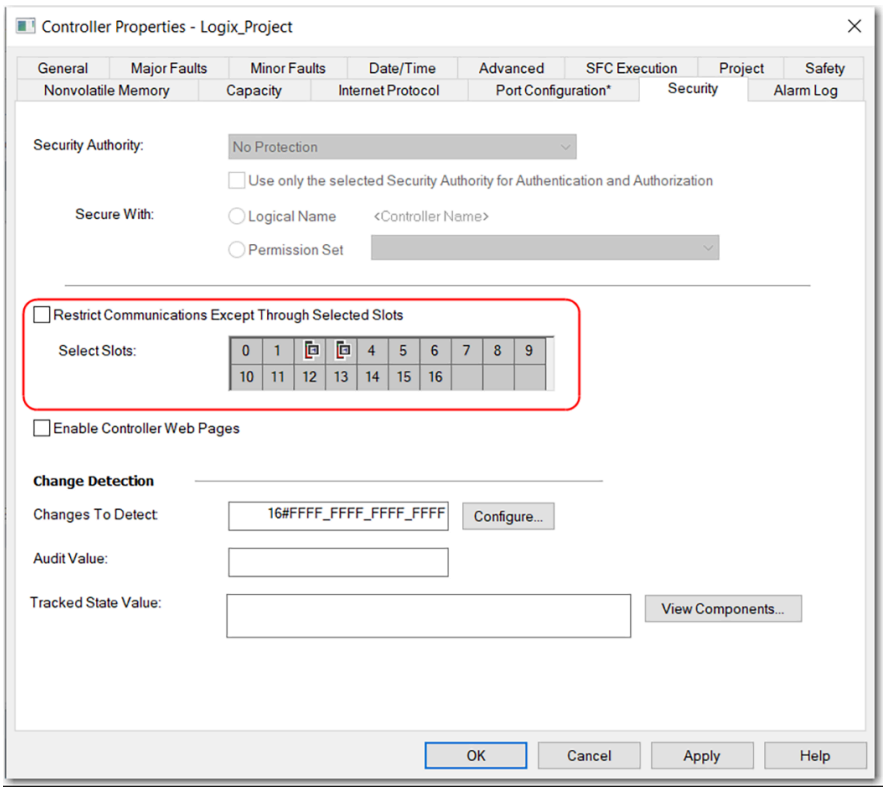
IMPORTANT: When this checkbox is selected, communication is restricted through the front Ethernet port and firmware updates are restricted to Trusted slots when using AutoFlash, or ControlFLASH Plus® software. Support is restricted for tools that require access to restricted data through Class 3 connections.

Select Slots

Only the slots that are selected under Select Slots are Trusted communication paths for the controller. The Select Slots grid configures the trusted slots for the controller. When you select the Restrict Communications Except Through Selected Slots checkbox, you must click at least one slot that is not occupied by the controller.

If the chassis size for the project is known, the number of slots equal to the chassis size appear on the dialog box. Otherwise, 17 slots (0...16) appear on the dialog box.

Figure 24. Selected Slot Options



Standard I/O Modules

Rockwell Automation offers many I/O modules for use in ControlLogix® controller systems. When you select I/O modules, remember the following:

- A wide variety of digital, analog, and specialty I/O modules support the following features:
  - Field-side diagnostics
  - Electronic fusing
  - Individually isolated inputs/outputs
  - Timestamping of inputs
  - Scheduling of outputs
  - Event detection of specific input patterns
- Removable terminal blocks (RTBs) or 1492 wiring systems are required for I/O modules.
- 1492 PanelConnect™ modules and cables can be used to connect input modules to sensors.

Electronic Keying

Electronic Keying reduces the possibility that you use the wrong device in a control system. It compares the device that is defined in your project to the installed device. If keying fails, a fault occurs. These attributes are compared.

Attribute	Description
Vendor	The device manufacturer.
Device Type	The general type of the product, for example digital I/O module.
Product Code	The specific type of the product. The Product Code maps to a catalog number.
Major Revision	A number than represents the functional capabilities of a device.
Minor Revision	A number that represents behavior changes in the device.

The following Electronic Keying options are available.

Keying Option	Description

Compatible Module	Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has the following characteristics:
	• Same catalog number
	• Same or higher Major Revision
	• Minor Revision as follows:
	  - If the Major Revision is the same, the Minor Revision must be the same or higher.
	  - If the Major Revision is higher, the Minor Revision can be any number.

Disable Keying	Indicates that the keying attributes are not considered when attempting to communicate with a device. With Disable Keying, communication can occur with a device other than the type specified in the project.

Keying Option	Description
	ATTENTION: Be cautious when using Disable Keying; if used incorrectly, this option can lead to personal injury or death, property damage, or economic loss. We **strongly recommend** that you **do not** use Disable Keying. If you use Disable Keying, you must take full responsibility for understanding whether the device being used can fulfill the functional requirements of the application. **IMPORTANT:** For safety I/O devices, do not use Disable Keying.
Exact Match	Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.

Carefully consider the implications of each keying option when selecting one.

IMPORTANT: When you change Electronic Keying parameters online, it interrupts connections to the device and any devices that are connected through the device. Connections from other controllers can also be broken.

If an I/O connection to a device is interrupted, the result can be a loss of data.

For more detailed information on Electronic Keying, see Electronic Keying in Logix 5000 Control Systems Application Technique, publication LOGIX-AT001.

Local I/O Modules

The ControlLogix® chassis that you choose affects how many local I/O modules you can use. Several ControlLogix® chassis sizes are available to suit your configuration requirements. You can fill the slots of your chassis with any combination of controllers, communication modules, and I/O modules.

Table 24. ControlLogix and ControlLogix-XT Chassis and Slots

Chassis	Slots
1756-A4	4
1756-A7	7
1756-A7XT	
1756-A10	10
1756-A10XT	
1756-A13	13
1756-A17	17

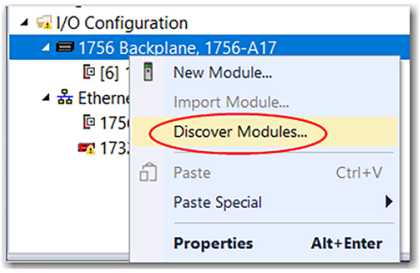
If you have empty slots in your chassis, you can use the 1756-N2 or 1756-N2XT slot-filler module.

Discover Local I/O Modules

While your Studio 5000 Logix Designer® application project is online, you can discover I/O modules to add them to the project.

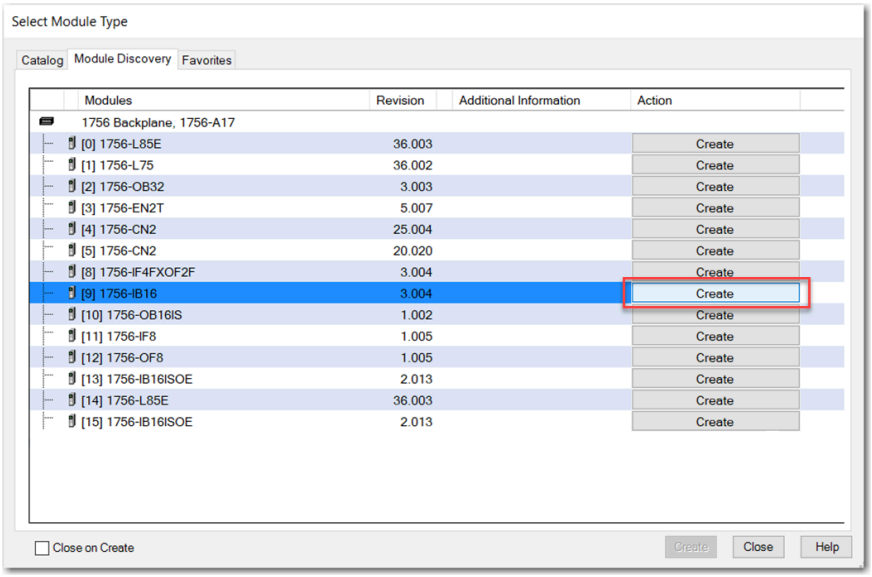
To use the Discover Modules option, complete the following steps.

1. Go online with the controller, if you are not online already.
2. In the I/O Configuration, click the backplane and choose Discover Modules.

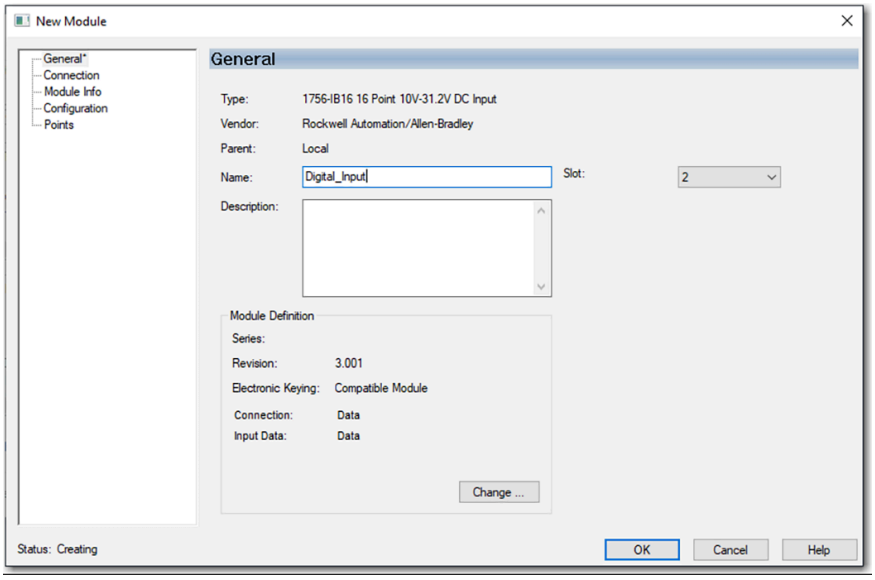


The Logix Designer application automatically detects available modules that are installed in the system.

3. On the Select Module Type dialog box, click Create next to the discovered module to add to your project.

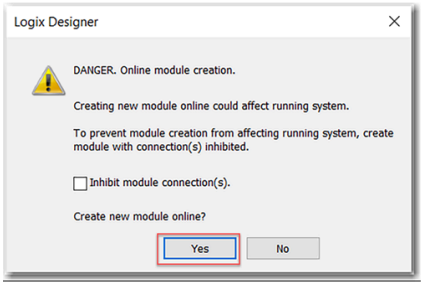


4. Configure the properties for the new module, and click OK.



5. At the warning dialog box, click Yes and then close the Select Module Type dialog box.

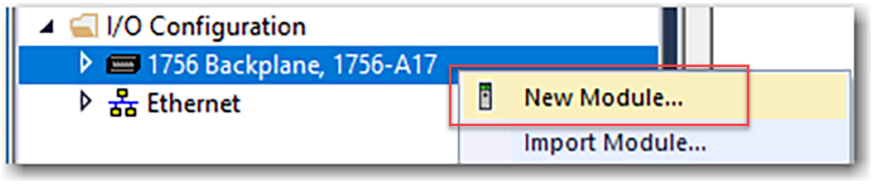
IMPORTANT: If you inhibit the module connection, you must remember to uninhibit the connection later.



Add Local I/O Modules

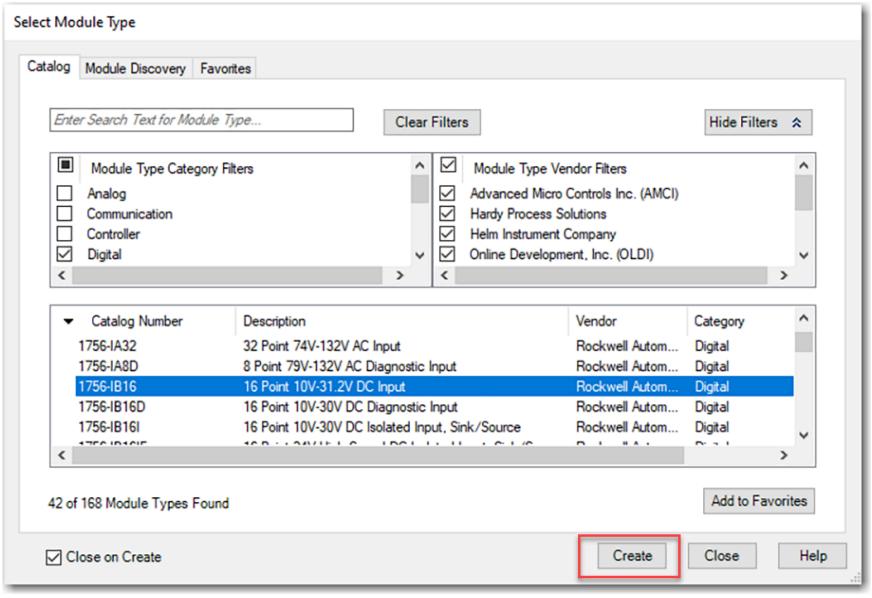
While your controller project is offline, use the New Module option to add I/O modules to add them to the project. To add modules while the project is offline, complete the following steps.

1. In the I/O configuration, right-click the backplane and select New Module.

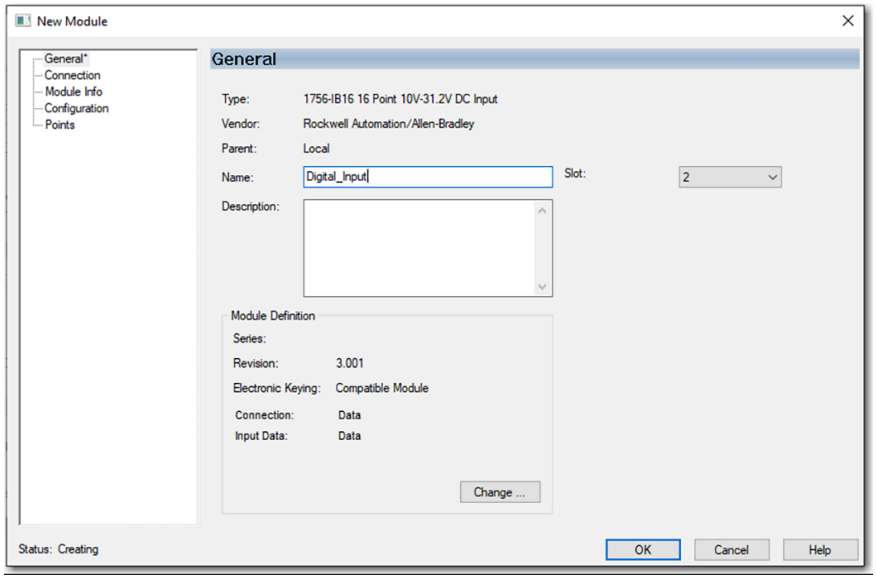


2. On the Select Module Type dialog box, select the I/O module and click Create.

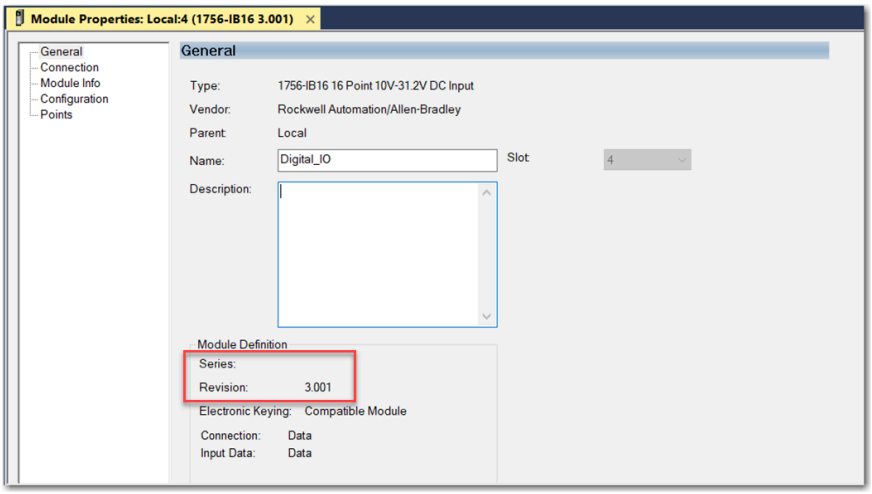
Use the filters to reduce the list of modules to choose from.



3. On the New Module dialog box, configure the module and click OK.



If the series or revision values in the module properties do not match those of the module for which this configuration is intended, your project can experience module faults.



Remote I/O Modules

Remote I/O refers to I/O modules that are not in the local chassis and connect to the controller via a communication network. There are several families of I/O modules that are remote from the controller:

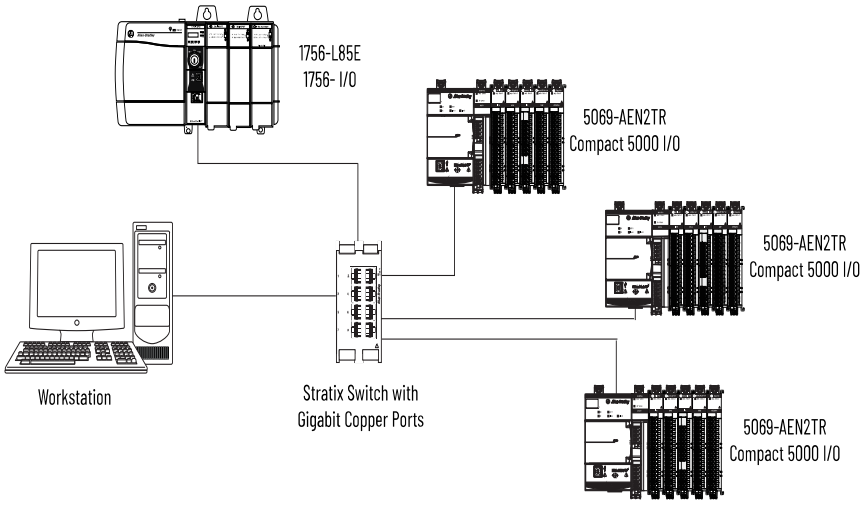
- I/O modules in a remote chassis via a network bridge module
- Distributed I/O families
- On-Machine™ I/O families

The ControlLogix® controller supports the use of remote I/O via these networks:

- EtherNet/IP™
- DeviceNet®
- Universal remote I/O

For more information about the network configurations that can be used to connect remote I/O, see Communication Networks on page 38.

Figure 25. ControlLogix 5580 Controller and Remote I/O on a 1 Gbps EtherNet/IP Network

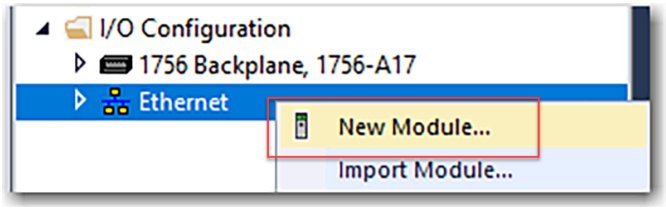


Add Remote I/O to the Ethernet Port on the Controller

If you are adding remote I/O modules, you can add the I/O modules to an Ethernet port of the controller. Typically, you must add a remote EtherNet/IP™communication module before you can add the remote I/O modules.
To add a remote EtherNet/IP™ communication module to your project, complete these steps.

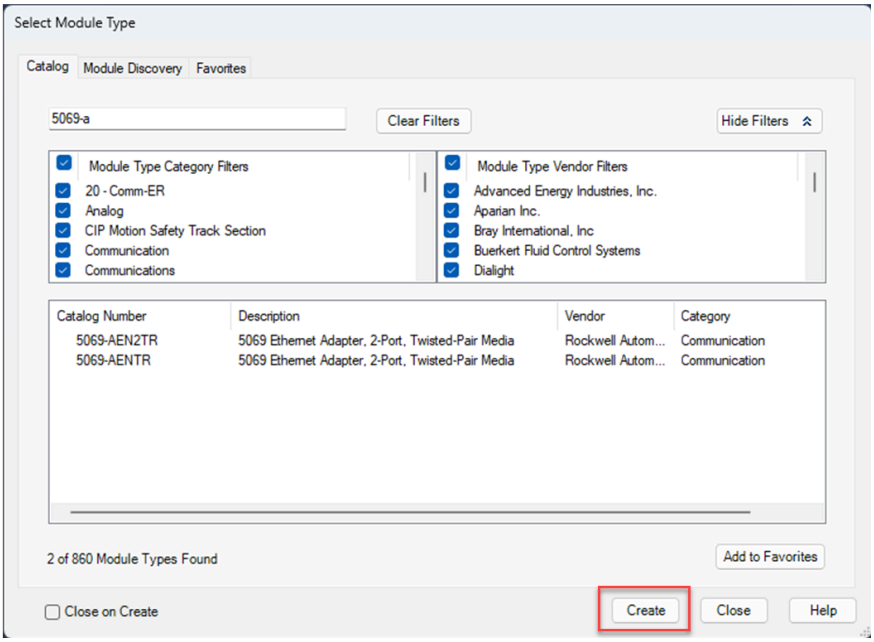
IMPORTANT: You cannot bridge through the front Ethernet port of another controller to add remote I/O.

1. In the I/O configuration, right-click Ethernet and select New Module.



2. On the Select Module Type dialog box, select the remote EtherNet/IP™ device and, click Create.

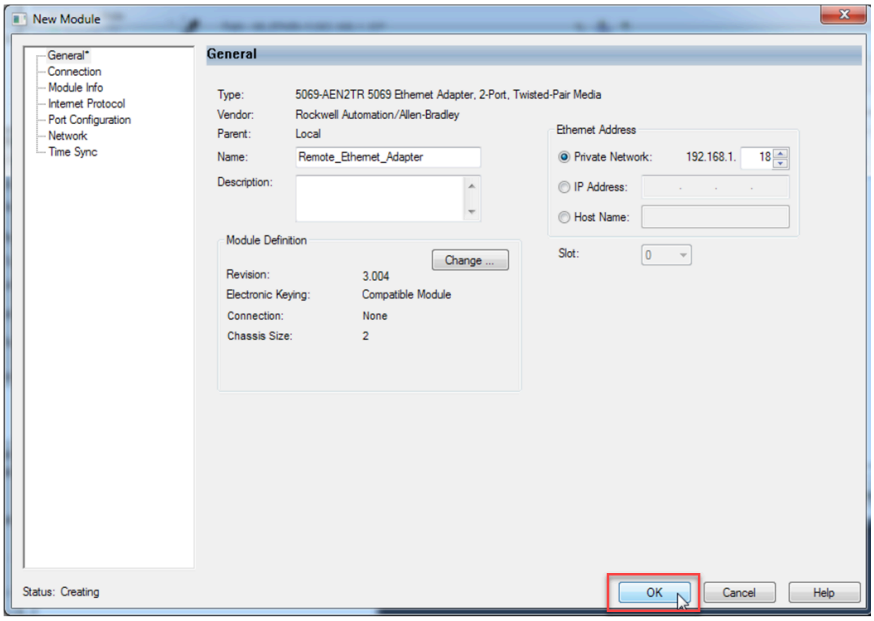
Use the filters to reduce the list of modules to choose from.



For some modules, the Select Major Revision dialog box can appear. If the dialog box appears, choose the major revision of the module and click OK.

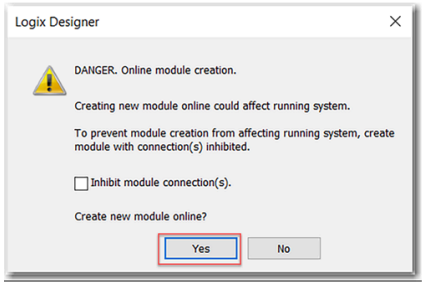
If the Series and Revision parameter values do not match those of the module for which this configuration is intended, your project can experience module faults.

3. Configure the remote EtherNet/IP™ communication module according to your network configuration, and click OK.

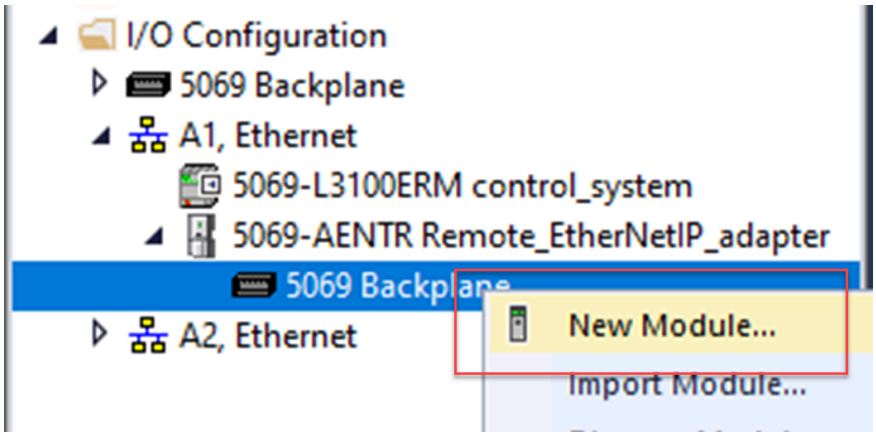


4. At the warning dialog box, click Yes and then close the Select Module Type dialog box.

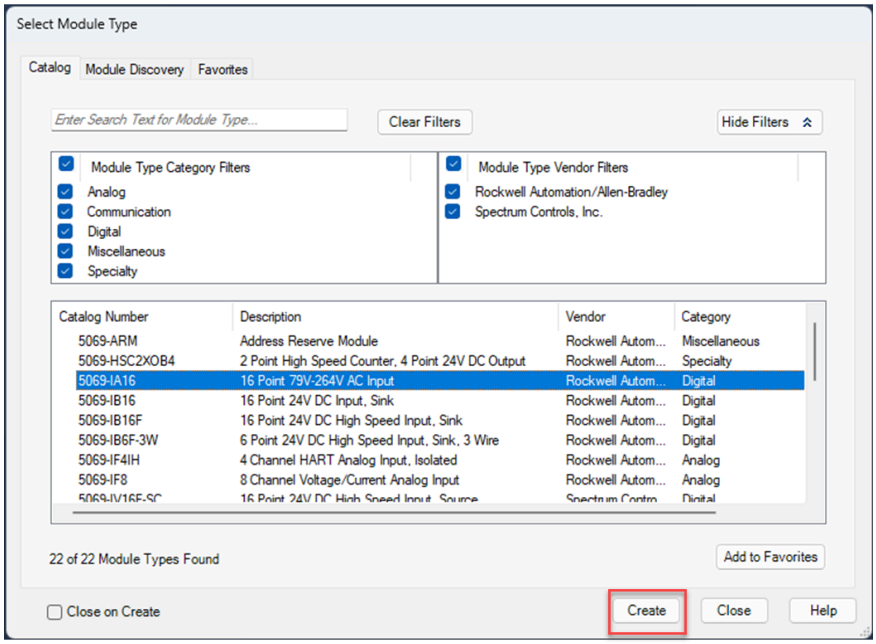
IMPORTANT: If you inhibit the module connection, you must remember to uninhibit the connection later.



5. Close the Select Module Type dialog box.
6. Right-click the backplane of the newly added EtherNet/IP™ communication module and select New Module.



7. On the Select Module Type dialog box, select the I/O module and click Create.

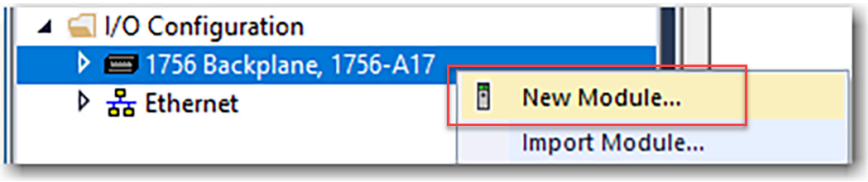


8. Configure the I/O module, and click OK.

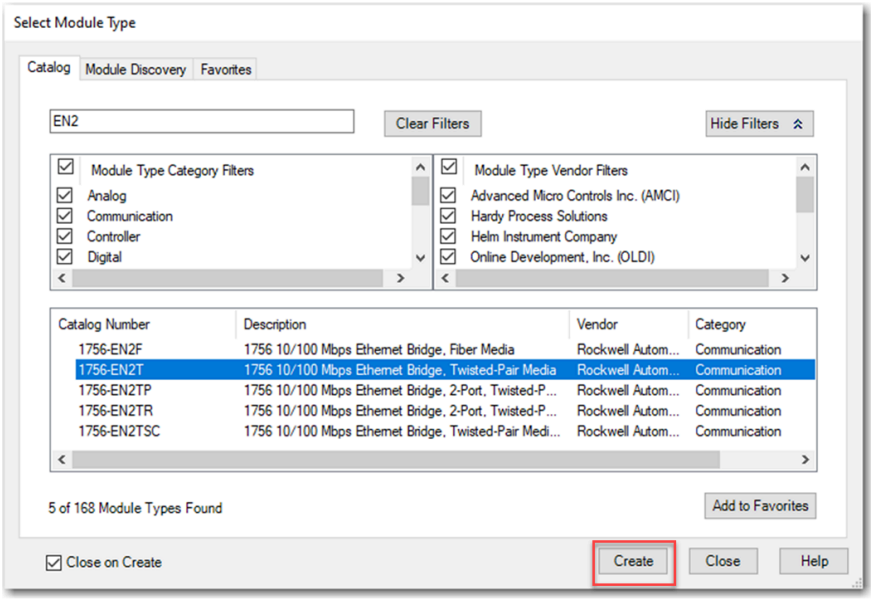
Add Remote I/O to a Local Communication Module

If you are using local communication modules that are connected to the controller, add the I/O modules to the backplane of the communication module.
To add remote I/O to the I/O Configuration in the Logix Designer application, complete these steps.

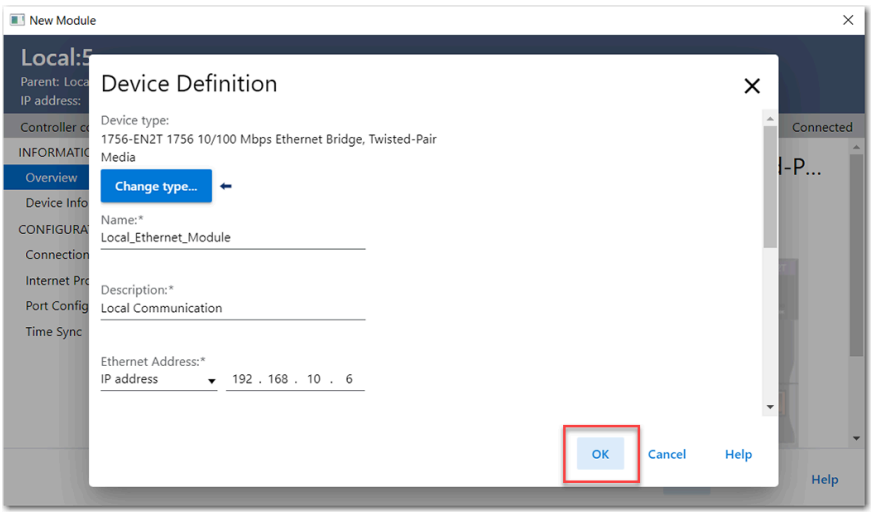
1. Right-click the backplane of the local chassis and select New Module.



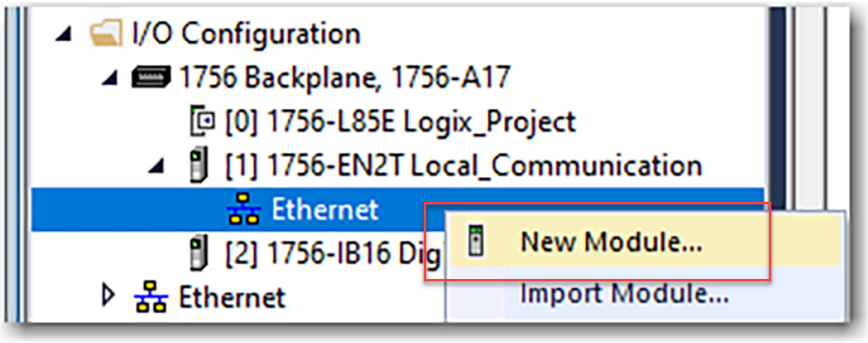
2. On the Select Module Type dialog box, select a communication module and click Create.



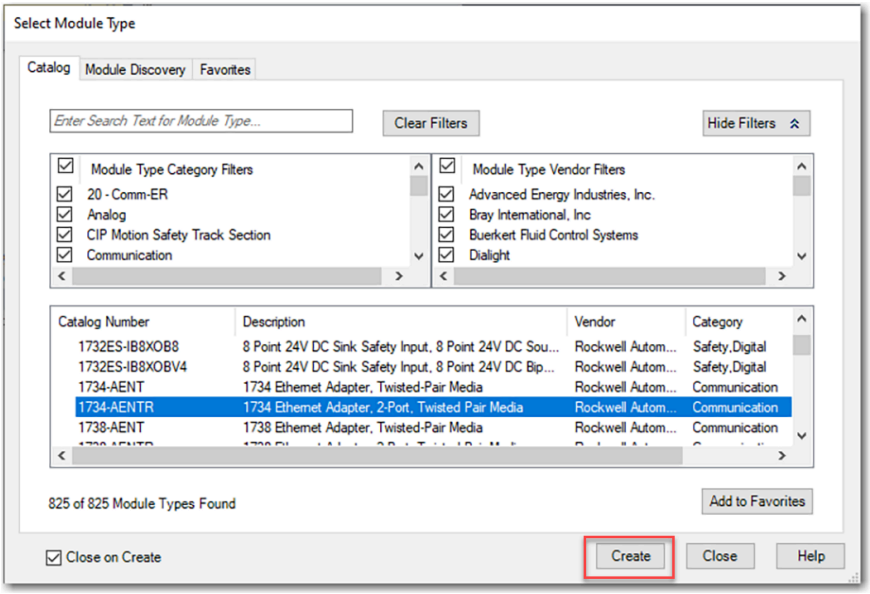
3. Specify the communication module properties according to your network configuration and click OK.



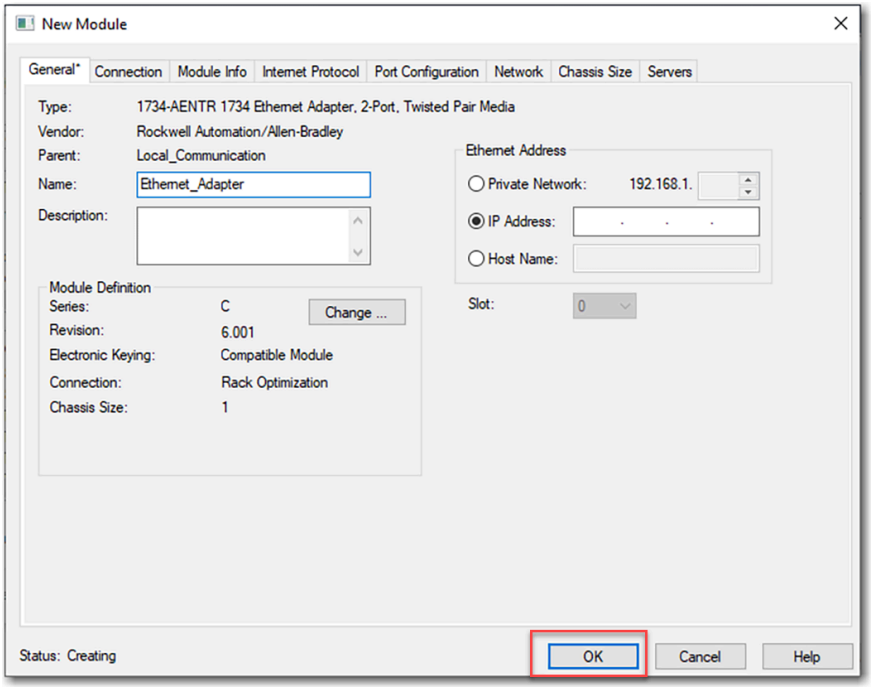
4. Right-click the communication network under the communication module and select New Module.



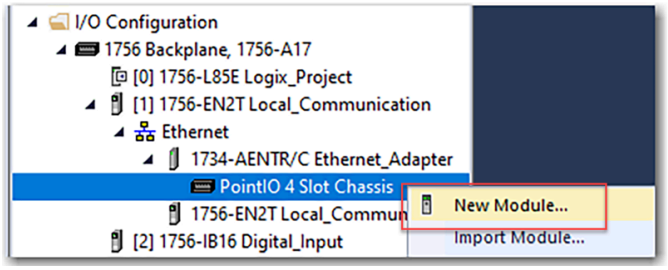
5. Select the communication adapter for the I/O platform that you are using and click Create.



6. Specify the module and connection properties according to your network configuration and click OK.

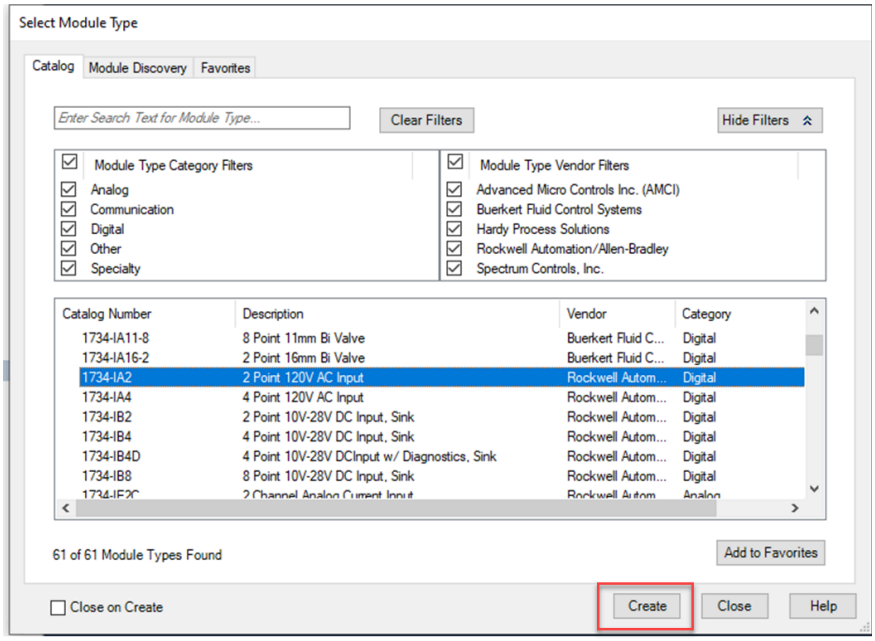


7. Right-click the backplane of the newly added communication adapter and select New Module.

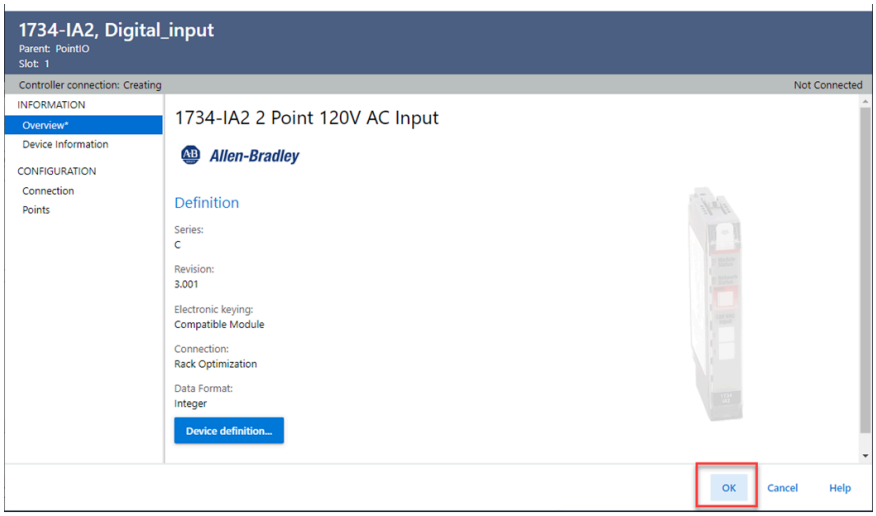


8. On the Select Module Type dialog box, select the I/O module to add and click Create.

Use the filters to reduce the list of modules to choose from.



9. Specify the module properties according to your module and application and click OK.



Add to the I/O Configuration While Online

You can add I/O and other devices to the controller configuration while you are online, and the keyswitch is in either the REM or PROG positions.

IMPORTANT: To add I/O modules when the controller is online, the controller keyswitch must be in the REM or PROG position. The I/O modules must already be installed in the system. You cannot install the I/O modules when the system is powered.

The modules and devices you can add while online depends on the version of the software you are using. Later versions have more modules and devices that can be added while online.

Add-on Profiles (AOP) for modules are made available between releases of different Logix Designer application versions. There are cases in which, after you download and install the AOP file for a module, you can add the module to a project while online.

To see a list of the available AOP files, go to: https://download.rockwellautomation.com/esd/download.aspx?downloadid=addonprofiles

You can add modules and devices to the local or remote chassis via an EtherNet/IP™ network, or via the unscheduled portion of a ControlNet® network.

For information on the number of nodes you can have for an EtherNet/IP™ network, see Manage Controller Communication on page .

For more information about adding to the I/O Configuration while online, see the Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094.

Modules that Can Be Added While Online

You can add these modules to the I/O configuration while online with Studio 5000 Logix Designer® application, version 28.00.00 or later.

- 1756 controllers
- 1756 ControlNet® modules
- 1756 DeviceNet® bridges
- 1756 EtherNet/IP™ modules
- Compact 5000® I/O EtherNet/IP™ adapters and I/O modules
- FLEX 5000® EtherNet/IP™ adapters and I/O modules
- 1756 I/O modules and specialty modules
- 1756-DHRIO
- 1756-DHRIOXT
- Compact 5000® I/O modules - As local or remote I/O modules
- Compact 5000® I/O EtherNet/IP™ adapters
- 1756 ControlLogix® EtherNet/IP™ modules
- 1756 ControlLogix® I/O modules

IMPORTANT: These ControlLogix® modules cannot be added while online:

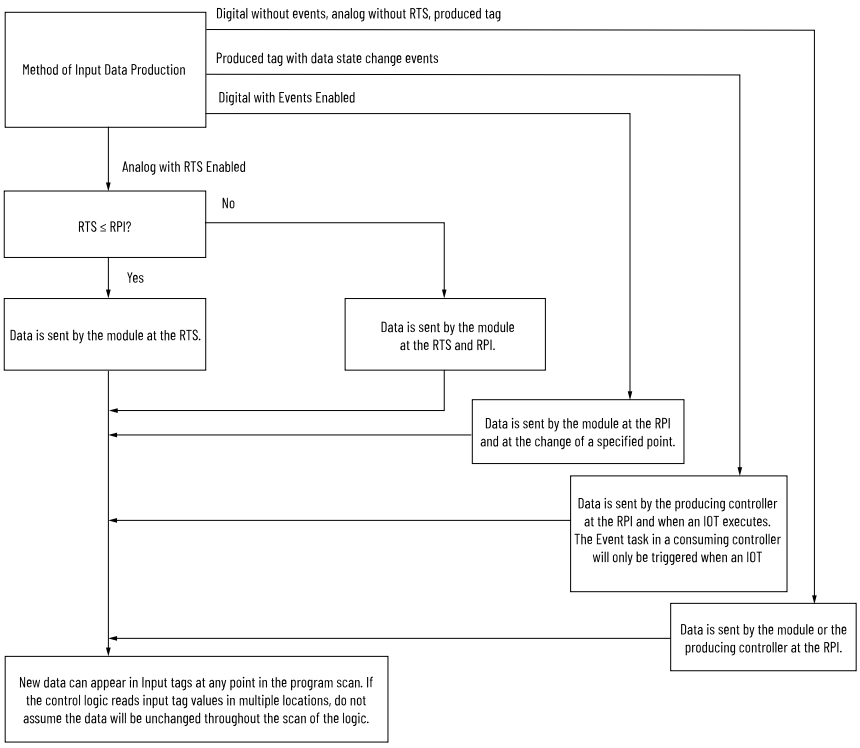
- Motion modules (1756-M02AE, 1756-HYD02, 1756-M02AS, 1756-M03SE, 1756-M08SE, 1756-M08SEG, 1756-M16SE)
- 1756-RIO
- 1756-SYNCH
- Safety I/O

Input Data Update Flowchart

ControlLogix® controllers update data asynchronously with the execution of logic.

IMPORTANT: GuardLogix® standard inputs are updated just like ControlLogix® standard inputs, but GuardLogix® safety input tags (inputs, consumed and mapped) are updated and frozen at the beginning of safety task execution.

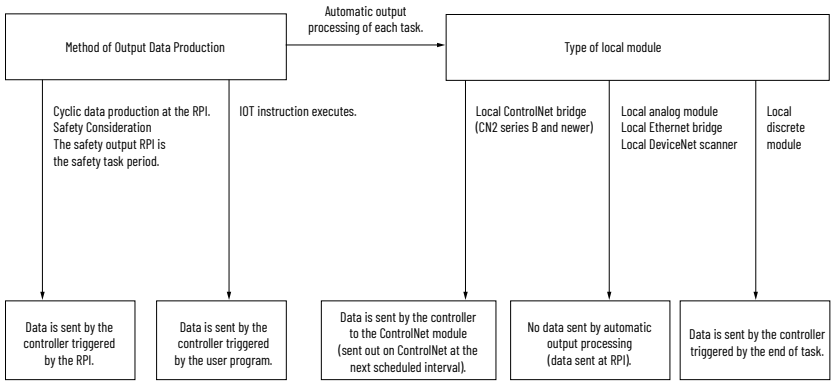
Figure 26. Input Data Update



Output Data Update Flowchart

ControlLogix® controllers update data asynchronously with the execution of logic.

Figure 27. Output Data Update



Safety I/O Devices

When you add a safety I/O device to the system, define a configuration for the device:

- Node address for DeviceNet® networks.

  NOTE: A Compact GuardLogix® 5380 controller can access devices on a DeviceNet® network only via a linking devices, for example, the 1788-EN2DN linking device. The controller can communicate with devices on the DeviceNet® network. However, typically Compact GuardLogix® 5380 controllers use EtherNet/IP™ networks to communicate with safety devices.

- IP address for EtherNet/IP™ networks.
- Safety network number (SNN). To set the SNN, see Change a Safety I/O Device SNN on page 118.
- Configuration signature. For information on when the configuration signature is set automatically and when you must set it, see Safety I/O Device Signature on page 121.
- Reaction time limit. For information on setting the reaction time limit, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012. Safety input, output, and test parameters complete the device configuration.

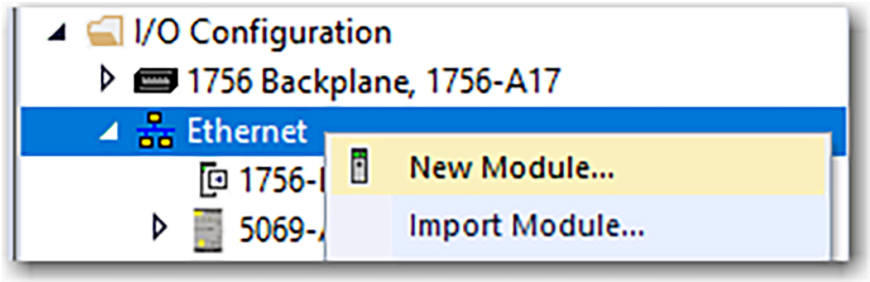
IMPORTANT: You cannot add safety I/O devices while online with the controller.

Configure Safety I/O Devices

Add the safety I/O device to the communication device in the I/O configuration of the controller project.

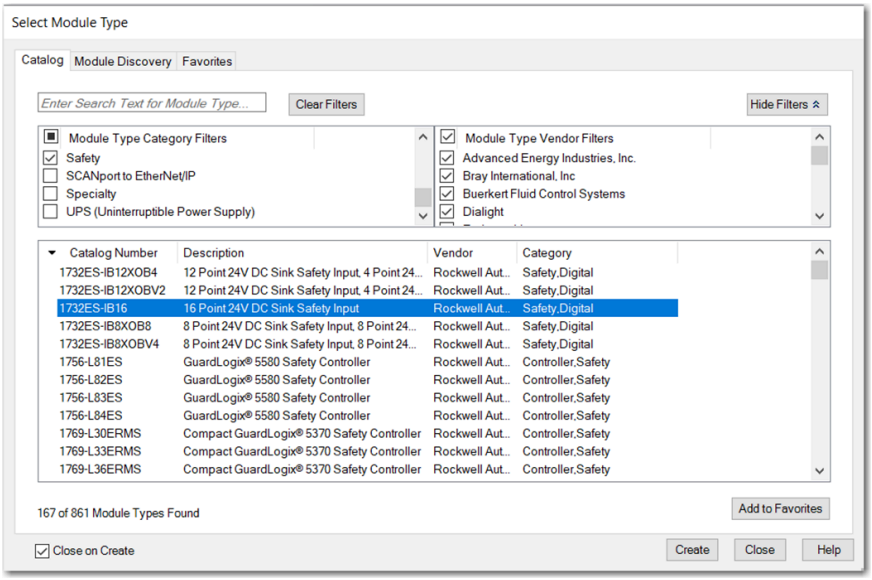
Some safety I/O devices support both standard and safety data. The device definition settings define what data is available.

1. Right-click the Ethernet network and select New Module.

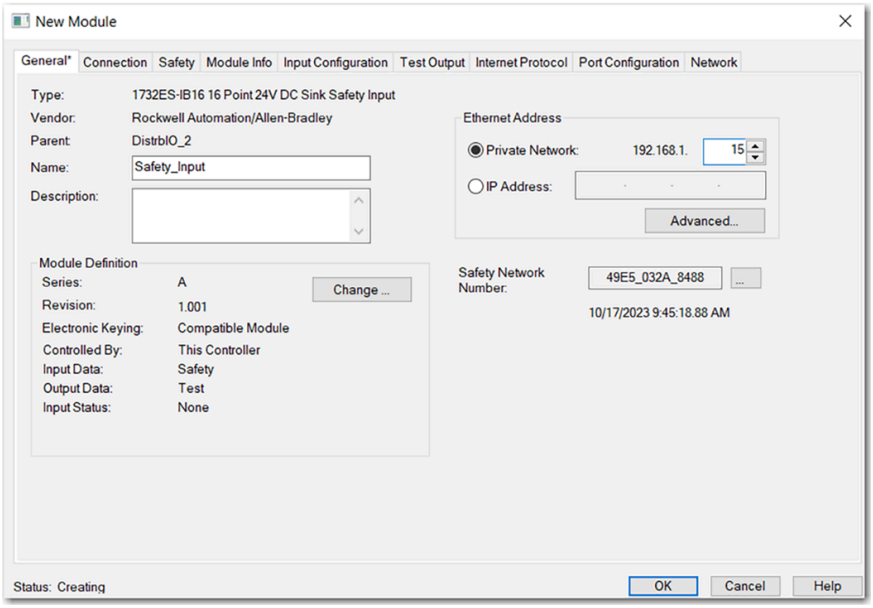


2. On the Select Module Type dialog box, select the safety I/O device and click Create.

   Use the filters to reduce the list of devices to choose from.



3. Enter a name and IP address for the new device. If your network uses Network Address Translation (NAT), see Use Network Address Translation (NAT) with CIP Safety Devices on page 117.



4. To modify the module definition settings, click Change.

IMPORTANT: For safety I/O devices, do not use Disable Keying. See Electronic Keying on page 100.

5. To modify the safety network number, click the ellipsis button.
   See Set the SNN of a Safety I/O Device on page 118.
6. Set the connection reaction time limit by using the Safety tab.
   For information about system reaction time, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012.
7. To complete configuration of the safety I/O device, refer to the user documentation and the Logix Designer online help.

Use Network Address Translation (NAT) with CIP Safety Devices

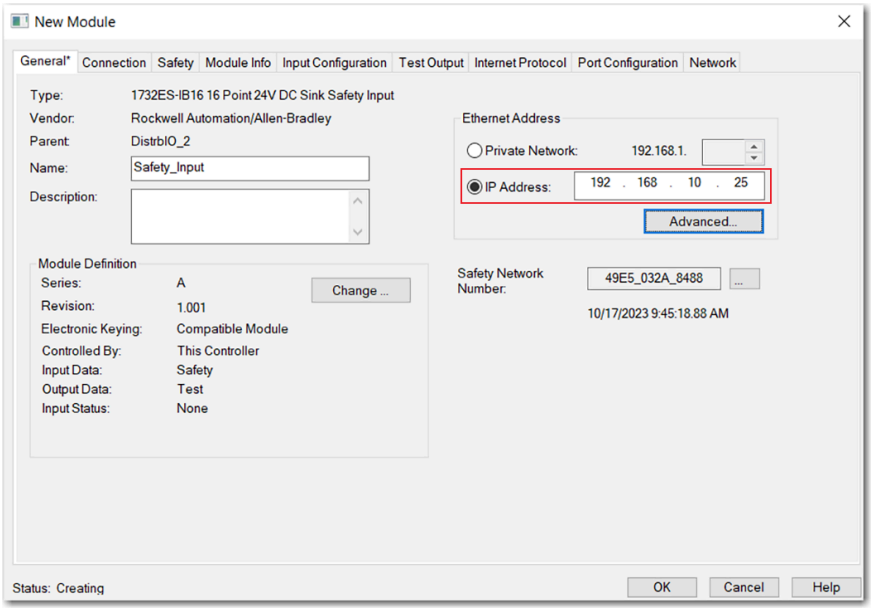
Network Address Translation (NAT) translates one IP address to another IP address via a NAT-configured router or switch. The router or switch translates the source and destination addresses within data packets as traffic passes between subnets.
This service is useful if you must reuse IP addresses throughout a network. For example, NAT makes it possible for devices to be segmented into multiple identical private subnets while maintaining unique identities on the public subnet, such as for multiple identical machines or lines.

This section only applies to safety users where the controller and the devices it talks to are on separate sides of the NAT-configured router or switch.

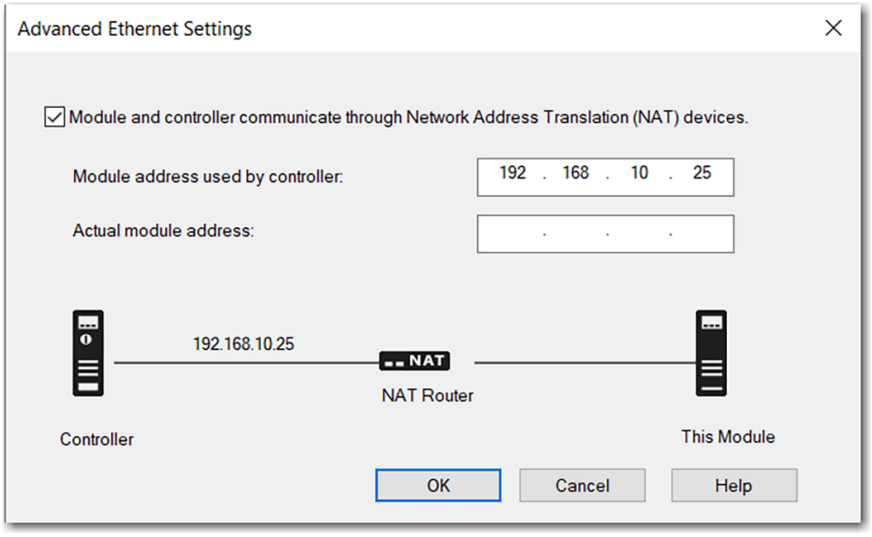
With CIP Safety™, the IP address of the device is part of the unique node reference that is part of the protocol. The device compares the IP address portion of the unique node reference in CIP Safety™ packets to its own IP address, and rejects any packets where they do not match. The IP address in the unique node reference must be the NAT'ed IP address. The controller uses the translated address, but the CIP Safety™ protocol requires the actual address of the device.

If you use NAT to communicate with a CIP Safety™ device, follow these steps to set the IP address.

1. In the IP Address field, enter the IP address for the controller. This is usually the IP address on the public network when using NAT.



2. Click Advanced to open the Advanced Ethernet Settings dialog box.



3. Select the checkbox to indicate that this device and the controller communicate through NAT devices.
4. Enter the actual device address.

If you configured the IP address using the rotary switches, this is the address, you set on the device. Alternately, the actual device address is the same address that is shown on the Internet Protocol tab.

5. Click OK.

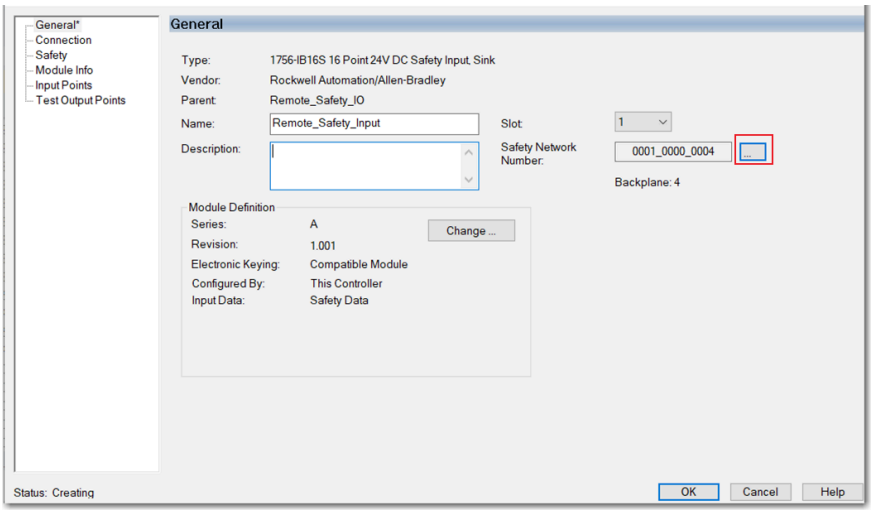
Set the SNN of a Safety I/O Device

A time-based SNN is automatically assigned when you add the first safety I/O device on the network. This does not apply to the controller backplane or Ethernet port since the controller counts as a device on the network.
When subsequent safety devices are added to the same network, they are assigned the same SNN as defined in the lowest address on that CIP Safety™ network or the controller itself if ports are attached to the controller. For most applications, the automatic, time-based SNN is sufficient.

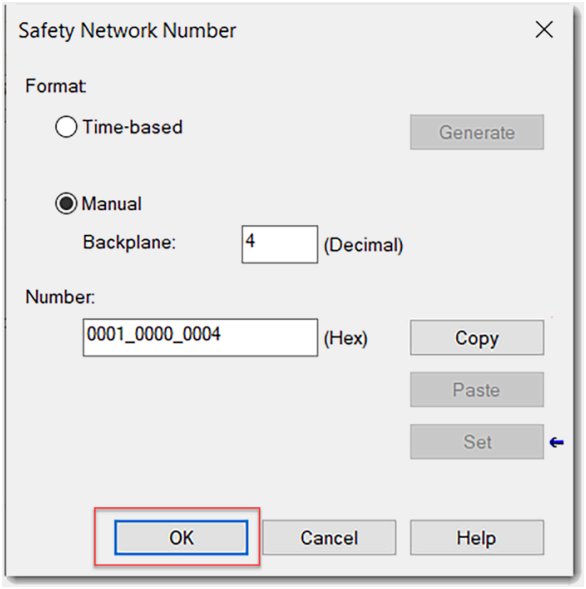
If your application requires you to assign the SNN of safety I/O devices manually, you only have to assign the SNN of the first safety I/O device you add in a remote network or backplane. The Logix Designer application then assigns the SNN of the first device to any additional devices that you add to that same remote network or backplane.

For an explanation on SNN, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012.

1. In the I/O configuration, right-click the remote EtherNet/IP™ communication device and select New Module.
2. Select the safety I/O device and select Create.
3. On the New Module dialog box, select the ellipse next to the safety network number.



4. On the Safety Network Number dialog box, select Manual.
5. Enter the SNN as a value from 1...9999 (decimal) and select OK.

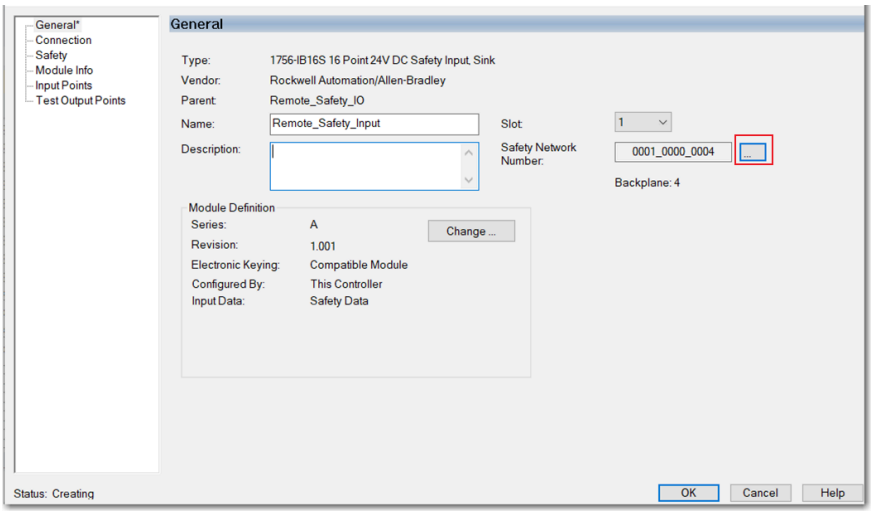


6. On the New Module dialog box, click OK.

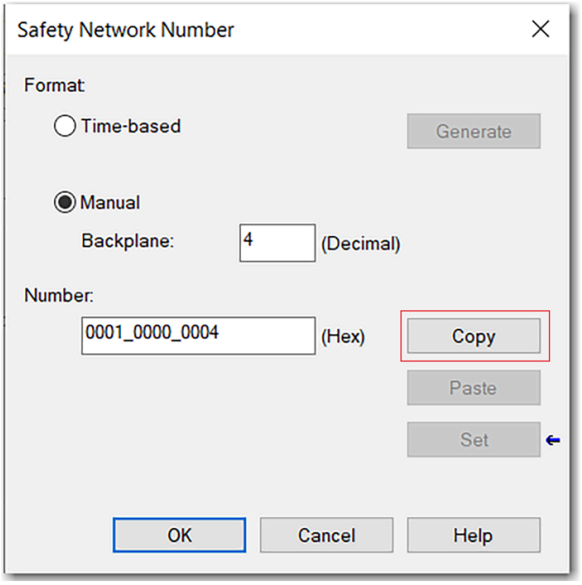
Copy and Paste a Safety I/O Device SNN

If you must apply an SNN to other safety I/O devices, you can copy and paste the SNN.

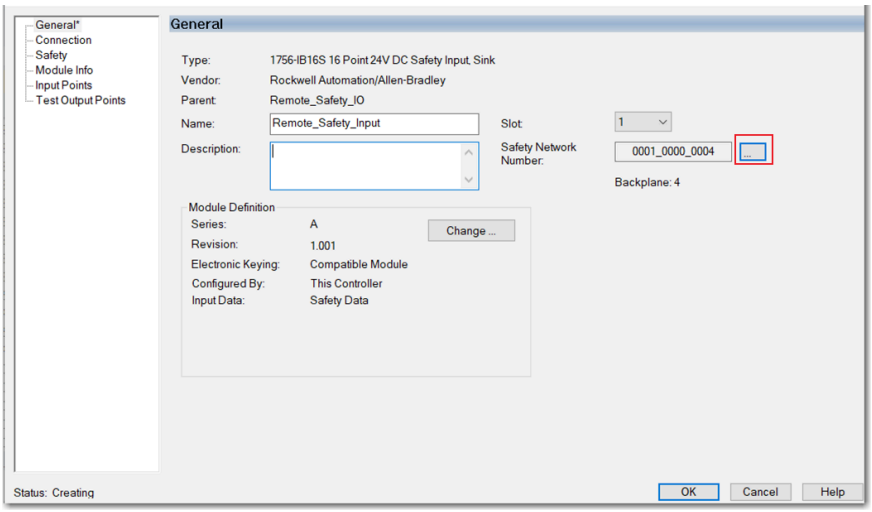
1. On the General view of the Module Properties dialog box, click the ellipse next to the safety network number.



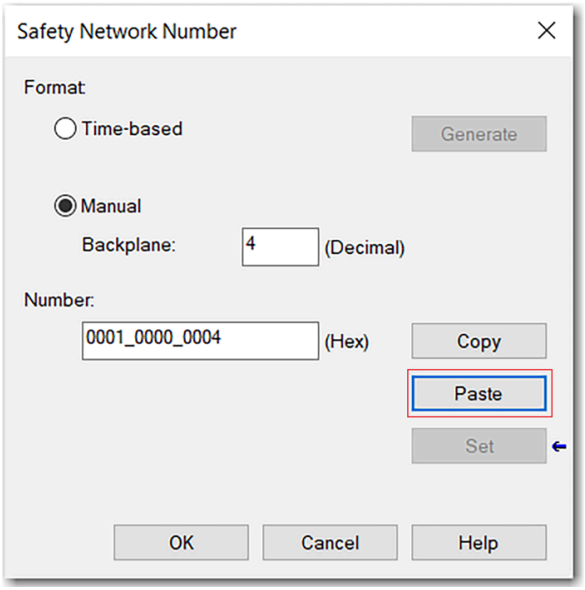
2. On the Safety Network Number dialog box, select Copy.



3. On the General view of the Module Properties dialog box, click the ellipse next to the safety network number.



4. On the Safety Network Number dialog box, click Paste.

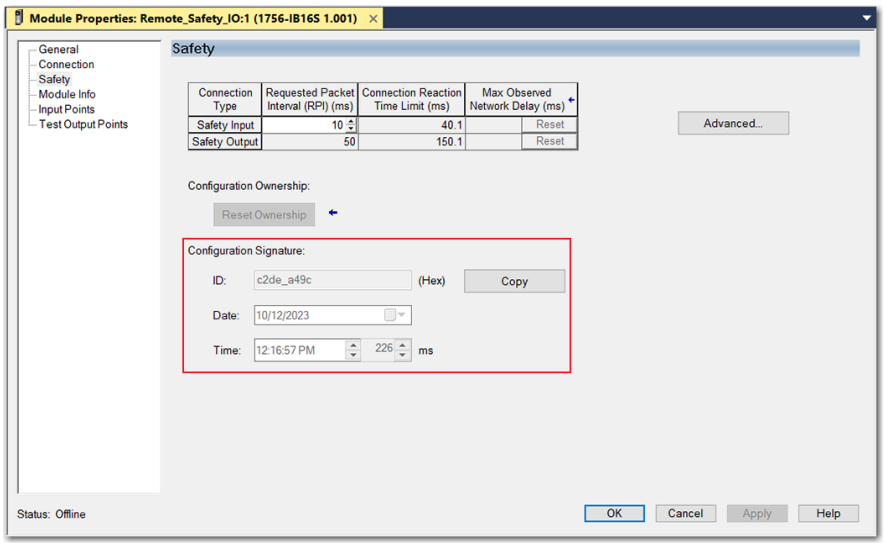


Safety I/O Device Signature

Each safety device has a configuration signature that uniquely identifies the device configuration. The configuration signature is composed of an ID number, date, and time, and is used to verify a device's configuration.

When the I/O device is configured via the Logix Designer application, the configuration signature is generated automatically. You can view and copy the configuration signature on the Safety view of the Module Properties dialog box.

Figure 28. View and Copy the Configuration Signature

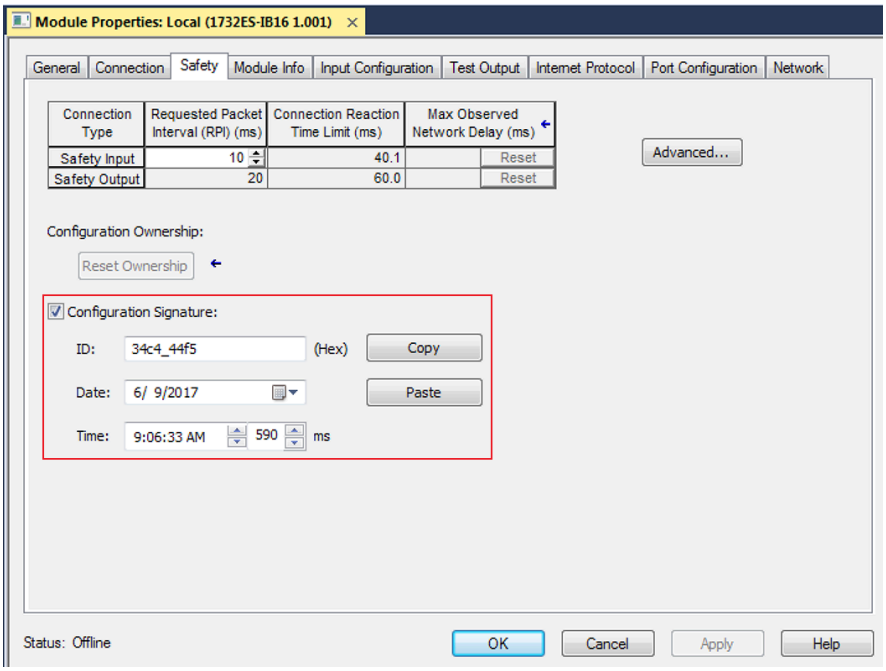


Different Configuration Owner (Data-only Connection)

When the I/O device configuration is owned by another controller, you must copy the device configuration signature from its owner's project and paste it into the Safety view of the device properties.

If the device is only configured for inputs, you can copy and paste the configuration signature. If the device has safety outputs, they are owned by the controller that owns the configuration, and the configuration signature ID text box is unavailable.

Figure 29. View and Copy the Configuration Signature From a Different Device



Reset Safety I/O Devices to the Out-of-box Condition

If a Guard I/O™ device was used previously, clear the existing configuration before installing it on a safety network by resetting the device to its out-of-box condition.

When the controller project is online, the Safety tab of the device properties displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the SNN and node address or slot number of the configuration owner. A communication error appears if the device read fails.

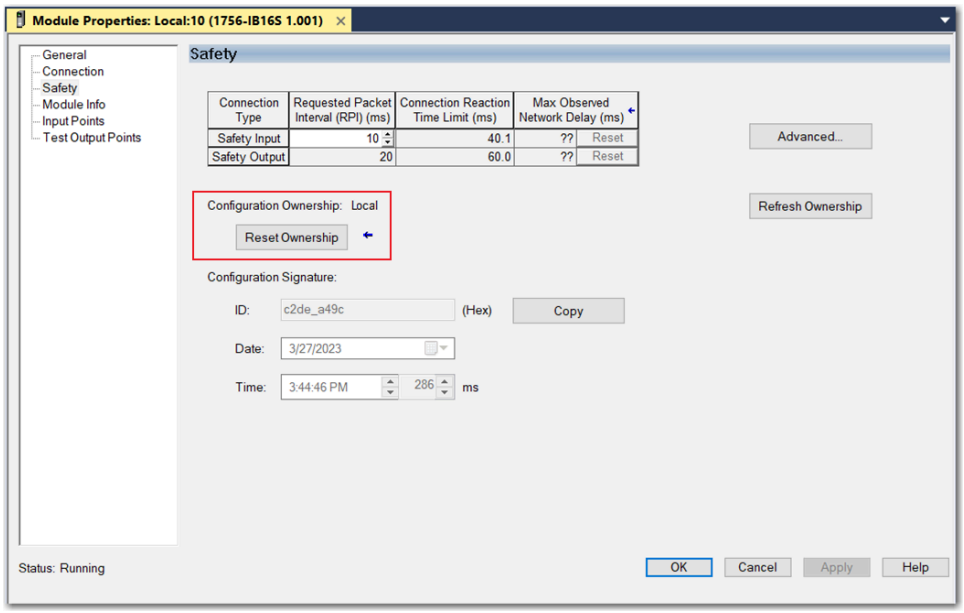
If the connection is local, you must inhibit the device connection before resetting ownership.

Follow these steps to inhibit the device.

1. Right-click the device and choose Properties.
2. Click the Connection tab.
3. Check Inhibit Connection.
4. Click Apply and then OK.

Follow these steps to reset the device to its out-of-box configuration when online.

1. Right-click the device and choose Properties.
2. Click the Safety tab.
3. Click Reset Ownership.



You cannot reset ownership when there are pending edits to the device properties, when a safety signature exists, or when safety-locked.

I/O Device Address Format

When you add a device to the I/O configuration, the Studio 5000 Logix Designer® application creates controller-scoped tags for the device.

I/O information is presented as a set of tags. Each tag uses a structure of data, depending on the type and features of the I/O device. The name of a tag is based on the name of the device.

A safety I/O device address follows this example: *devicename:Type.Member*

Table 25. Safety I/O Device Address Format

Where	Is	
device name	The name of the safety I/O device.	
Type	Type of data	Input: I Output: O
Membership	Specific data from the I/O device	
	Input-only device	devicename:I.RunMode (required) devicename:I.ConnectionFaulted (required) devicename:I.Input Members
	Output-only device	devicename:I.RunMode (required) devicename:I.ConnectionFaulted (required) devicename:O.Output Members
	Combination I/O	devicename:I.RunMode (required) devicename:I.ConnectionFaulted (required) devicename:I.Input Members devicename:O.Output Members

For more information on addressing standard I/O devices, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

Change Configuration Ownership

When the controller project is online, the Safety tab of the device Properties dialog box displays the current configuration ownership: .

- When the opened project owns the configuration, Local is displayed.
- When a second device owns the configuration, Remote is displayed, along with the SNN and the node address or slot number of the configuration owner.
- If the device read fails, a communication error appears

If the connection is Local, you must inhibit the device connection before resetting ownership. Follow these steps to inhibit the device.

1. Right-click the device and choose Properties.
2. Click the Connection tab.
3. Check Inhibit Connection.
4. Click Apply and then OK.

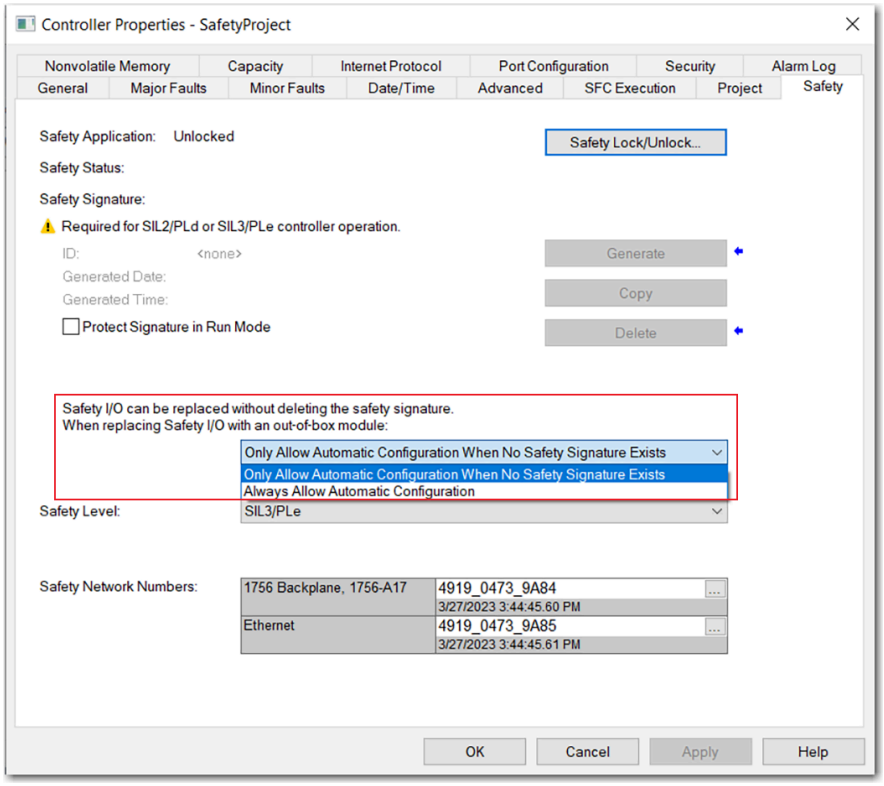
Safety I/O Replacement Options

Two options for safety I/O device replacement are available on the Safety tab of the Controller Properties dialog box in the Logix Designer application:

- Only Allow Automatic Configuration When No Safety Signature Exists
  Select this option if you rely on a portion of the CIP Safety system to maintain SIL 2 or SIL 3 behavior during device replacement and functional testing.
- Always Allow Automatic Configuration
  Select this option if you do not rely on the entire routable CIP Safety system to maintain SIL 2 or SIL 3 behavior during device replacement and functional testing.

For more considerations about choosing an automatic configuration setting, including example use cases, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication 1756-RM012.

Figure 30. Safety I/O Replacement Options



Only Allow Automatic Configuration When No Safety Signature Exists

When a safety I/O device is replaced, the configuration is downloaded from the safety controller if the DeviceID of the new device matches the original. The DeviceID is a combination of the node/IP address and the Safety Network Number (SNN) and is updated whenever the SNN is set.

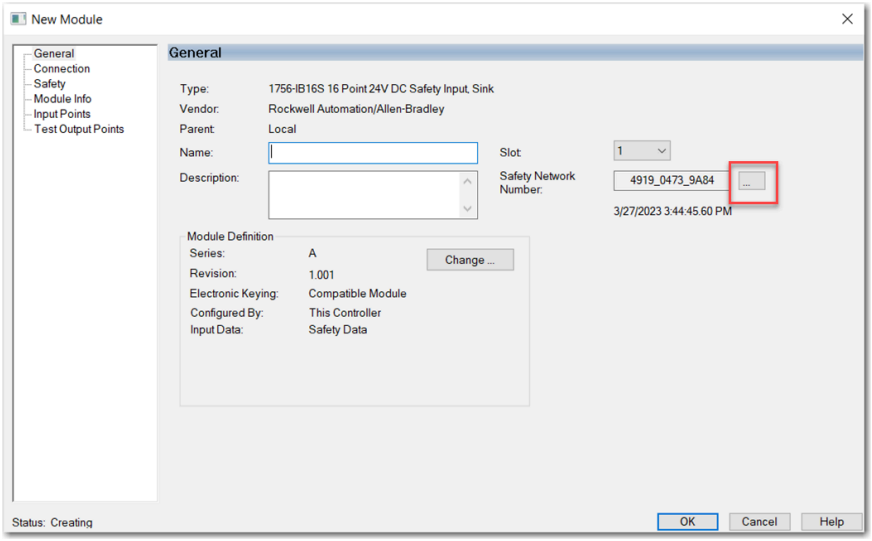
If you select the Only Allow Automatic Configuration When No Safety Signature Exists option, follow the guidance in the following table to replace a safety I/O device based on your scenario. After you complete the steps, the DeviceID matches the original and enables the safety controller to download the proper device configuration and re-establish the safety connection.

Table 26. Replace a Device

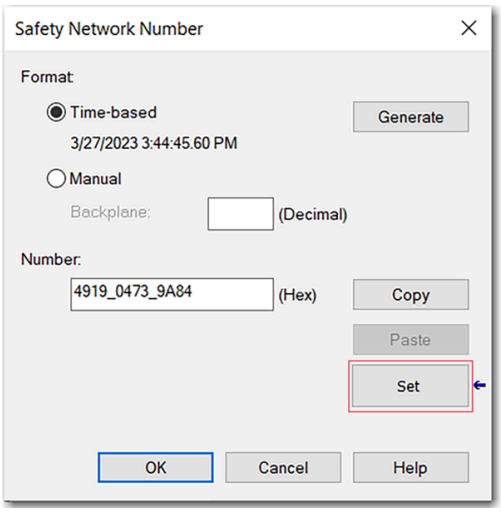
Safety Signature Exists	Replacement Device Condition	Action Required
No	No SNN (out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (out-of-box)	See Replacement Device is Out-of-box and Safety Signature Exists on page 126
Yes	Different SNN from original safety task configuration	See Replacement Device SNN is Different from Original and Safety Signature Exists on page 127
No		See Replacement Device SNN is Different from Original and No Safety Signature Exists on page 128

Scenario 1 - Replacement Device is Out-of-box and Safety Signature Exists

1. Remove the old I/O device and install the new device.
2. Right-click the replacement safety I/O device and choose Properties.
3. Click the ellipse to the right of the safety network number to open the Safety Network Number dialog box.



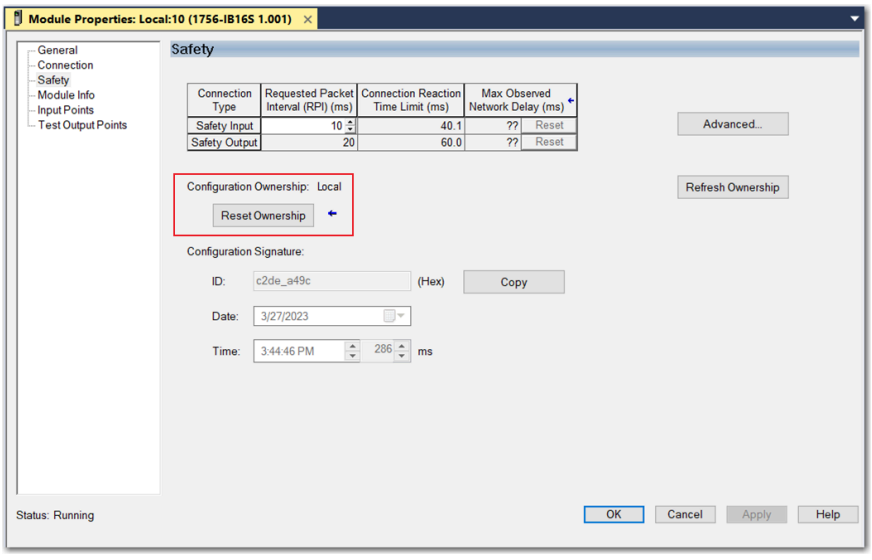
4. Click Set.



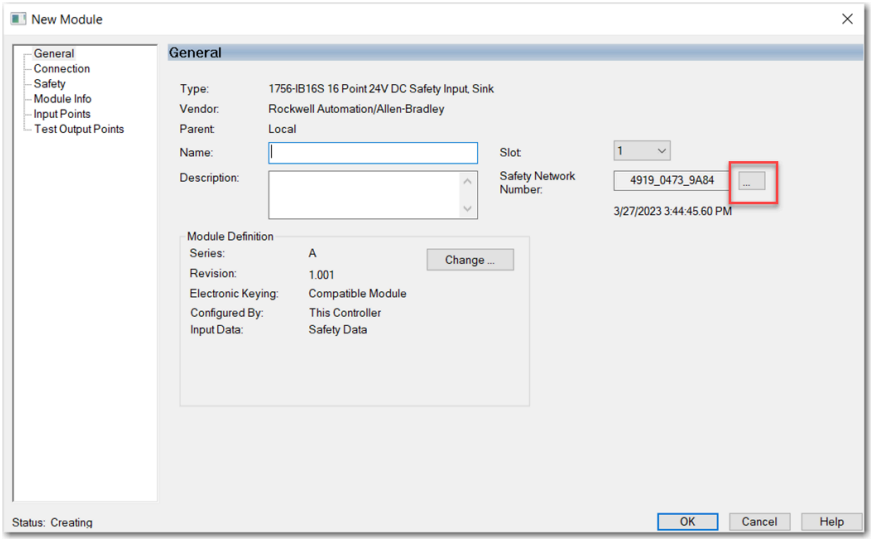
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists

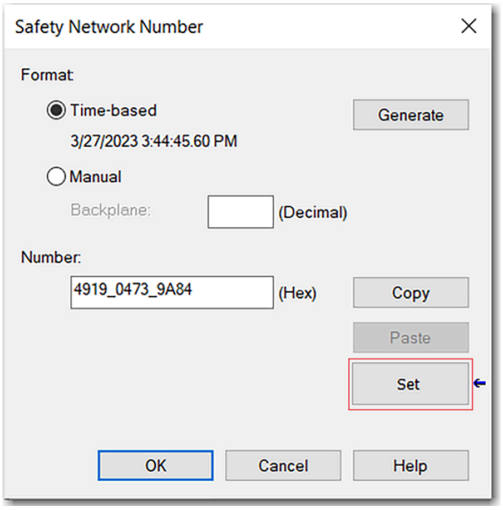
1. Remove the old I/O device and install the new device.
2. Right-click your safety I/O device and select Properties.
3. In the navigation pane, click Safety.
4. Click Reset Ownership.



5. Click OK.
6. Right-click the device and select Properties.
7. Click the ellipse to the right of the safety network number to open the Safety Network Number dialog box.



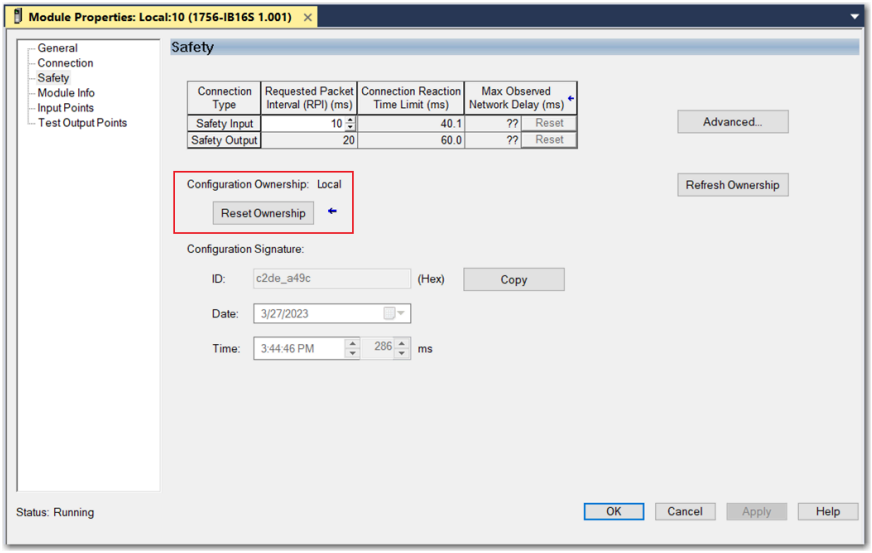
8. Click Set.



9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.
10. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

Scenario 3 - Replacement Device SNN is Different from Original and No Safety Signature Exists

1. Remove the old I/O device and install the new device.
2. Right-click your safety I/O device and select Properties.
3. In the navigation pane, click Safety.
4. Click Reset Ownership.



5. Click OK.
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

Always Allow Automatic Configuration

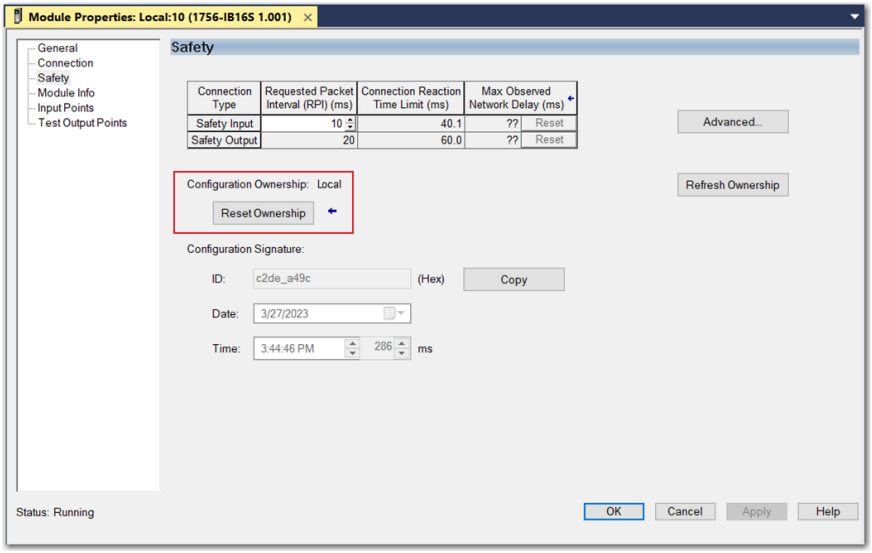
ATTENTION: Select the Always Allow Automatic Configuration option only if the entire CIP Safety Control System is not being relied on to maintain SIL 2 or SIL 3 behavior during the replacement and functional testing of a device. Do not place devices that are in the out-of-box condition on a CIP Safety network when the Always Allow Automatic Configuration option is selected, except while following this replacement procedure.

When the Always Allow Automatic Configuration option is selected in the controller project, the controller automatically checks for and connects to a replacement device that meets all the following requirements:

- The controller has configuration data for a compatible device at that network address.
- The device is in out-of-box condition or has an SNN that matches the configuration.

If the Always Allow Automatic Configuration option is selected, follow these steps to replace a safety I/O device.

1. Remove the old I/O device and install the new device.
   a. If the device is in out-of-box condition, go to the last step in this procedure. No action is needed for the GuardLogix® controller to take ownership of the device.
   b. If an SNN mismatch error occurs, go to the next step to reset the device to an out-of-box condition.
2. Right-click the safety I/O device and select Properties.
3. In the navigation pane, select Safety.
4. Click Reset Ownership and click OK.



5. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

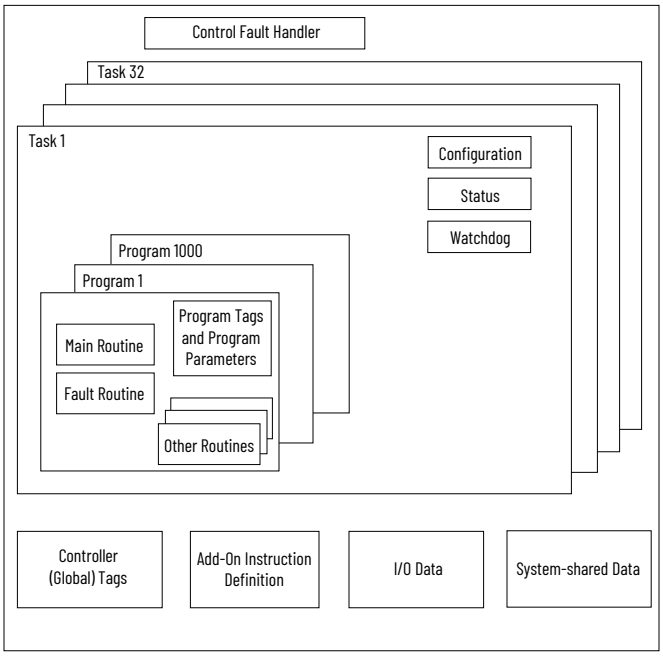
Develop Standard Applications

A control application consists of several elements that require planning for efficient application execution.

Application elements include the following:

- Tasks
- Programs
- Routines
- Parameters and Local Tags
- Add-On Instructions

Figure 31. Elements of a Control Application



Tasks

The controller lets you use multiple tasks to schedule and prioritize the execution of your programs based on criteria. This multitasking allocates the processing time of the controller among the operations in your application:

- The controller executes only one task at a time.
- One task can interrupt the execution of another and take control based on its priority.
- In any given task, multiple programs can be used. However, only one program executes at a time.
- You can display tasks in the Controller or Logical Organizer views, as necessary.

Figure 32. Task Within a Control Application

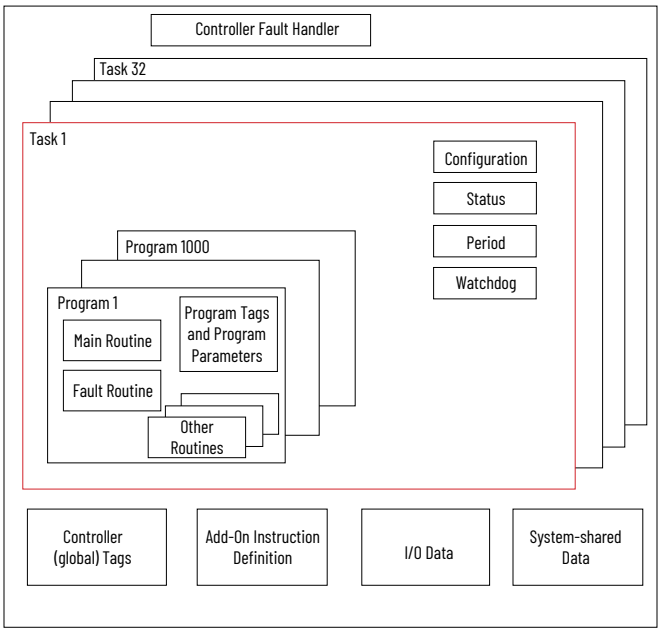
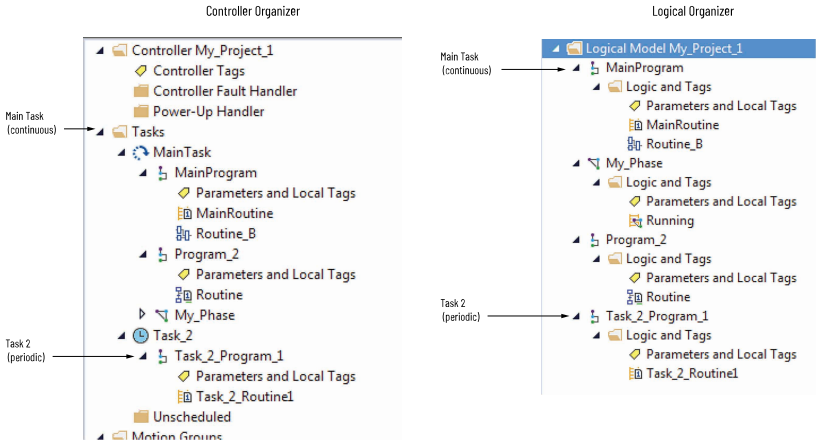
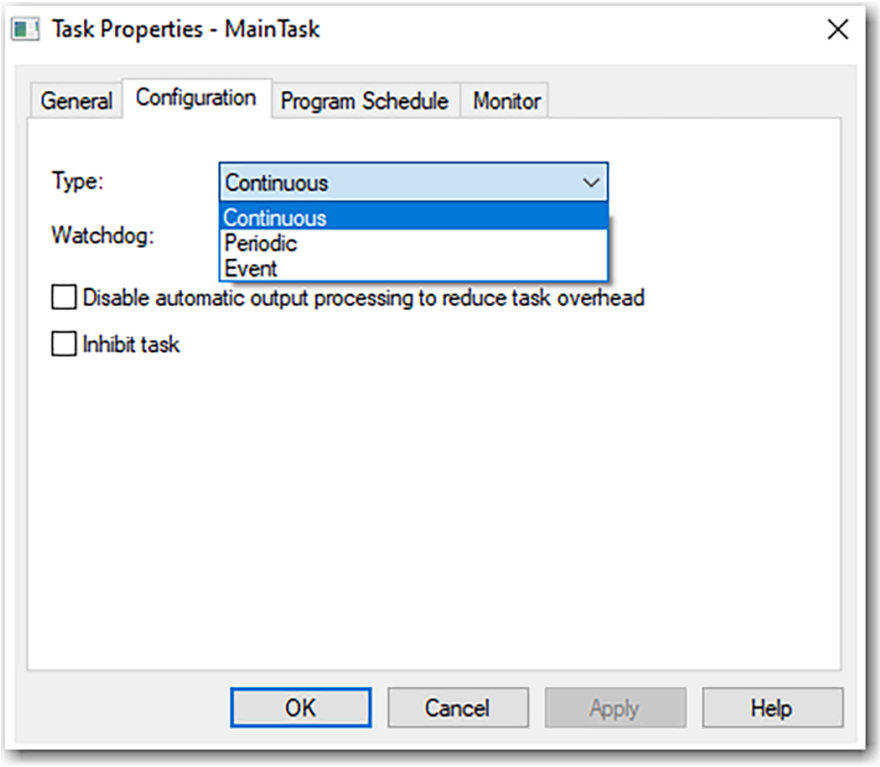


Figure 33. Tasks in the Controller Organizer and Logical Organizer



A task provides scheduling and priority information for a set of one or more programs. Configure tasks as continuous, periodic, or event by using the Task Properties dialog box.

Figure 34. Configure the Task Type



This table explains the types of tasks that you can configure.

Table 27. Task Types and Execution Frequency

Task Type	Task Execution	Description
Continuous	Constant	The continuous task runs in the background. Any CPU time that is not allocated to other operations (such as motion and other tasks) is used to execute the programs in the continuous task. • The continuous task runs constantly. When the continuous task completes a full scan, it restarts immediately. • A project does not require a continuous task. If used, there can be only one continuous task.
Periodic	At a set interval, such as each 100 ms	A periodic task performs a function at an interval. • Whenever the time for the periodic task expires, the task interrupts any lower priority tasks, executes once, and returns control to where the previous task left off. • You can configure the time period from 0.1...2,000,000.00 ms. The default is 10 ms. It is also controller and configuration dependent.
Event	Immediately when an event occurs	An event task performs a function when an event (trigger) occurs. The trigger for the event task can be the following: • Module input data change of state • A consumed tag trigger • An EVENT instruction

Table 27. Task Types and Execution Frequency (continued)

Task Type	Task Execution	Description
		• An axis trigger • A motion event trigger You can configure an optional timeout interval for missed event triggers, which causes the event tasks to execute even in the absence of the trigger. Set the Check the Executed Task If No Event Occurs Within <timeout period> checkbox for task.

The controllers support up to 32 tasks. Only one of the tasks can be continuous.

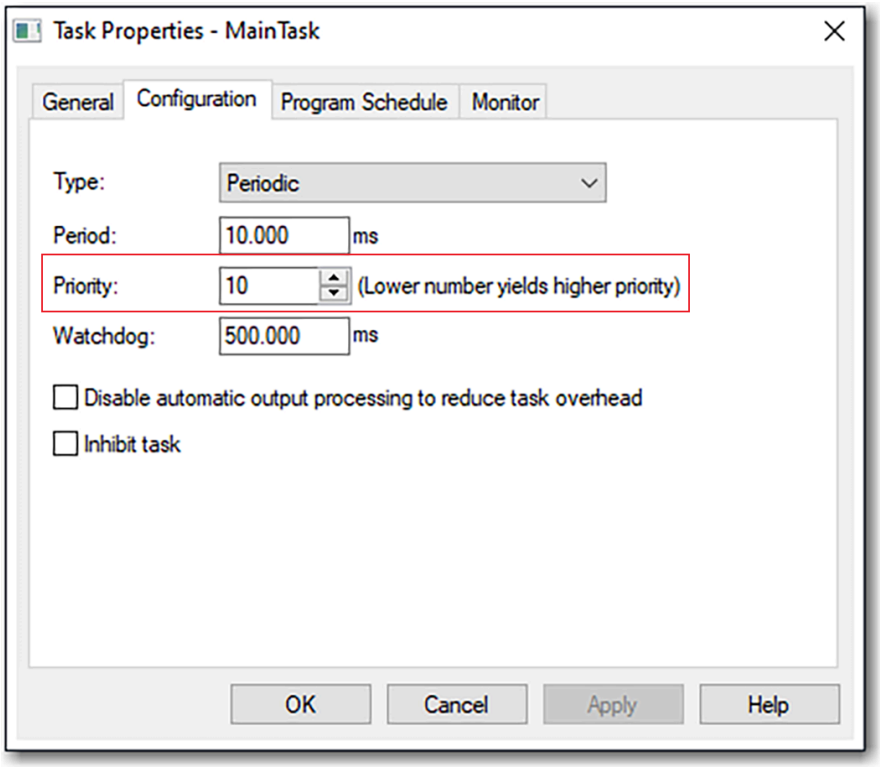
A task can have up to 1000 programs, each with its own executable routines and program-scoped tags. Once a task is triggered (activated), the programs that are assigned to the task execute in the order in which they are grouped. Programs can appear only once in the Controller Organizer and multiple tasks cannot share them.

Task Priority

Each task in the controller has a priority level. The operating system uses the priority level to determine which task to execute when multiple tasks are triggered. A higher priority task interrupts any lower priority task. The continuous task has the lowest priority, and a periodic or event task interrupts it.

You can configure periodic and event tasks to execute from the lowest priority of 15 up to the highest priority of 1. Configure the task priority by using the Task Properties dialog box.

Figure 35. Configure the Task Priority



Programs

The controller operating system is a preemptive multitasking system that is in compliance with IEC 61131-3. This system provides the following:

- Programs to group data and logic
- Routines to encapsulate executable code that is written in one programming language

Each program contains the following:

- Local Tags
- Parameters
- A main executable routine
- Other routines
- An optional fault routine

Figure 36. Program Within a Control Application

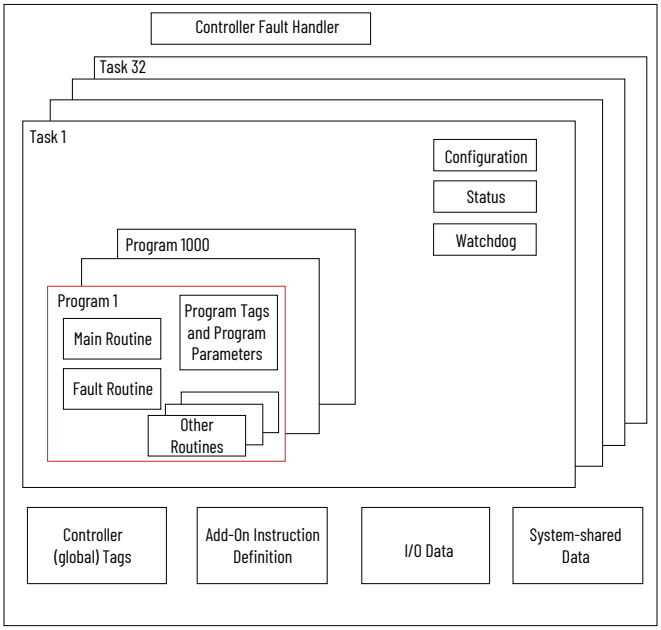
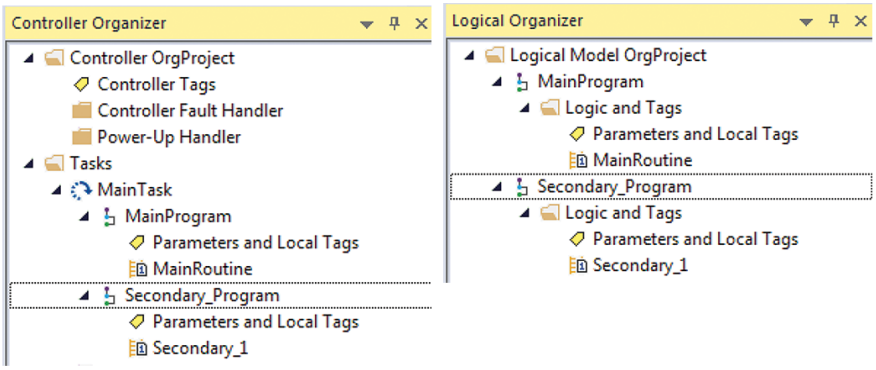


Figure 37. Programs the Controller Organizer and Logical Organizer



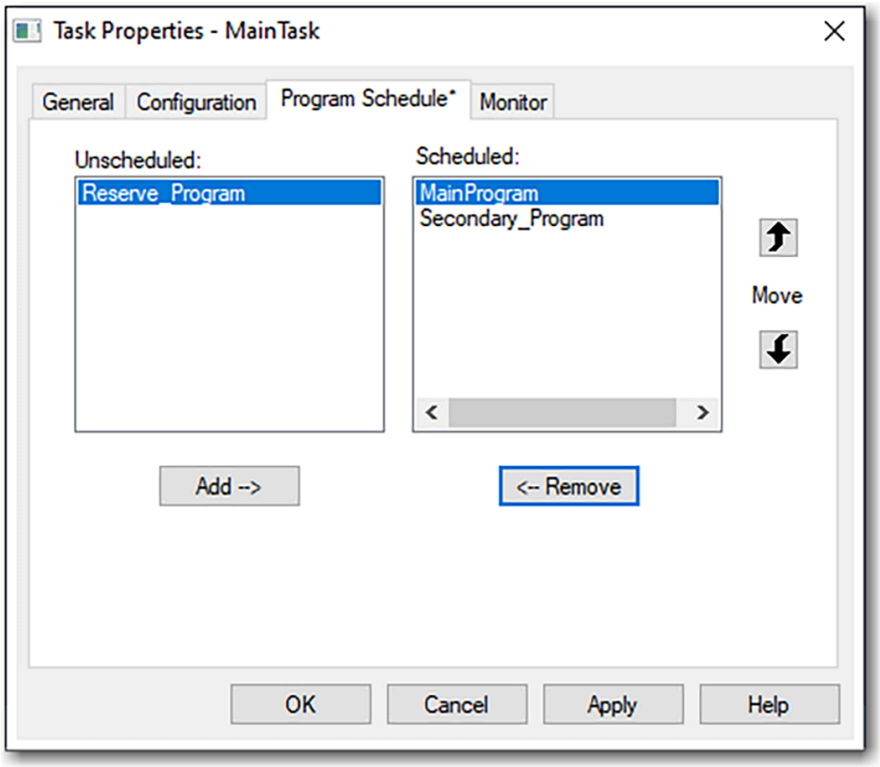
Scheduled and Unscheduled Programs

The scheduled programs within a task execute to completion from first to last. Programs that are not attached to any task show up as unscheduled programs.

Unscheduled programs within a task are downloaded to the controller with the entire project. The controller verifies unscheduled programs but does not execute them.

You must schedule a program within a task before the controller can scan the program. To schedule an unscheduled program, use the Program/Phase Schedule tab of the Task Properties dialog box.

Figure 38. Schedule an Unscheduled Program



Routines

A routine is a set of logic instructions in one programming language, such as Ladder Diagram (ladder logic). Routines provide the executable code for the project in a controller.

Each program has a main routine. The main is the first routine to execute when the controller triggers the associated task and calls the associated program. Use logic, such as the Jump to Subroutine (JSR) instruction, to call other routines.

You can also specify an optional program fault routine. The controller executes this routine if it encounters an instruction-execution fault within any of the routines in the associated program.

Figure 39. Routines in a Control Application

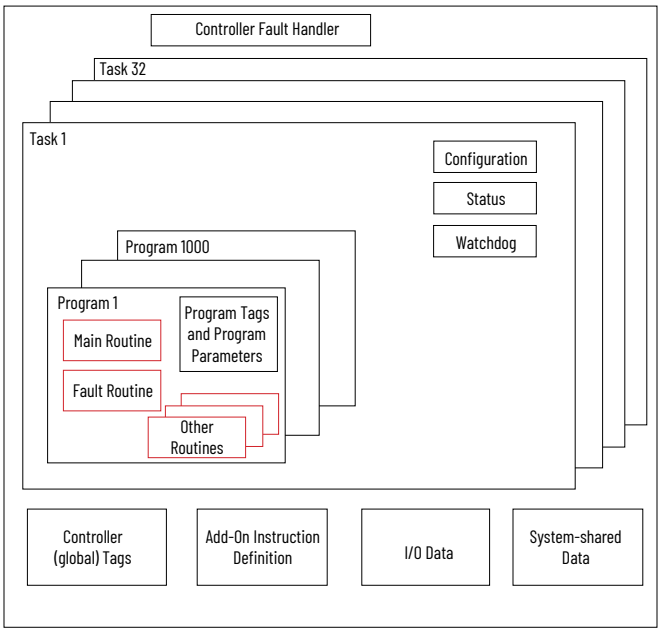
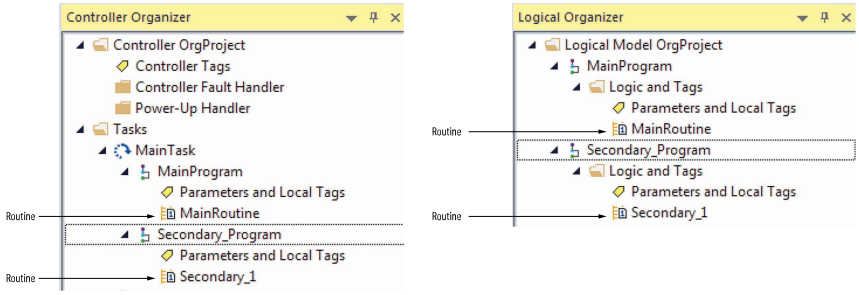


Figure 40. Routines in the Controller Organizer and Logical Organizer



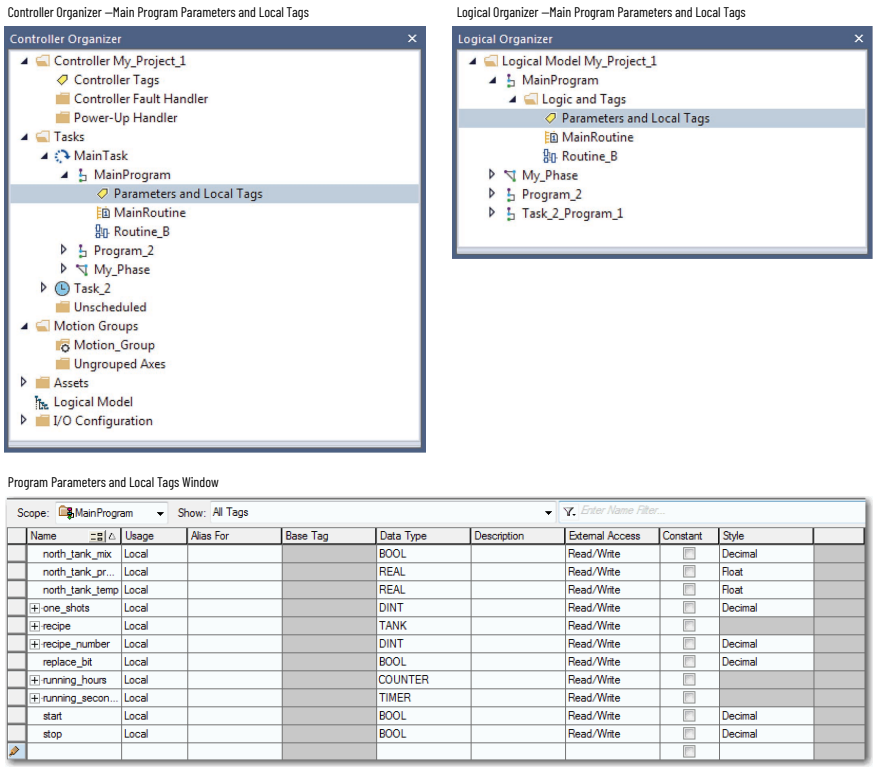
Parameters and Local Tags

With a Logix 5000® controller, you use a tag (alphanumeric name) to address data (variables). In Logix 5000® controllers, there is no fixed, numeric format. The tag name identifies the data and lets you do the following:

- Organize your data to mirror your machinery.
- Document your application as you develop it.

This example shows data tags that are created within the scope of the Main Program of the controller.

Figure 41. Parameters and Local Tags



Program Parameters

Program parameters define a data interface for programs to facilitate data sharing. Data sharing between programs can be achieved either through pre-defined connections between parameters or directly through a special notation.

Unlike local tags, all program parameters are publicly accessible outside of the program. Additionally, HMI external access can be specified on an individual basis for each parameter.

There are several guidelines on how to create and configure parameters and local tags for optimal task and program execution:

- Logix 5000 Controllers and I/O Tag Data Programming Manual, publication 1756-PM004
- Logix 5000 Controllers Program Parameters Programming Manual, publication 1756-PM021
- Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094

Programming Languages

The Studio 5000 Logix Designer® application supports these programming languages.

Table 28. Supported Programming Languages

Language	Is best used in programs with
Ladder Diagram (LD)	Continuous or parallel execution of multiple operations (not sequenced). Boolean or bit-based operations. Complex logical operations. Message and communication processing.

Table 28. Supported Programming Languages (continued)

Language	Is best used in programs with
	Machine interlocking. Operations that service or maintenance personnel have to interpret to troubleshoot the machine or process. **IMPORTANT**: Ladder Diagram is the only programming language that can be used with the Safety Task on GuardLogix® 5580 controllers. **IMPORTANT**: Ladder Diagram is the only programming language that can be used with the Safety Task on Compact GuardLogix® 5380 controllers.
Function Block Diagram (FBD)	Continuous process and drive control. Loop control. Calculations in circuit flow.
Sequential Function Chart (SFC)	High-level management of multiple operations. Repetitive sequence of operations. Batch process. Motion control that uses structured text. State machine operations.
Structured Text (ST)	Complex mathematical operations. Specialized array or table loop processing. ASCII string handling or protocol processing.

For more information, see the Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001.

Add-On Instructions

With your programming software, you can design and configure sets of commonly used instructions to increase project consistency. Similar to the built-in instructions that are contained in the controllers, these instructions you create are called Add-On Instructions.

Add-On Instructions reuse common control algorithms. With them, you can do the following:

- Ease maintenance by creating logic for one instance.
- Apply source protection to help protect intellectual property.
- Reduce documentation development time.

You can use Add-On Instructions across multiple projects. You can define your instructions, obtain them from somebody else, or copy them from another project. This table explains some of the capabilities and advantages of using Add-On Instructions.

Table 29. Add-On Instruction Capabilities

Capability	Description
Save Time	With Add-On Instructions, you can combine your most commonly used logic into sets of reusable instructions. You save time when you create instructions for your projects and share them with others. Add-On Instructions increase

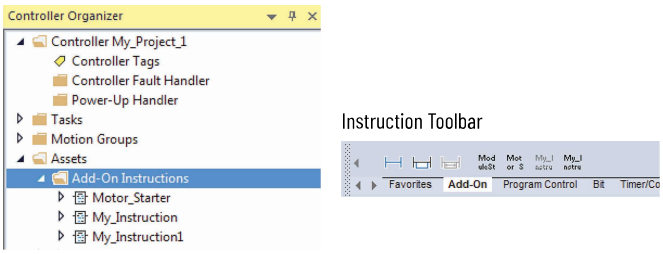
Table 29. Add-On Instruction Capabilities (continued)

Capability	Description
	project consistency because commonly used algorithms all work in the same manner, regardless of who implements the project.
Use Standard Editors	You create Add-On Instructions by using one of three editors: • Ladder Diagram • Function Block Diagram • Structured Text
Export/Import Add-On Instructions	You can export/import Add-On Instructions to other projects and copy and paste them from one project to another. Give each instruction a unique, descriptive name to make it easier to manage and reuse your collection of Add-On Instructions.
Use Context Views	Context views let you visualize the logic of an instruction for instant, simplified online troubleshooting of your Add-On Instructions.
Document the Instruction	When you create an instruction, you enter information for the description fields. Each instruction definition includes revision, change history, and description information. The description text also becomes the help topic for the instruction. You can also generate a signature for the Add-On Instruction and include the Add-On Instruction in a tracking group.
Apply Source Protection	When you create Add-On Instructions, you can limit users of your instructions to read-only access, or you can bar access to the internal logic or local parameters that are used by the instructions. This source protection lets you stop unwanted changes to your instructions and helps protect your intellectual property. You can pre-compile and encrypt your Add-On Instruction for better Intellectual property protection. This feature has less of a performance impact than the Logix Designer application source protection.

Once defined in a project, Add-On Instructions behave similarly to the built-in instructions in the controllers.

With Studio 5000 Logix Designer® application version 31 and greater, Add-On Instructions appear under the Assets folder in the organizer. They also appear on the instruction toolbar for easy access along with internal instructions.

Figure 42. Add-On Instructions Example



Extended Properties

The Extended Properties feature lets you define more information, such as limits, engineering units, or state identifiers for various components within your controller project.

Table 30. Extended Properties

Component	Extended Properties
Tag	In the tag editor, add extended properties to a tag.
User-defined data type	In the data type editor, add extended properties to data types.
Add-On Instructions	In the properties that are associated with the Add-On Instruction definition, add extended properties to Add-On Instructions.

Pass-through behavior is the ability to assign extended properties at a higher level of a structure or Add-On Instruction and have that extended property automatically available for all members. Pass-through behavior is available for descriptions, state identifiers, and engineering units and you can configure it.

Configure pass-through behavior on the Project tab of the Controller Properties dialog box. If you choose not to show pass-through properties, only extended properties that have been configured for a given component are displayed.

Pass-through behavior is not available for limits. When an instance of a tag is created, if limits are associated with the data type, the instance is copied.

Use the .@Min and .@Max syntax to define tags that have limits, as there is no indication in the tag browser that limit extended properties are defined for a tag. If you try to use extended properties that have not been defined for a tag, the editors show a visual indication and the routine does not verify. Visual indicators include the following:

- A rung error in Ladder Logic
- A verification error X in Function Block Diagrams
- The error underlined in Structured Text

You can access limit extended properties that .@Min and .@Max syntax defines. However, you cannot write to extended properties values in logic.

For more information on Extended Properties, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

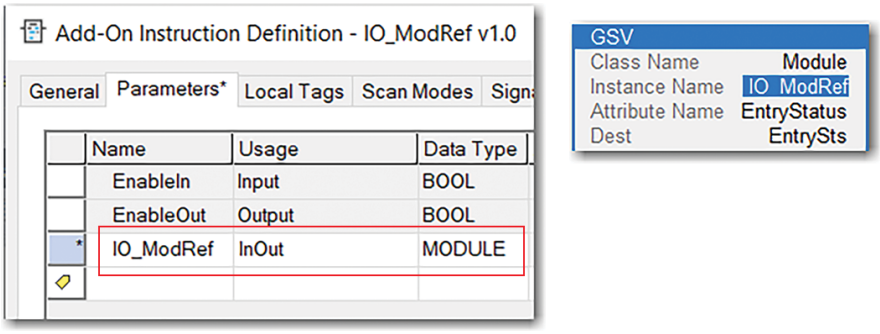
Module Object

The MODULE object provides status information about a module. To select a particular module object, set the Object Name operand of the GSV/SSV instruction to the module name. The specified module must be present in the I/O Configuration section of the controller organizer and must have a device name.

You can access a MODULE object directly from an Add-On Instruction. Previously, you could access the MODULE object data but not from within an Add-On Instruction.

You must create a Module Reference parameter when you define the Add-On Instruction to access the MODULE object data. A Module Reference parameter is an InOut parameter of the MODULE data type that points to the MODULE Object of a hardware module. You can use module reference parameters in both Add-On Instruction logic and program logic.

Figure 43. Module Reference Parameter



For more information on the Module Reference parameter, see the Studio 5000 Logix Designer® application online help and the Logix 5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010.

The MODULE object uses the following attributes to provide status information:

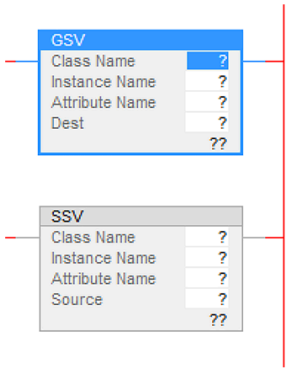
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Controller Status

The controller uses Get System Value (GSV) and Set System Value (SSV) instructions to get and set (change) controller data. The controller stores system data in objects.

The GSV instruction retrieves the specified information and places it in the destination. The SSV instruction sets the specified attribute with data from the source. Both instructions are available from the Input/Output tab of the Instruction toolbar.

Figure 44. GSV and SSV Instructions for Monitoring and Setting Attributes



When you add a GSV/SSV instruction to the program, the object classes, object names, and attribute names for the instruction are shown. For the GSV instruction, you can get values for the available attributes. For the SSV instruction, only the attributes you can set are shown.

Some object types appear repeatedly, so you have to specify the object name. For example, there can be several tasks in your application. Each task has its own Task object that you access by the task name.

The GSV and SSV instructions monitor and set many objects and attributes. See the Studio 5000 Logix Designer® online help for the GSV and SSV instructions.

I/O Connections

If communication with a device in the I/O configuration of the controller does not occur in an application-specific period, the communication times out and the controller produces warnings.

The minimum timeout period that, once expired without communication, causes a timeout is 100 ms. The timeout period can be greater, depending on the RPI of the application. For example, if your application uses the default RPI = 20 ms, the timeout period is 160 ms.

When a timeout does occur, the controller produces these warnings;

- I/O Fault status information scrolls across the 4-character status display of the controller.
- An exclamation point shows over the I/O configuration folder and over the devices that have timed out.
- A module fault code is produced, which you can access via the following:
  - The Module Properties dialog box
  - A GSV instruction

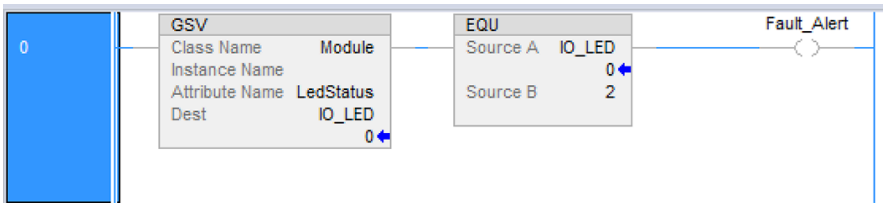
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication 1756-PM014.

I/O Communication Timeout

You can use this example to help determine if controller communication has timed out:

- The GSV instruction gets the status of the I/O status indicator (via the LEDStatus attribute of the Module object) and stores it in the IO_LED tag.
- IO_LED is a DINT tag that stores the status of the I/O status indicator or status display on the front of the controller.
- If IO_LED equals 2, then at least one I/O connection has been lost and the Fault_Alert is set.

Figure 45. GSV Used to Identify I/O Timeout



IMPORTANT: Safety Consideration

Safety controllers have individual connection status on each safety I/O module as part of the input tag.

I/O Communication to a Specific I/O Module Time Out

If communication times out with a device (module) in the I/O configuration of the controller, the controller produces a fault code and fault information for the module. You can use GSV instructions to get fault code and information via the FaultCode and FaultInfo attributes of the Module object.

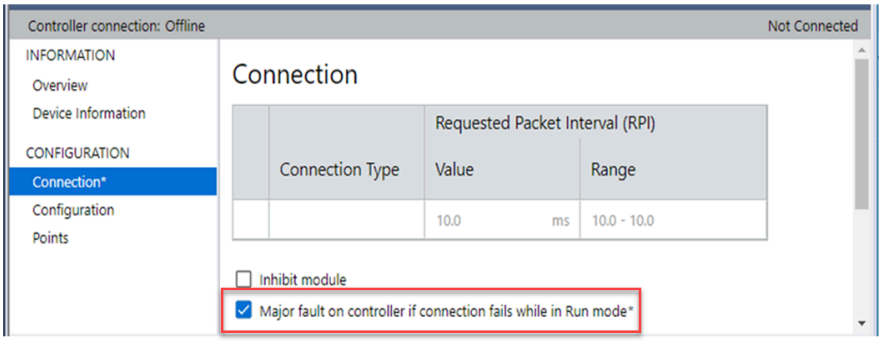
I/O Module Connection Faults

Depending on your application, you may want an I/O connection error to cause the Controller Fault Handler to execute. To do so, set the module property that causes a major fault to result from an I/O connection error. The major fault causes the execution of the Controller Fault Handler.

ATTENTION: You cannot program Safety I/O module connections or safety produce/consume connections to automatically cause a major fault on the controller.

If it is important to interrupt your normal program scan to handle an I/O connection fault, set the 'Major Fault On Controller If Connection Fails While In Run Mode' and put the logic in the Controller Fault Handler.

Figure 46. I/O Connection Fault Causes Major Fault



If responding to a failed I/O module connection can wait until the next program scan, put the logic in a normal routine and use the GSV technique that is described on page 140 to call the logic.

First, develop a routine in the Controller Fault Handler that can respond to I/O connection faults. Then, in the Module Properties dialog box of the I/O module or parent communication module, check 'Major Fault On Controller If Connection Fails While in Run Mode.

It takes at least 100 milliseconds to detect an I/O connection loss, even if the Controller Fault Handler is used.

For more information about programming the Controller Fault Handler, see the Logix 5000 Major, Minor, and I/O Faults Programming Manual, publication1756-PM014.

Sample Controller Projects

The Studio 5000 Logix Designer® application includes sample projects that you can copy and modify to fit your application. To access the sample projects, choose Sample Project on the dialog box.

Figure 47. Sample Projects

Develop Safety Applications

You can use both standard (non-safety-related) and safety-related components in a safety control system. Within a safety project, you can perform standard automation control from standard tasks. Controllers with safety functions also support the same functions as other controllers. What differentiates these controllers from standard controllers is that the controllers also support a SIL 2 or SIL 3 capable safety task.

A logical and visible distinction is required between the standard and safety-related portions of the application. The Studio 5000 Logix Designer® application provides this differentiation via the safety task, safety programs, safety routines, safety tags, and safety I/O devices.

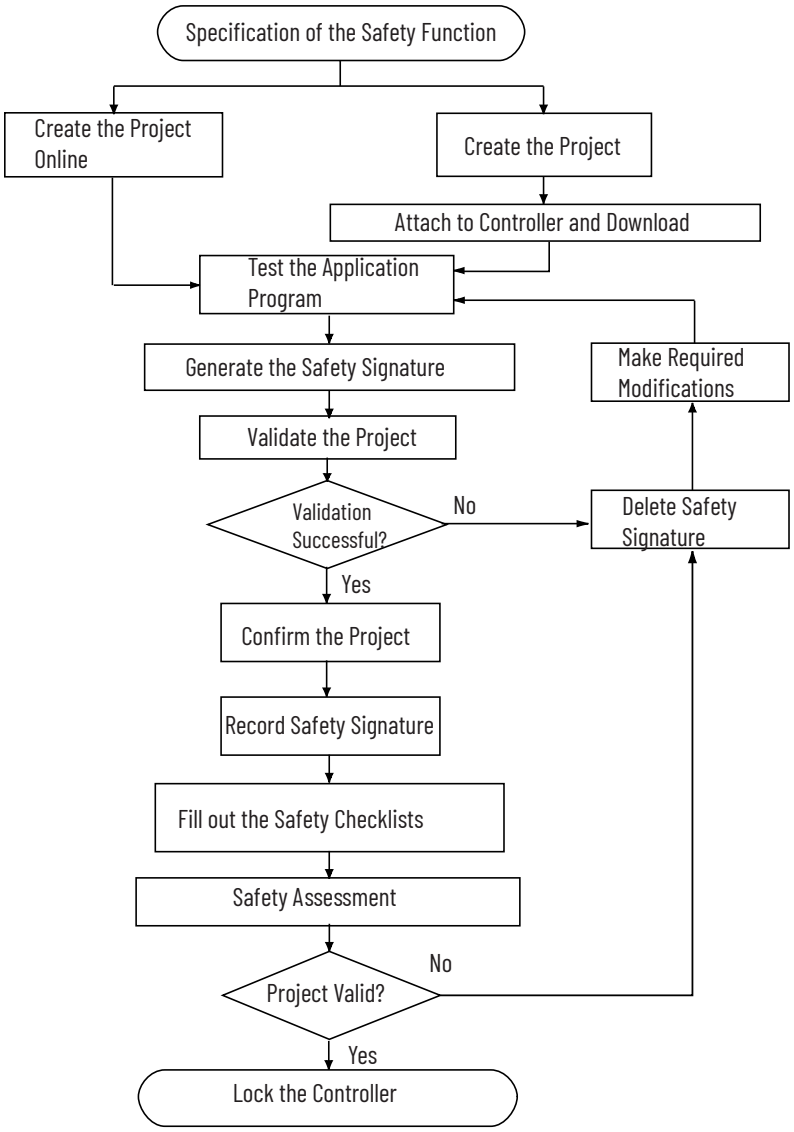
ATTENTION: Performing online edits to logic, data, or the configuration can affect the safety functions of the system if the edits are performed while the application is running. Online edits should only be done if necessary. If the edits are not performed correctly, they can stop the application. You must use alternative safety measures and constraints during online edits.

Program Safety Applications

The diagram below shows the steps required to commission a safety system. For more information, see one of the following: 1756-RM012.

Table 31. Safety Reference Manuals

Controller Type	Safety Reference
ControlLogix®5590	ControlLogix 5590 Controller High Availability User Manual, 1756-UM901
GuardLogix®5580 Compact GuardLogix®5580	GuardLogix 5580 and Compact GuardLogix 5380 Controllers Reference Manual,1756-RM012.


Specification of the Safety Function
Create the Project Online
Create the Project
Attach to Controller and Download
Test the Application Program
Generate the Safety Signature
Make Required Modifications
Validate the Project
Validation Successful?
No
Delete Safety Signature
Yes
Confirm the Project
Record Safety Signature
Fill out the Safety Checklists
Safety Assessment
No
Project Valid?
Yes
Lock the Controller

Develop Secure Applications

The following controllers support IEC-62443-4-2 SL 1 security certification.

Table 32. IEC 62443-4-2 SL 1-certified Controllers

Controller	Firmware Revision
ControlLogix® 5580 standard controllers	32 or later
ControlLogix®5580 NSE, XT, K, and Process controllers	33 or later
GuardLogix®5580 controllers	37 or later

IMPORTANT: If enabled, the following features cause the controller to be excluded from IEC-62443-4-2 SL 1 security certification:

- OPC UA
- Redundancy
- Secure socket objects
- Remote deployment of save/restore images

To help meet these requirements, you must use this publication and the Configure System Security Features User Manual, publication SECURE-UM001. The Configure System Security Features User Manual describes how to configure and use Rockwell Automation® products to improve the security of your industrial automation system.

The controller accepts all values appropriate for a tag data type, and it is the responsibility of the user program to specify valid ranges and perform validity to check for those ranges. The controller verifies incoming messages for syntax, length, and format.

You can apply these same measures to other ControlLogix® and GuardLogix® controllers, but without security certification.

Table 33. Security Additional Resources

Resource	Description
Security Design Guide Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct vulnerability assessments, implement Rockwell Automation® products in a secure system, harden the control system, manage user access, and dispose of equipment.
Logix 5000 Controllers Security Programming Manual, publication 1756-PM016	Describes how to configure security for the Studio 5000 Logix Designer® application, and explains how to configure source protection for your logic and projects.
CIP Security Application Technique, publication SECURE-AT001	Describes how to plan an implement a Rockwell Automation® system that supports the CIP Security™ protocol.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Defines manufacturing-focused reference architectures to help accelerate the successful deployment of

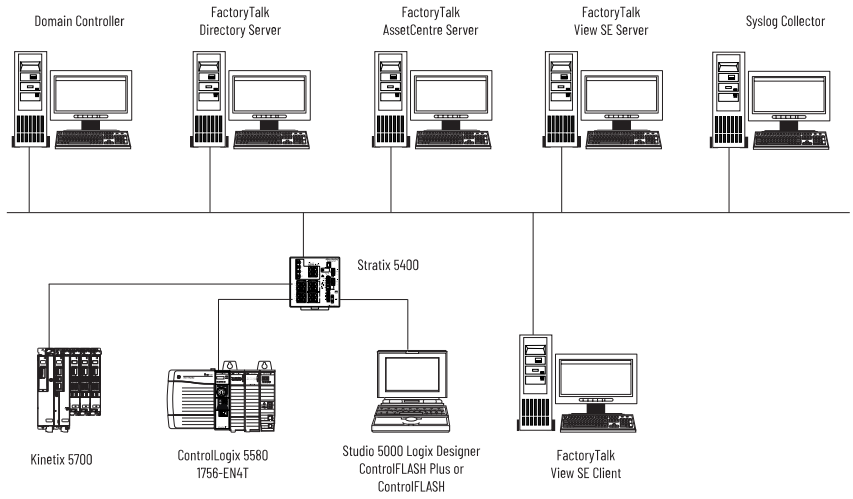
Table 33. Security Additional Resources (continued)

Resource	Description
	standard networking technologies and convergence of manufacturing and enterprise/business networks.

Security Certification Requirements

The following figure shows an example of a secure control system that implements other security-focused products. For certification requirements related to other security-focused products, see the security checklists.

Figure 48. Secure Architecture Example



Follow the security requirements in this section to secure the system and controller. It is your responsibility to monitor the system periodically to make sure that the security settings function as you configured them.

Requirements for Identification and Authorization

Table 34. Requirements for Identification and Authorization

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® Securitysoftware Studio 5000 Logix Designer® application	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. • The Logix Designer application enforces the policy based on the access policies that are provided to it by FactoryTalk® Security for the software authenticated user. Once authenticated, the Logix Designer application acts as your interface to the controller. This applies to all protected CIP™ communications to the controller, whether from Ethernet, backplane, or USB. • The FactoryTalk Services Platform offers feature access control to manage user access to product features such as controller download, project import, project create, and firmware update. For more information, see Configure System Security Features User Manual, SECURE-UM001 .

Table 34. Requirements for Identification and Authorization (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
(Safety controllers only). Access control to generate and delete the safety signature	May be required based on system design, threat model, and risk assessment.	Configure FactoryTalk® Security to restrict access to generate and delete the safety signature. To configure FactoryTalk Security permissions, see the Configure System Security Features User Manual, SECURE-UM001.
(Safety controllers only). Access control to safety-lock and safety-unlock actions	May be required based on system design, threat model, and risk assessment.	Configure FactoryTalk® Security to restrict access to safety-lock and safety-unlock actions. To configure FactoryTalk Security permissions, see the Configure System Security Features User Manual, SECURE-UM001.

Requirements for Use Control

Table 35. Requirements for Use Control

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
Studio 5000 Logix Designer®application	May be required based on system design, threat model, and risk assessment.	Configure the controller project in the Logix Designer application to use these user access methods: • License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. • License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. • Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. • The Logix Designer application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag. For more information, see Logix 5000 Controllers Security Programming Manual, 1756-PM016 .
FactoryTalk® Security software Studio 5000 Logix Designer® application	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. • The Logix Designer application enforces the policy based on the access policies that are provided to it by FactoryTalk® Security for the software authenticated user. Once authenticated, the Logix Designer application acts as your interface to the controller, including all protected CIP™ communication to the controller, whether from Ethernet, backplane, or USB. • The FactoryTalk® Services Platform offers feature access control to manage user access to product features, such as controller download, project import, project create, and firmware update. • In FactoryTalk® Security, define which users can change controller modes and download projects to the controller. • Security authority binding restricts the controller to a specific FactoryTalk® Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
Controller keyswitch position	May be required based on system design,	Place the keyswitch in the RUN position to help prevent unauthorized remote configuration changes to the controller, and restrict some communication services.

Table 35. Requirements for Use Control (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
	threat model, and risk assessment.	Remove the keyswitch from a running controller to help prevent modifications to the configuration or program. **IMPORTANT:** Do not apply a new security policy while the controller is in RUN mode. RUN mode does not help prevent updates to the security policy, and a policy change has the potential to disrupt a running control system.
Disable the controller Ethernet port	May be required based on system design, threat model, and risk assessment.	The Ethernet port is enabled by default. Disable the Ethernet port if required by the system design, threat model, or risk assessment. For more information, see Disable the Ethernet Port on the Port Configuration Tab on page 162 and Disable the Ethernet Port with an MSG Instruction on page 163.
Disable Simple Network Management Protocol (SNMP) on the controller (firmware revision 32 or later)	May be required based on system design, threat model, and risk assessment.	SNMP is disabled by default. If SNMP has been enabled, disable SNMP if required by the system design, threat model, or risk assessment. For more information, see Use a CIP Generic MSG to Disable SNMP on the Controller on page 95.
Disable the controller CIP Security™ ports	May be required based on system design, threat model, and risk assessment.	CIP Security™ ports on the controller are enabled by default. Disable the CIP Security™CIP Security™ ports if required by the system design, threat model, or risk assessment. For more information, see Disable CIP Security Ports via FactoryTalk Linx on page 165 and Disable CIP Security Ports via a CIP Generic MSG Instruction on page 166.
Disable the controller USB ports	May be required based on system design, threat model, and risk assessment.	The USB port on the controller is enabled by default. Disable the USB port if required by the system design, threat model, or risk assessment. For more information, see Disable the Controller USB Port on page 168.
Disable the controller SD card	May be required based on system design, threat model, and risk assessment.	The SD card is enabled by default. Disable the SD card if required by the system design, threat model, or risk assessment. For more information, see Disable the Controller SD Card on page 170.
Disable controller webpages	May be required based on system design, threat model, and risk assessment.	Controller webpages for diagnostics are read-only. With Studio 5000 Logix Designer® application version 33 or later, controller webpages are disabled by default. Disable the controller webpages if required by the system design, threat model, or risk assessment. For more information, see Disable Controller Web Pages on page 177.

Requirements for System Integrity

Table 36. Requirements for System Integrity

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	The FactoryTalk® AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes based on FactoryTalk® Security settings. This server functionality assists with diagnostics and troubleshooting and reduces maintenance time for production assets.
FactoryTalk® Security software		

Table 36. Requirements for System Integrity (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		Configure the Device Monitor - Change Detect operation for the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
ControlFLASH Plus® or ControlFLASH™ software	Yes	Use ControlFLASH Plus® or ControlFLASH™ software to update controller firmware. Digitally signed firmware files have a .DMK (Device Management Kit) extension. ControlFLASH™ software authenticates the origin of a DMK file and validates the file before downloading in the device.
Studio 5000 Logix Designer® application	Yes	You can generate a signature on an Add-On Instruction. This signature seals (encrypts) the Add-On Instruction to help prevent modification.
Controller firmware update	Yes	To meet IEC-62443-4-2 SL 1 security requirements, you must use a certified version of the controller firmware. We recommend that you use the latest minor revision of your firmware. The controller is designed such that: • You cannot update firmware when the keyswitch is in the RUN position. • You cannot go online with a controller that is in a firmware update process. For more information, see Controller Firmware and Logix Designer Application Compatibility on page 34.
Trusted® slots on the controller	May be required to maintain network segmentation.	The Trusted slots feature restricts communication paths through which certain operations are performed on Logix 5000® controllers. A Trusted slot is not configured by default. For more information, see Trusted Slots on the Controller on page 97.
User-definable major controller faults	May be required based on system design, threat model, and risk assessment.	If your application requires a major fault in addition to those already monitored by the controller, define a predetermined state with a major fault so that outputs are off. For more information, see Configure User-definable Major Faults on page 155.
(Safety controllers only). Safety signature	Yes for SIL 2 or SIL 3 configuration.	Safety controllers use a safety signature to verify the integrity of a safety application. The safety signature must be applied on a SIL 2/PLd or SIL 3/PLe safety controller to perform automated background integrity checks on the safety application. We recommend that you record and store the safety signature in a separate location to verify its integrity during audits or when tampering is suspected.

Requirements for Data Confidentiality

Table 37. Requirements for Data Confidentiality

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® Security software	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. • The FactoryTalk® Services Platform offers feature access control to manage user access to product features such as controller download, project import, project create, and firmware update. • In FactoryTalk® Security, define which users can change controller modes and download projects to the controller. • Security authority binding restricts the controller to a specific FactoryTalk® Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access.

Table 37. Requirements for Data Confidentiality (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		For more information, see Configure System Security Features User Manual, SECURE-UM001 .
FactoryTalk® Policy Manager software	Yes	Use the FactoryTalk® Policy Manager software to define a secure data transport over an EtherNet/IP™ network to the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
License-based source and execution protection	May be required based on system design, threat model, and risk assessment.	Configure licenses to manage access to controller source logic and execution of that logic. These licenses are not enabled by default. • License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. • License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. • License-based source protection **cannot** restrict access to safety logic and safety Add-On Instructions. For more information, see License-based Source and Execution Protection on page 156.
Access to tag data	May be required based on system design, threat model, and risk assessment.	Configure the following attributes in the Logix Designer application to control access to tag data: • External Access attribute—Controls how external applications can access tags. • Constant attribute—Determines if controller logic can change a tag.

Requirements for Restricted Data Flow

Table 38. Requirements for Restricted Data Flow

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
CIP Security™	Yes	Use FactoryTalk® Policy Manager software to define zones and conduits. For more information, see CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001.

Requirements for Timely Response to Events

Table 39. Requirements for Timely Response to Events

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	Configure and use the following: • Audit log accessibility • Continuous monitoring

Table 39. Requirements for Timely Response to Events (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		For more information, see the following: • Configure System Security Features User Manual, SECURE-UM001 . • System Security Design Guidelines Reference Manual, SECURE-RM001
Syslog collector	Yes, if not using FactoryTalk® AssetCentre for logging	The controller supports syslog event logging. Choose a syslog collector that supports the following: • RFC-5424 syslog protocol • Ability to receive messages from the controller **IMPORTANT:** The controller sends events to a syslog collector through a front Ethernet port. The Ethernet port must be connected to the same network as the syslog collector. To set the IP address of the syslog collector, use FactoryTalk® Policy Manager software. For more information, see CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001. To view a list of syslog messages and their descriptions, see 1756-RD001.
Controller change detection	Yes	Enable the change detection feature to monitor program components to determine whether they change. The change detection feature is not enabled by default. For more information, see Change Detection on page 159.
Controller component tracking	May be required based on system design, threat model, and risk assessment	Enable component tracking to monitor configurable program components to determine whether they change. Component tracking is not enabled by default. For more information, see Component Tracking on page 160.
Disabled controller log auto-write	Yes	The controller log stores security-related events that can be accessed via FactoryTalk AssetCentre software. To help prevent the potential loss of controller logs before FactoryTalk® AssetCentre can access them, follow these guidelines: • Do not use a Message to Self (MSG with a Path of THIS) to auto-write controller logs to the SD card. • Do not manually force a write of controller logs to the SD card. By default, the controller log auto-write is disabled. For more information, see Controller Logging on page 161.

Requirements for Resource Availability

Table 40. Requirements for Resource Availability

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	Configure and use the following: • Asset inventory • Control system backup • Disaster recovery

Table 40. Requirements for Resource Availability (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		For more information, see Configure System Security Features User Manual, SECURE-UM001.
UPS	Yes	Provide your own UPS with a separate battery unit and redundant power supplies. Size the UPS so that is correctly supports the system and provides enough power to shut down servers and workstations properly.

Configure User-definable Major Faults

To suspend (shut down) the controller based on conditions in the application, create a user-defined major fault. With a user-defined major fault:

- The fault type = 4.
- Define a value for the fault code. Choose a value between 990...999. These codes are reserved for user-defined faults.
- The controller handles the fault the same as other major faults:
- The controller changes to the Program mode and stops running the logic. Outputs are set to their configured state or value for faulted mode.

To create a user-defined major fault, do the following.

1. Create a fault routine for the program.
2. Configure the program to use the fault routine.
3. Jump to the fault routine.

Create a Fault Routine

To create a fault routine, do the following.

1. In the Controller Organizer, right-click the program and click Add > New Routine.
2. On the New Routine dialog box, in the Name field, type a name for the fault routine.
3. In the Type field, use the default setting, Ladder Diagram.
4. In Program or Phase field, select the program or phase where the routine will reside.
5. In the Assignment field, select Fault.
6. (optional) Select the Open Routine checkbox, to open the ladder logic program immediately.
7. Click OK.

Configure the Program to Use the Fault Routine

To configure the program to use the fault routine, do the following.

1. In the Controller Organizer, right-click the program and click Properties.
2. On the Properties dialog box, click the Configuration tab.
3. In the Fault field, select the fault routine.
4. Click OK.

Jump to the Fault Routine

In the main routine of the program, enter the following rung, where:

- Fault_Routine_1 is the name of the fault routine for the program.
- 999 is the value for the fault code.

When Tag_1.0 = 1, execution jumps to name_of_fault_routine, a major fault occurs and the controller enters the faulted mode. Outputs go to the faulted state. The Controller Properties dialog box, Major Faults tab, displays the code 999.

CIP Bridging Control

CIP™ Bridging Control enables you to control the traffic flow between physical communication interfaces and backplanes.

Devices within an Industrial Control System (ICS) may involve multiple network interfaces. The use of Common Industrial Protocol (CIP™) on the backplanes and communication ports of Rockwell Automation devices can facilitate physical network segmentation. For EtherNet/IP™ interfaces, you can provide data bridging between two separate physical Ethernet networks by using CIP™.

The CIP Security™ communication modules and embedded EtherNet/IP™ interfaces can analyze and then allow or deny network traffic according to device-specific policies. You can use CIP™ Bridging to help prevent unintended data flows from occurring, especially data flows originating from unsecured parts of the system to secure parts of the system.

For more information, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

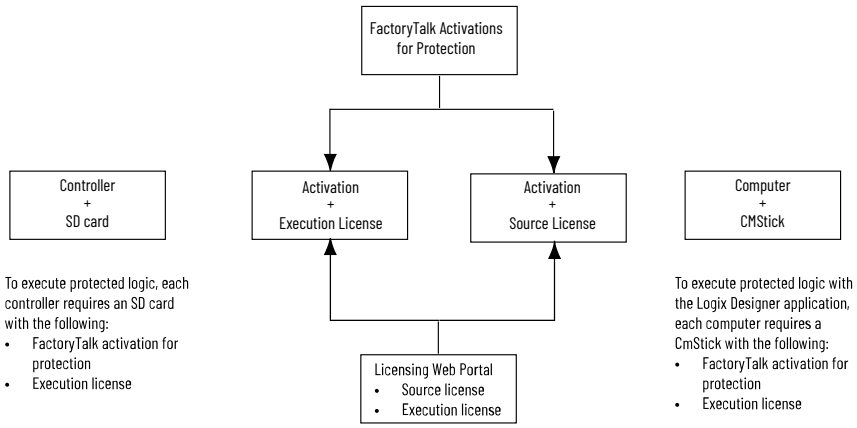
License-based Source and Execution Protection

Source protection helps prevent logic components from being modified based on a license.

Execution protection adds additional protection to controller logic. Execution protection makes sure that the right controller has access to execute the protected program. Use this with source protection to make sure that the right programmer has access to modify the logic.

Each device (controller or computer) requires an activation to access protection features. Each logic component or program requires a license to be accessed or executed.

Figure 49. Source and Execution Protection Example



To enable license-based protection, you need the following:

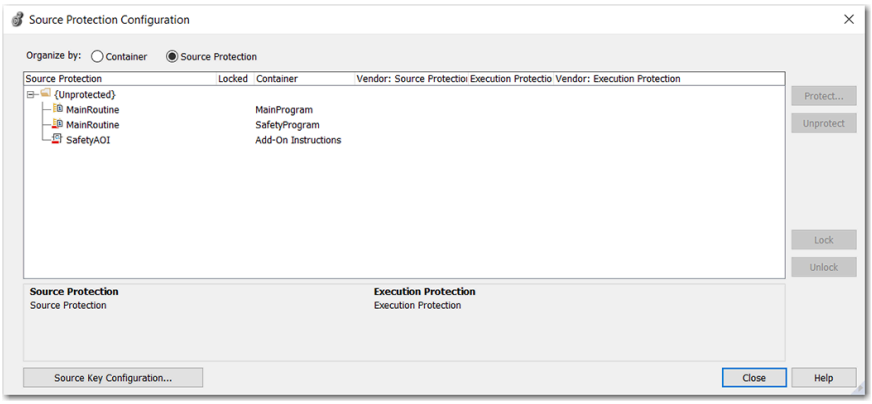
- A CmStick that contains a license with Use permission must be present locally on any USB port on the computer. Use permission cannot be obtained from a network license server. All other license privileges can be contained on the local CmStick, or provided by a license server on the network.
- A license that contains the Protect permission, either on a local CmStick or provided by a license server on the network. When components are locked, unauthorized users cannot view or edit the component, but authorized users can run the project without a CmStick.

IMPORTANT: Enabling license-based protection can have a significant impact on download times.

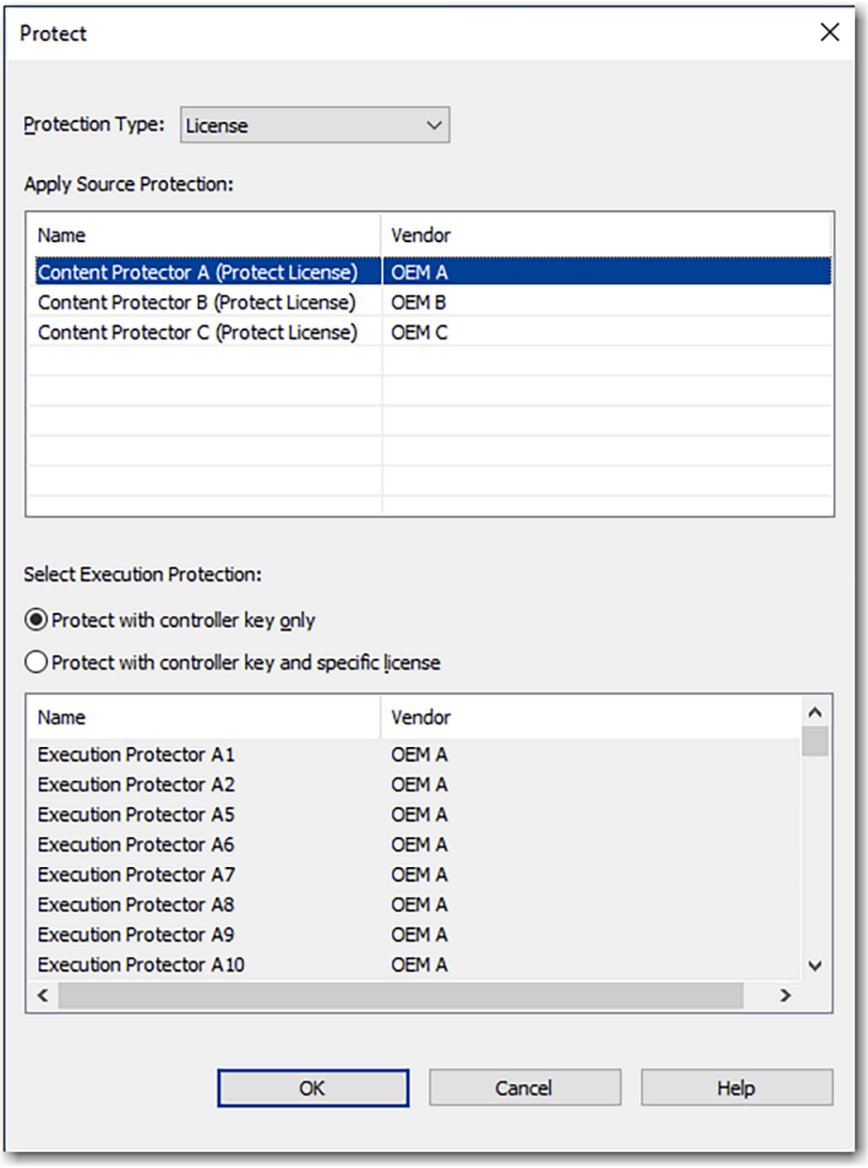
Enable License-based Protection

Complete the following.

1. Select Tools > Security > Configure Source Protection to open the Source Protection Configuration dialog box.



2. Insert the CmStick that contains the license that you want to use to help protect the component into the USB port on the computer. Licenses must contain the Protect permission to be used to protect components. If a license does not contain the Protect permission, it does not appear in the list of licenses.
3. In the Source Protection Configuration dialog box, select the component to be protected and click Protect.
4. In the Protect dialog box, select the license to apply.



5. Select the Execution Protection type:
   - Protect with controller key only. This option is selected by default. With this option selected, the component, when locked, runs only on a controller in the same family as the one specified for the project. For example, if you lock a License-based Protected component for a project on a ControlLogix® 5580 controller, the component can only be executed on another ControlLogix® 5580 controller.
   - Protect with controller key and specific license. When you select this option, the component runs only on a controller in the same family as the one specified for the project and that contains a CmCard with the execution license that you select. If you select Protect with controller key and specific license, select the execution license from the list of available licenses. After components are protected, they can also be locked. When you lock a component, it helps prevent users from viewing or editing the component, but allows authorized users to run it.

6. To return to the Source Protection Configuration dialog box, click OK.

To save changes to a component that is protected with License-Based Source Protection, a CmStick that contains the required license must be plugged into the computer that runs the Logix Designer application.

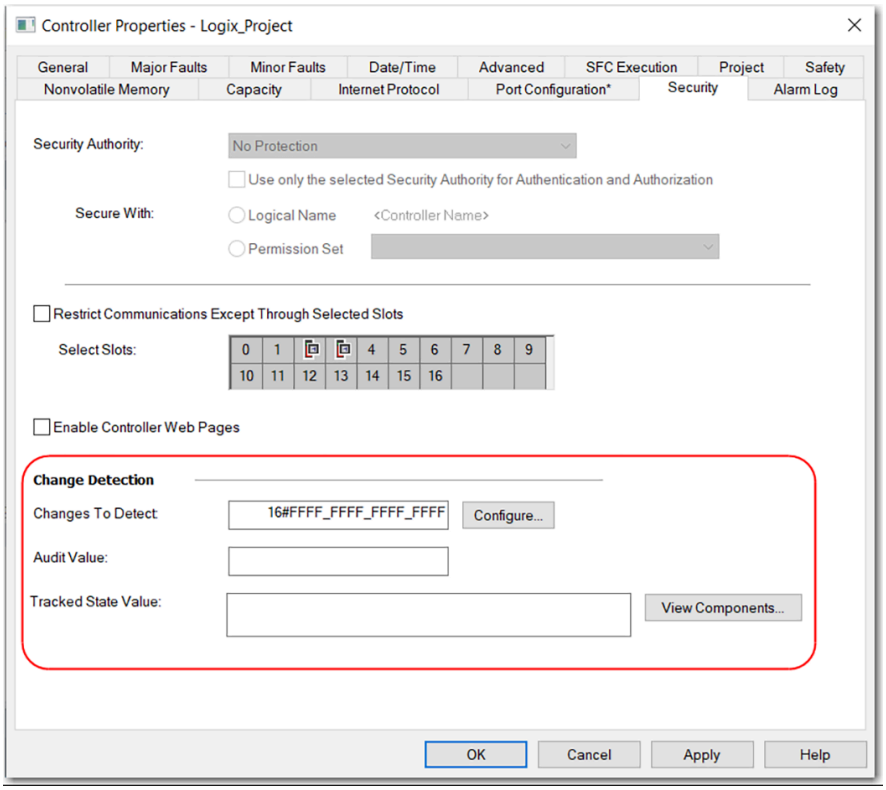
Make sure that you save your edits to the project or lock the protected components before removing the CmStick that contains the required license. If the license is not present, you could lose your edits to the project.

Change Detection

On the Security tab of the controller properties, the Change Detection feature tracks changes to a controller and generates an audit value when a monitored change occurs.

For more information about change detection, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.

Figure 50. Change Detection



Changes to Detect

Click Configure to open the Configure Changes to Detect dialog box. We recommend tracking the following changes for a standard controller. By default, all event types can cause the audit value to change, resulting in a default value of 0xFFFFFFFFFFFFFFFF.

- Project stored to removable media
- Online edits modified controller program
- Transaction committed
- SFC forces enabled
- SFC forces disabled

- SFS forces removed
- SFC element force value changed
- I/O forces enabled
- I/O forces disabled
- I/O forces removed
- I/O forces modified
- Firmware update attempted
- Firmware update from removable media attempted
- Remote mode change
- Controller switch mode change
- A major fault occurred
- All major faults cleared
- All major faults cleared through controller switch
- Task properties modified
- Program properties modified
- Removable media removed
- Removable media inserted
- Constant Tag value changed
- Multiple constant Tag values changed
- Constant Tag attribute cleared
- Constant Tag attribute set
- Custom Log Entry Added
- Correlation affected
- Alarm Log values cleared
- Parameter Connection has been modified
- Port configuration has been changed

By default, all event types can cause the audit value to change, resulting in a default value of 0xFFFFFFFFFFFFFFFF.

Audit Value

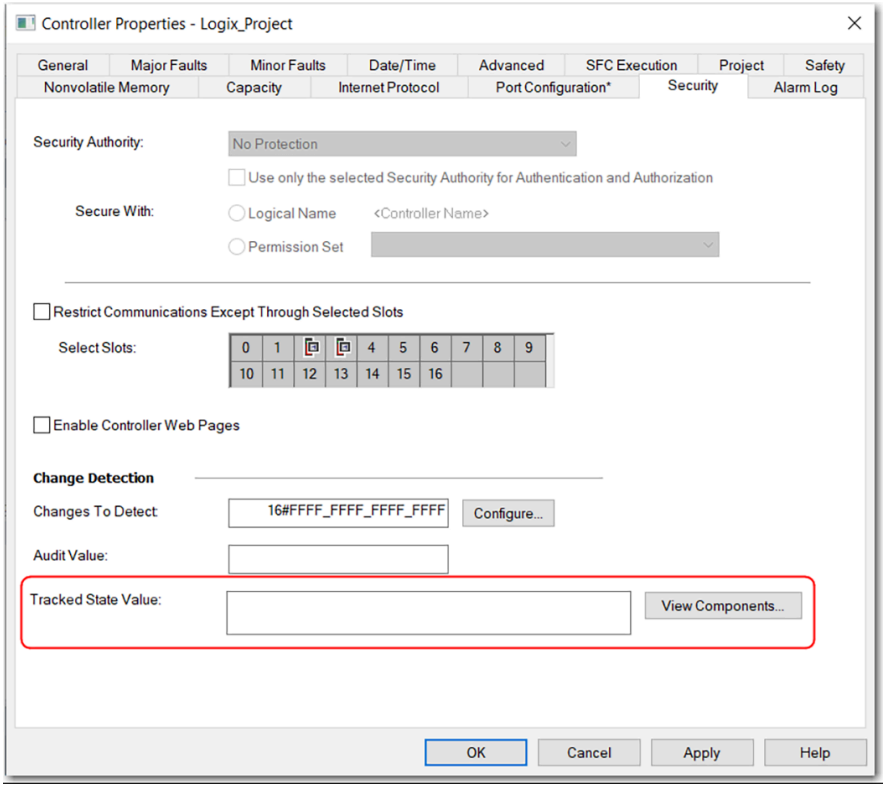
A unique value that is generated when a project is downloaded to the controller or loaded from a storage device. This value is updated when a change to an event occurs. Some events always cause an Audit Value change, while others are selectable in the Configure Changes to Detect dialog box. When the controller is offline, the Audit Value box is blank.

Component Tracking

On the Security tab of the Controller Properties dialog box, component tracking enables you to determine whether tracked routines, Add-On Instructions, I/O modules, and constant tags have been changed. The Studio 5000 Logix Designer® application creates a tracked state value to indicate the current state of all components.

For more information about component tracking, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.

Figure 51. Tracked State Value



Controller Logging

The controller log stores various security-related events that can be written to a memory card or accessed via FactoryTalk® AssetCentre or a third-party syslog collector. Some of these events are Logix Designer application request errors, control system events, backup/restore events, and configuration changes.

For more information on how to access the controller log, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.

For more robust logging and to help prevent rollover, use FactoryTalk® AssetCentre or a syslog collector.

Controller Ethernet Port

You can disable a controller Ethernet port with the Studio 5000 Logix Designer® application.

IMPORTANT: Remember the following:

- For controllers with two Ethernet ports, you can disable either of the Ethernet ports whether the controller uses Dual-IP mode or Linear/DLR mode.
- Once a port is disabled, you lose any connection that is established through the controller Ethernet port.
- You cannot disable Ethernet ports if the controller switch is in Run mode or if the FactoryTalk® Security settings deny this editing option.

Ethernet ports return to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset

- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - These examples clear the program from a controller:
  - Major nonrecoverable fault occurs.
  - Firmware update occurs.

You must reconfigure the settings to disable an Ethernet port after the port returns to its default settings.

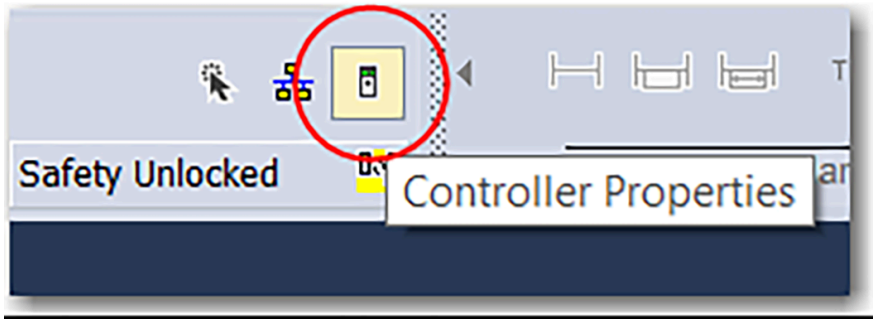
There are two ways to disable an Ethernet port:

- Disable an Ethernet Port on the Port Configuration Tab on page 162
- Disable an Ethernet Port with an MSG Instruction on page 163

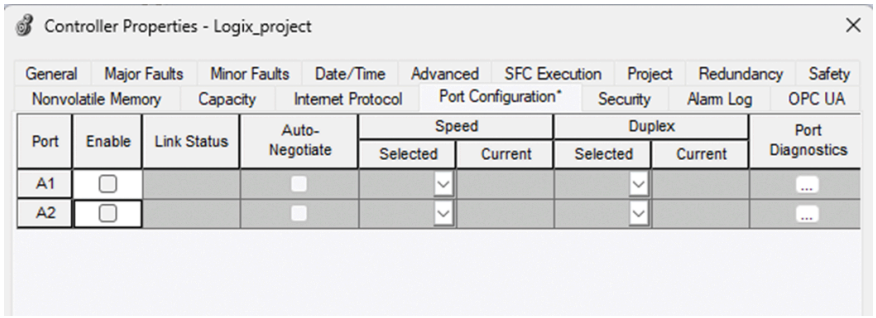
Disable an Ethernet Port on the Port Configuration Tab

You can disable an embedded Ethernet port on the controller. This method retains the setting in the project, so every time you download the project to the controller, the Ethernet port is disabled.

1. On the Online toolbar, click the Controller Properties button.



2. On the Controller Properties dialog box, click the Port Configuration tab.
3. On the Port Configuration tab, clear the Enable checkbox.



4. On the Port Configuration tab, click Apply.
   - If you are online when you make this change, then an Alert dialog box appears. On the dialog box, click Yes. The change takes effect immediately.
   - If you are offline, then the change takes effect when you download the program to the controller.
5. On the Port Configuration tab, click OK.

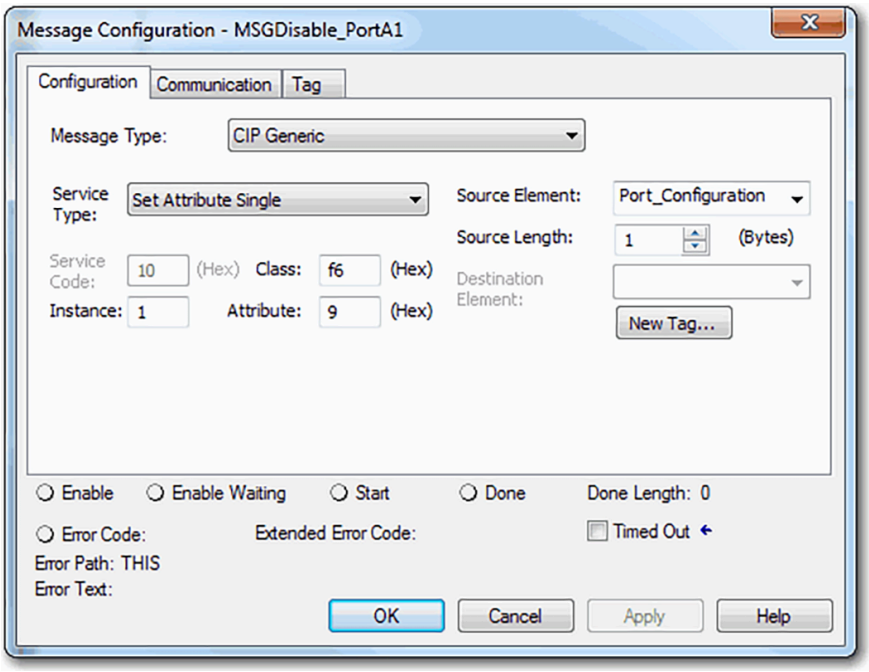
Disable an Ethernet Port with an MSG Instruction

You can use a CIP™ Generic MSG with a Path of THIS to execute this option. You cannot use this MSG instruction to disable an Ethernet port on another controller.

1. Add an MSG instruction to your program.
   This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.



IMPORTANT: These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

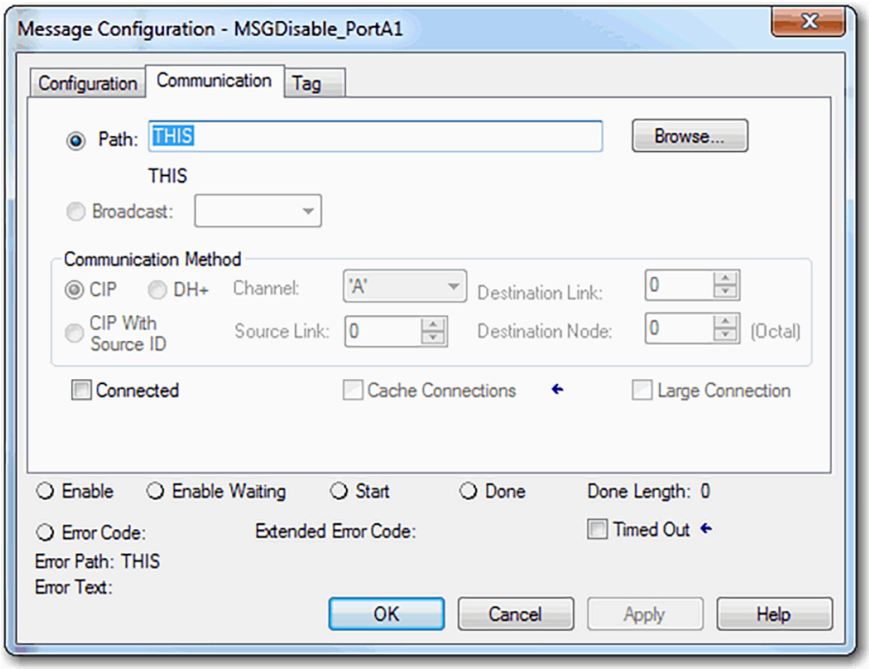
Table 41. Disable the Ethernet Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1 to disable the Ethernet port on controllers with a single Ethernet port, or disable Port A1 on controllers with two Ethernet ports. 2 to disable Port A2 on controllers with two Ethernet ports.
Class	f6

Field	Description
Attribute	9
Source Element	Controller tag of SINT data type. Source Element Tag Data: - 1 = Enable port - 2 = Disable Port In this example, the controller tag is name Port_Configuration.
Source Length	1

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, verify that the Source Element tag value is 2.

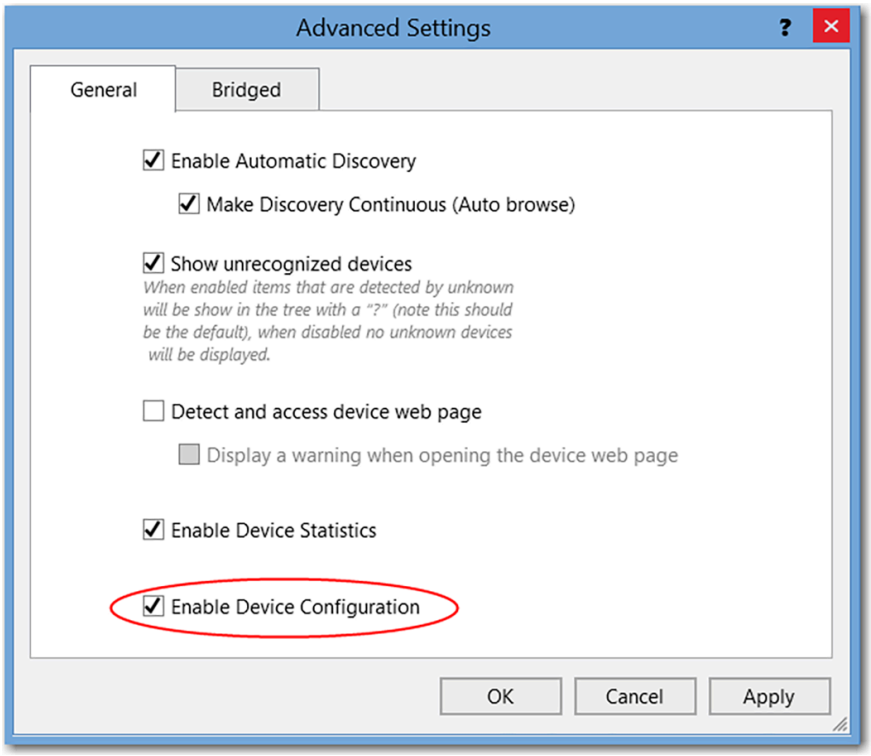
IMPORTANT: You can re-enable an Ethernet port after it is disabled.

To re-enable the port, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 1.

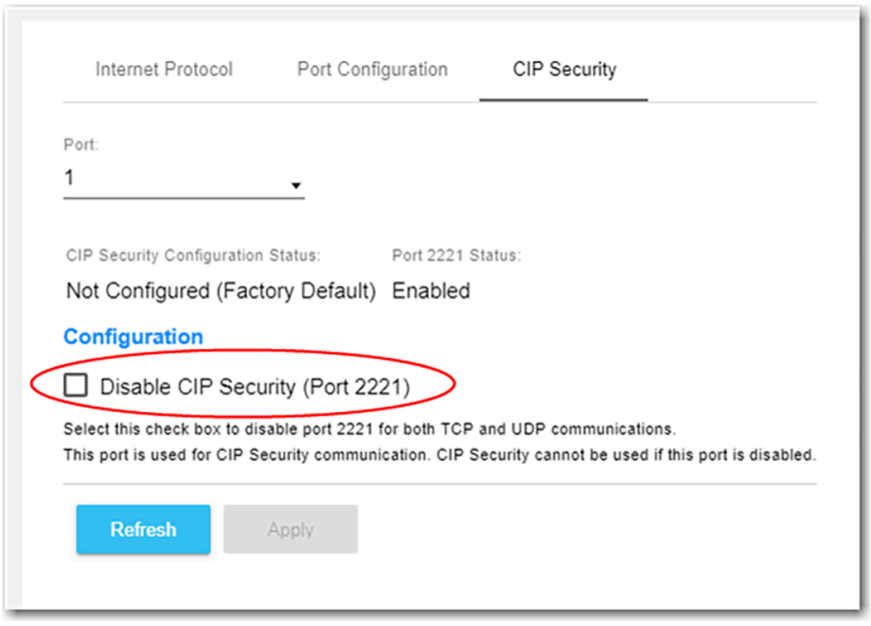
Disable CIP Security Ports via FactoryTalk Linx

To disable CIP Security™ ports via FactoryTalk® Linx, complete the following.

1. If the Device Configuration menu in FactoryTalk® Linx is not enabled, go to the Advanced Settings dialog box and check the Enable Device Configuration checkbox.



2. From the Device Configuration menu, click the CIP Security tab, and then check the Disable CIP Security (Port 2221) checkbox.



Disable CIP Security Ports via a CIP Generic MSG Instruction

To disable CIP Security™ ports via CIP™ Generic MSG instructions, complete the following.

IMPORTANT: This procedure disables CIP Security™ ports. To re-enable the ports, use the controller reset button to perform a Stage 2 reset, which returns the controller to a factory default state. For more information, see Stage 2 Reset on page 74.

You cannot use this MSG instruction to disable the CIP Security™ ports on another controller. The message only has to execute once rather than with every program scan.

1. Create a controller tag with the SINT[9] data type. In this example, the controller tag is named CIPSEC_DISABLE and must match the following image.

Name	Value	Style	Data Type
CIPSEC_DISABLE	{...}	Hex	SINT[9]
CIPSEC_DISABLE[0]	16#02	Hex	SINT
CIPSEC_DISABLE[1]	16#ad	Hex	SINT
CIPSEC_DISABLE[2]	16#08	Hex	SINT
CIPSEC_DISABLE[3]	16#11	Hex	SINT
CIPSEC_DISABLE[4]	16#00	Hex	SINT
CIPSEC_DISABLE[5]	16#ad	Hex	SINT
CIPSEC_DISABLE[6]	16#08	Hex	SINT
CIPSEC_DISABLE[7]	16#06	Hex	SINT
CIPSEC_DISABLE[8]	16#00	Hex	SINT

   Before you enable the MSG instruction, consider the following:
   - The element CIPSEC_DISABLE[4] is responsible for disabling UDP port 2221 and EtherNet/IP™ over DTLS, transport class 0/1.
   - The element CIPSEC_DISABLE[8] is responsible for disabling TCP port 2221 and EtherNet/IP™ over TLS, UCMM, and transport class 3.
   - To disable the controller CIP Security ports, the elements CIPSEC_DISABLE[4] and CIPSEC_DISABLE[8] in the SINT array for the Source Element CIPSEC_DISABLE must be 0.
2. Add an MSG instruction to your program.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in RUN mode or if the FactoryTalk® Security settings deny this editing option.
3. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.

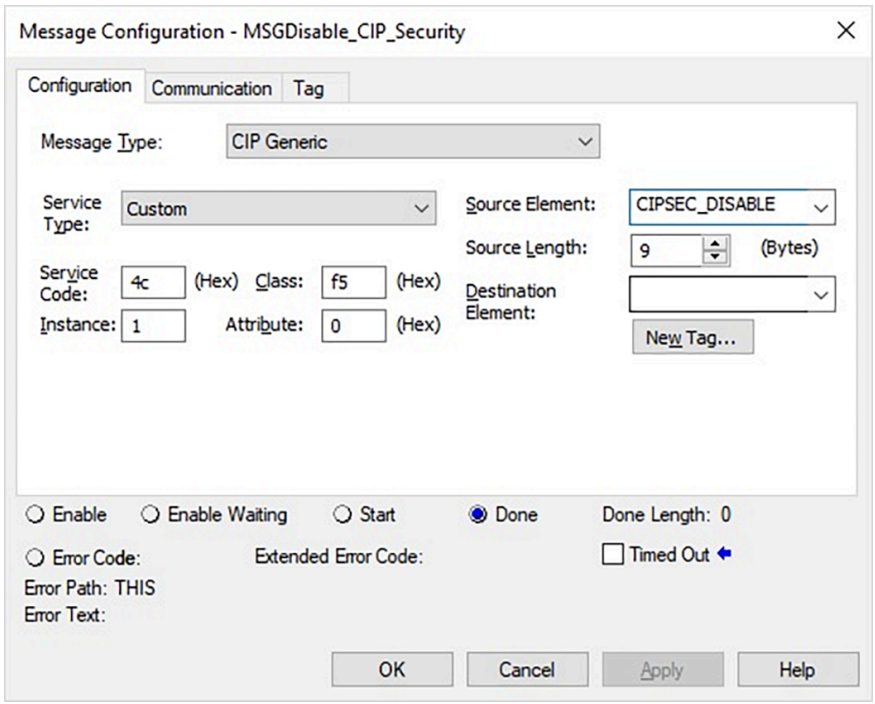
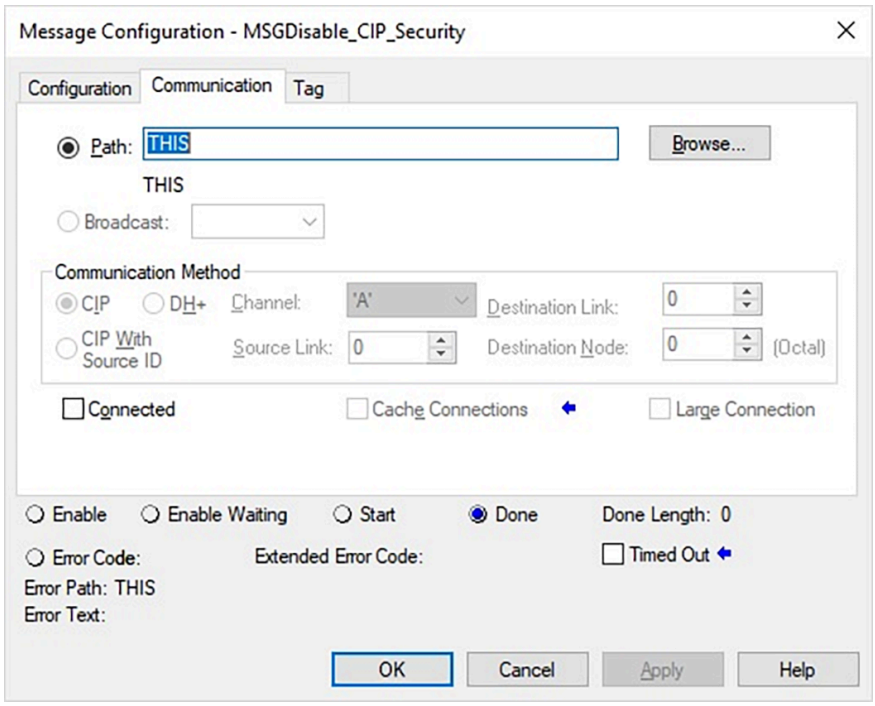


Table 42. Disable the CIP Security Port

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1
Class	f5
Attribute	0
Source Element	Controller tag of SINT[9] data type. This is the controller tag that you created previously.
Source Length	9

4. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



5. Cycle power on the controller for the configuration to take effect.

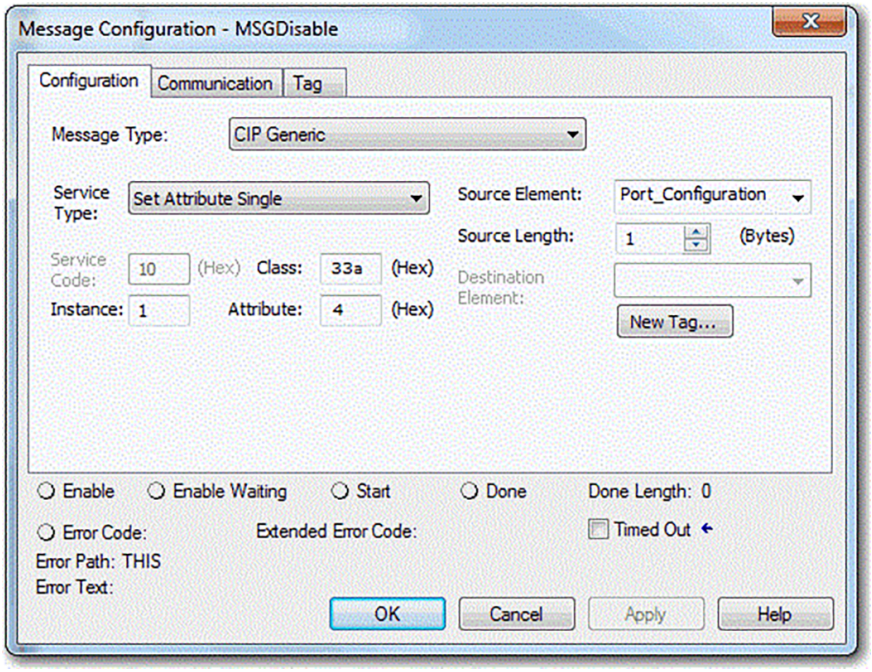
Disable the Controller USB Port

With the Studio 5000 Logix Designer® application, version 32 or later, you can use a CIP™ Generic MSG with a Path of THIS to execute this option.

1. Add an MSG instruction to your program.
   This message only has to execute once, it does not need to execute with every program scan.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.



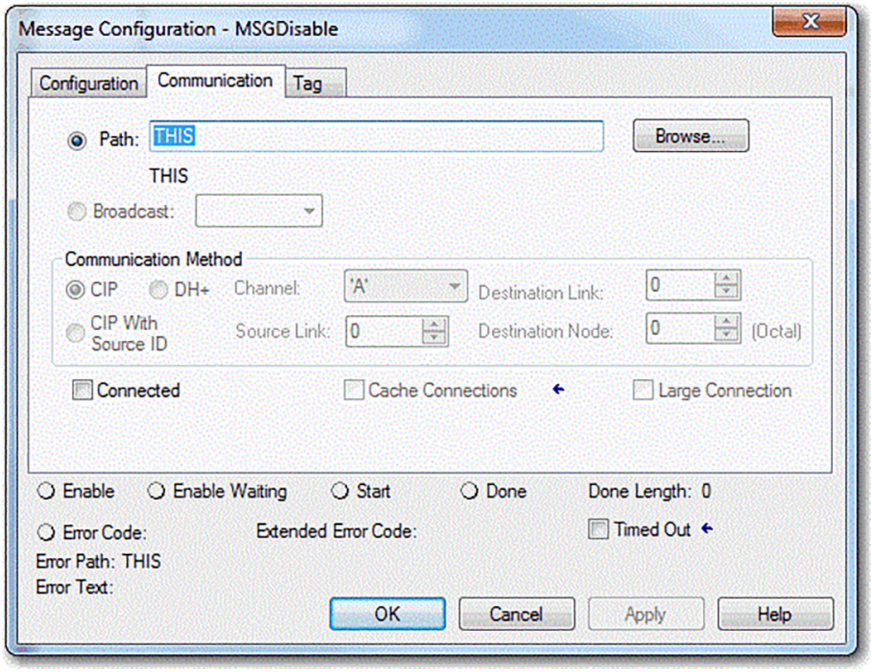
IMPORTANT: These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute up each time the controller powers up.

Table 43. Disable the USB Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	33a
Attribute	4
Source Element	Controller tag of SINT data type. In this example, the Source Element is named Port_Configuration.
Source Length	1

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



Disable the Controller Memory Card

With the Studio 5000 Logix Designer® application, version 32 or later, you can use a CIP™ Generic MSG with a Path of THIS to execute this option.

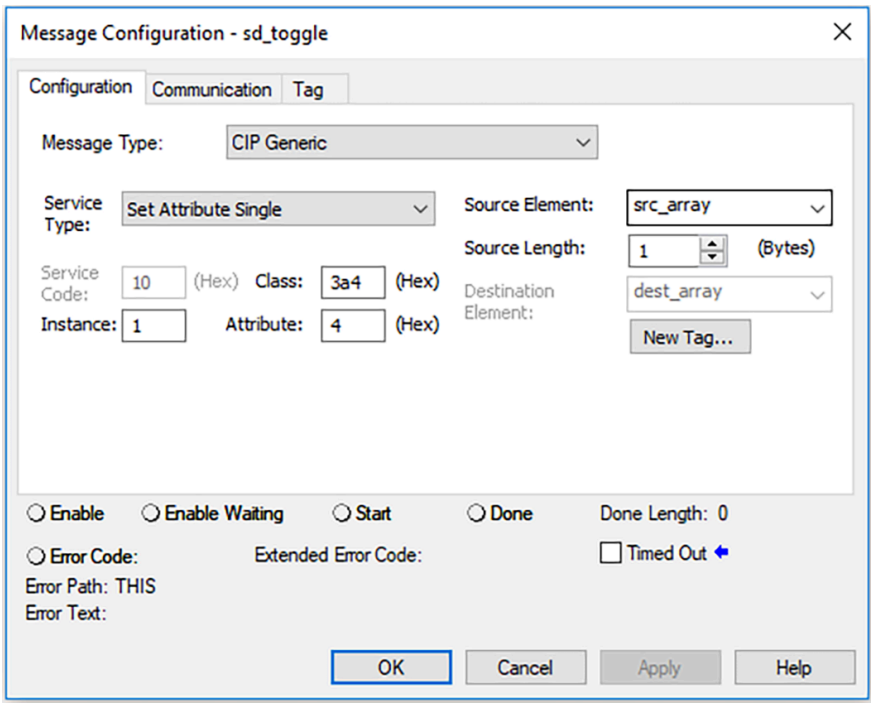
IMPORTANT: Remember the following:

- A memory card can only be disabled with a Message to Self.
- Once a memory card slot is disabled, you lose all ability to communicate to a memory card inserted into the slot. This includes any diagnostic information.

1. Add an MSG instruction to your program. This message only has to execute once, it does not need to execute with every program scan.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.



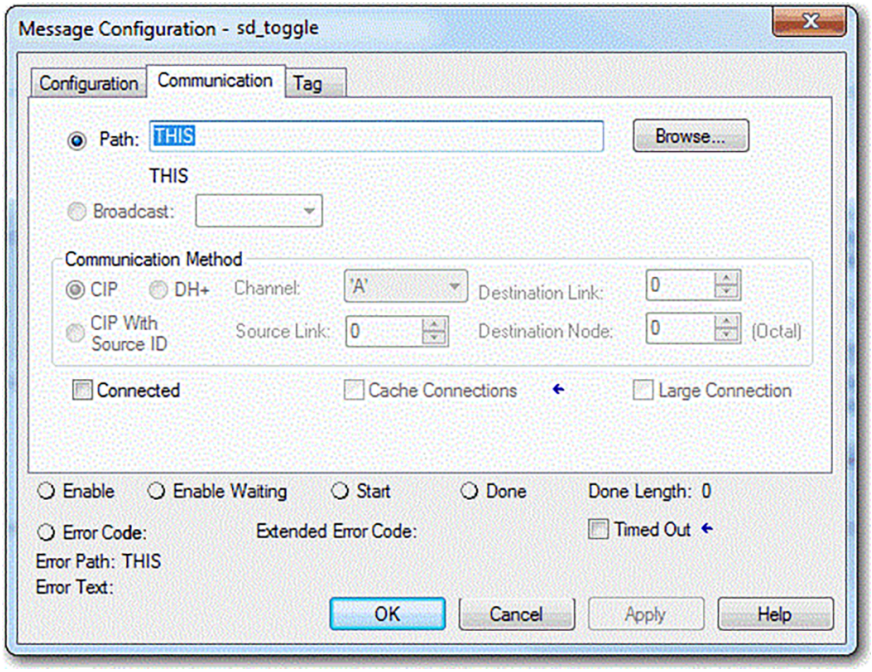
IMPORTANT: These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

Table 44. Disable the Memory Card

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a4
Attribute	4
Source Element	Controller tag of SINT Array. Source Element Tag Data: - 0 = Enable memory card - 1 = Disable memory card In this example, the Source Element is named src_array.
Source Length	1

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Message to THIS must be unconnected messages.



4. Before you enable the MSG instruction, make sure that the Source Element tag value is 1.

IMPORTANT: You can re-enable the memory card after it's been disabled.

To re-enable the memory card, complete the steps that are described in this section. Before you enable the MSG instruction, be sure that the appropriate bit in the Source Element tag value is 0.

Controller 4-character Status Display

With the Studio 5000 Logix Designer® application, version 29 or later, you can disable certain categories of messages on the four-character status display.

You use a CIP Generic MSG to execute each option.

IMPORTANT: You cannot disable these system messages, and they always display:

- Power-up messages, such as TEST, PASS, CHRG
- Catalog number message
- Firmware revision message
- Major / Critical failure messages

The 4-character status display returns to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset
- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - these examples can clear the program from a controller:
  - Major nonrecoverable fault occurs.
  - Firmware update occurs.

You must reconfigure the settings to disable the 4-character status display after it returns to its default settings.

Disable All Categories of Messages

You can disable a subset of the information that scrolls across the controller 4-character display. You can disable these subsets:

- Project name
- Link status
- Port status and
- IP address

Complete these steps.

1. Add an MSG instruction to your program.
   This message only has to execute once, it does not need to execute with every program scan.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.

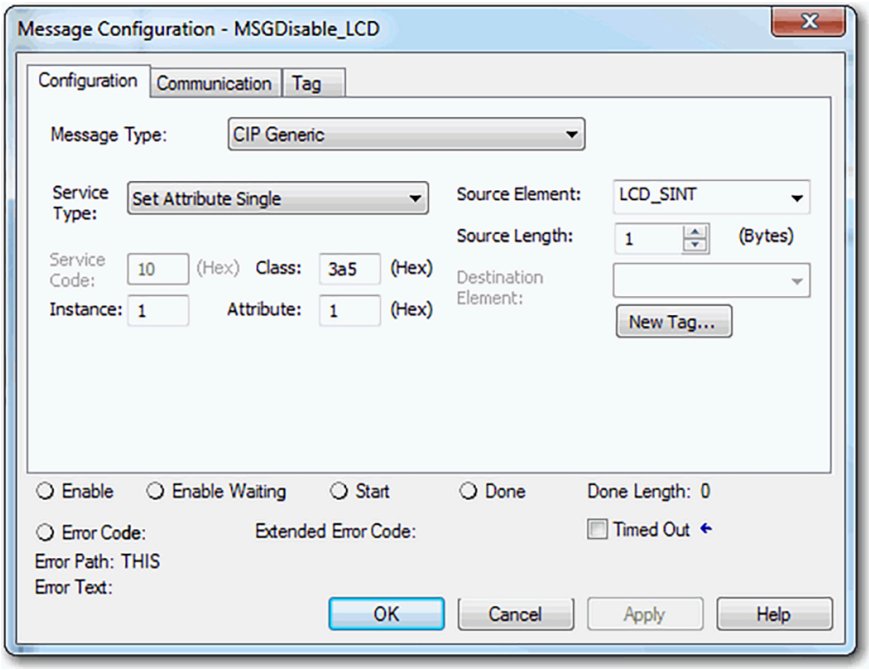


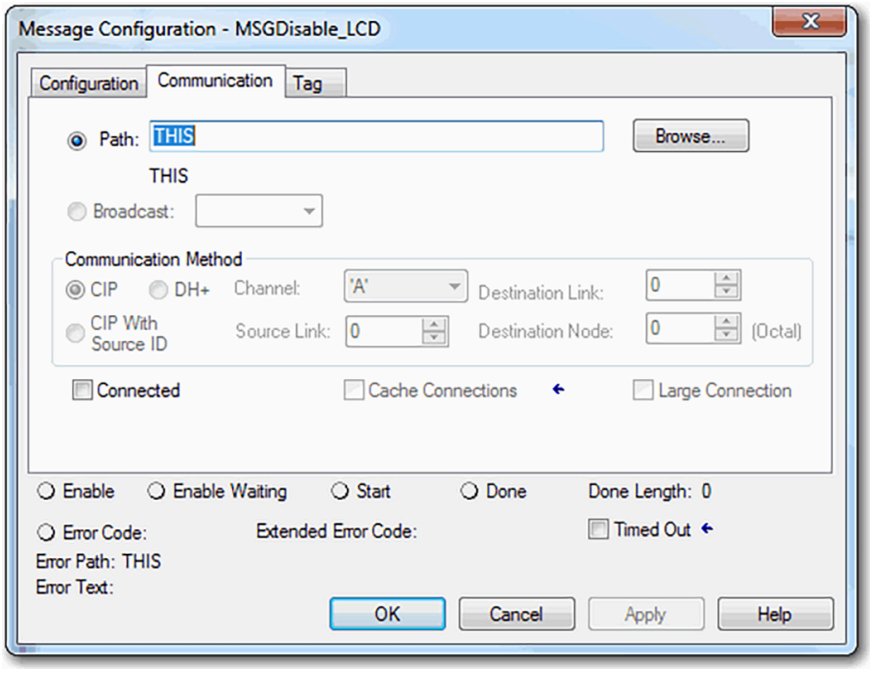
Table 45. Disable All Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1

Field	Description
Class	3a5
Attribute	1
Source Element	Controller tag of SINT data type. Source Element Tag Data: - 0 = Enable LCD Subset - 1 = Disable LCD Subset In this example, the controller tag is named LCD_SINT. To disable the subset of the information that scrolls across the controller 4-character display that are described in this section, the Source Element tag value must = 1.
Source Length	1

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, make sure that the Source Element tag value is 1.

IMPORTANT: You can re-enable the subsets of information on the 4-character display after they are disabled.

To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, be sure that the appropriate bit in the Source Element tag value is 0.

Disable Individual Categories of Messages

You can disable a subset of the information that scrolls across the controller 4-character display. You can disable these subsets:

- Project name and link status
- Port status and IP address

Complete these steps.

1. Add an MSG instruction to your program. This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT: You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration table on the Message Configuration dialog box as described in the table below.

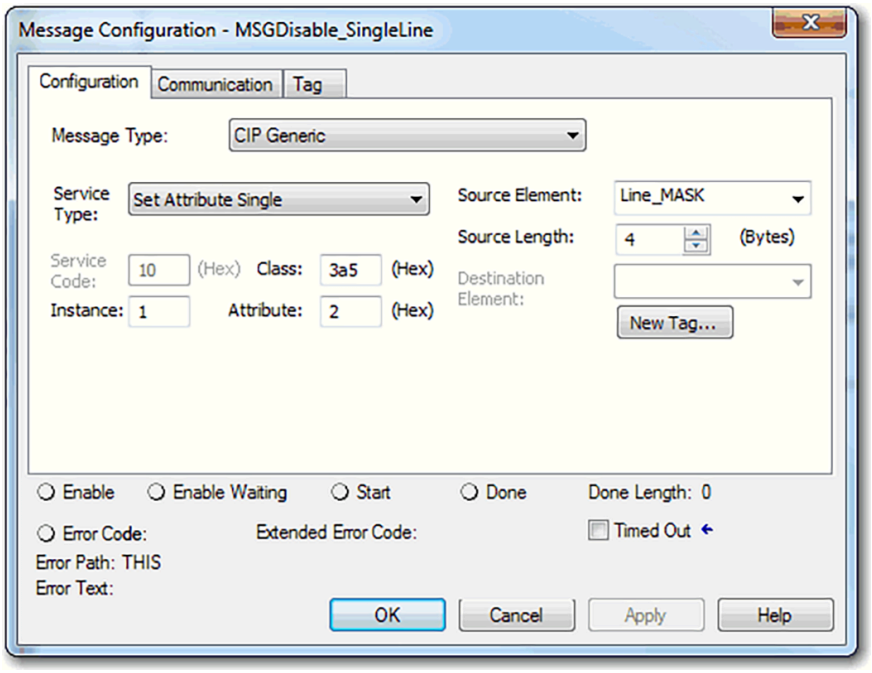


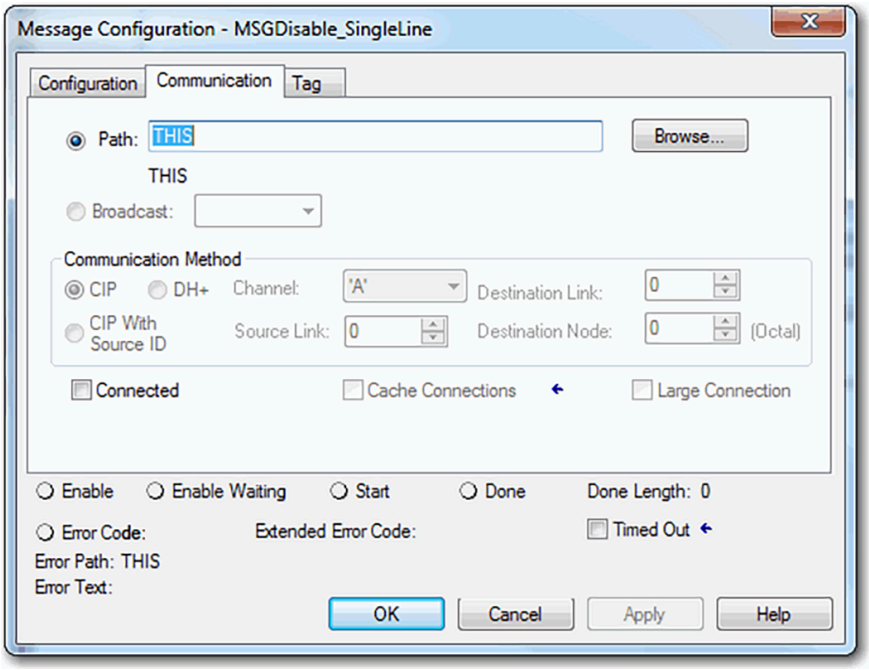
Table 46. Disable Individual Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a5
Attribute	2
Source Element	Controller tag of DINT data type.

Field	Description
	Source Element Tag Data: - Enable Project name and link status - Bit 0 of the Source Element = 0 - Enable Port status and IP address - Bit 1 of the Source Element = 0 - Disable Project name and link status - Bit 0 of the Source Element = 1 - Disable Port status and IP address - Bit 1 of the Source Element = 1 In this example, the controller tag is named Line_MASK.
Source Length	4

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, make sure that the Source Element uses one of the following tag values that are based on what information that you want to disable:
   - Project name and link status - Bit 0 of the Source Element = 1
   - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT: You can re-enable the subsets of information on the 4-character display after they are disabled.

To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, be sure that the appropriate bit in the Source Element tag value is 0.

Controller Webpage Default Settings

The following are the default settings for controller webpages:

- Webpages are enabled for controller firmware revision 32 or earlier. You must reconfigure the settings to disable the controller webpages after it returns to its default settings.
- Webpages are disabled for controller firmware revision 33 or later. You must reconfigure the settings to enable the controller webpages after it returns to its default settings.

Controller webpages return to the default setting in these situations:

- A stage 1 reset for all versions of the Studio 5000 Logix Designer® application.
- A stage 2 reset for all versions of the Studio 5000 Logix Designer® application.

IMPORTANT: When you update the controller firmware to revision 33 or later without a reset, the controller retains the previous controller webpage configuration (webpages enabled) and does not automatically change to the default setting for version 33 (disable the webpages).

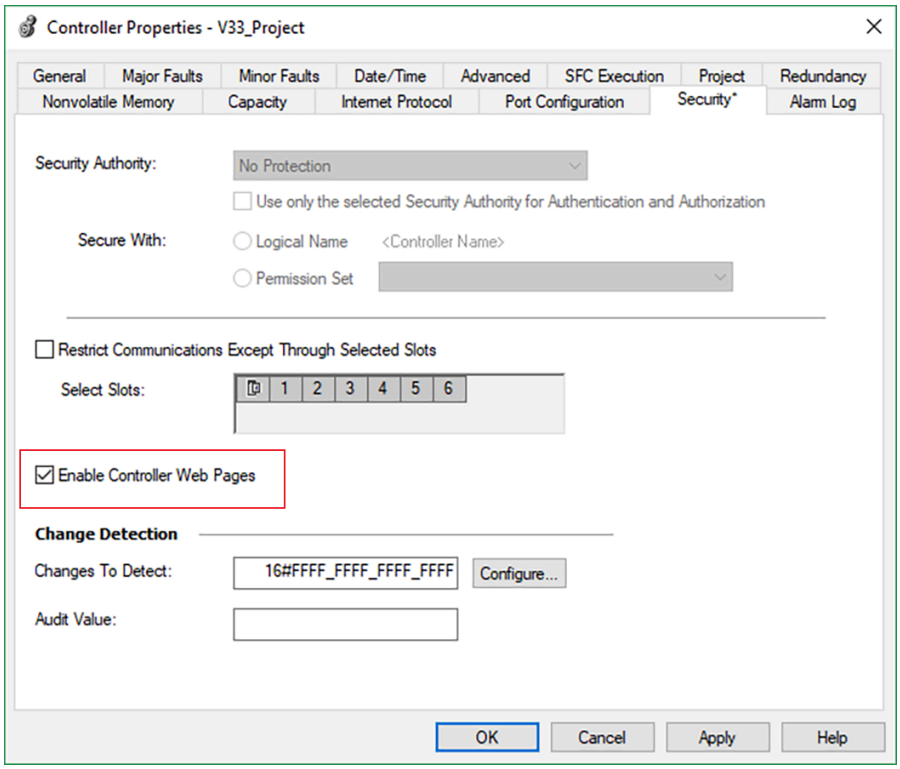
The setting of the controller webpages changes after the following occurs on the controller:

- New project is downloaded - in this case, the settings in the new project take effect.
- When the controller receives a configuration message, it takes the setting from the configuration message.

Disable Controller Webpages via Controller Properties

You can use one of the following methods to disable the controller webpages:

- If the controller web pages are enabled, disable them by clearing the Enable Controller Web Pages check box on the Security tab for the controller properties.



IMPORTANT: In version 36 or later, the status of the Enable Controller Web Pages checkbox is saved to and restored from the memory card when using the save/restore feature.

Previous versions maintain the status of the Enable Controller Web Pages checkbox that was applied to the controller prior to a restore from the memory card.

- For CIP Security™ applications, you can also use FactoryTalk® Policy Manager to disable the webpages (this overrides the Controller Properties checkbox).

Use a CIP Generic MSG to Disable the Controller Webpages

IMPORTANT: If you use FactoryTalk® Policy Manager to disable the webpages in a CIP Security™ application, the CIP™ generic message-to-self overrides the FactoryTalk® Policy Manager setting.

1. Add an MSG instruction to your program.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration table on the Message Configuration dialog box as described in the table below.

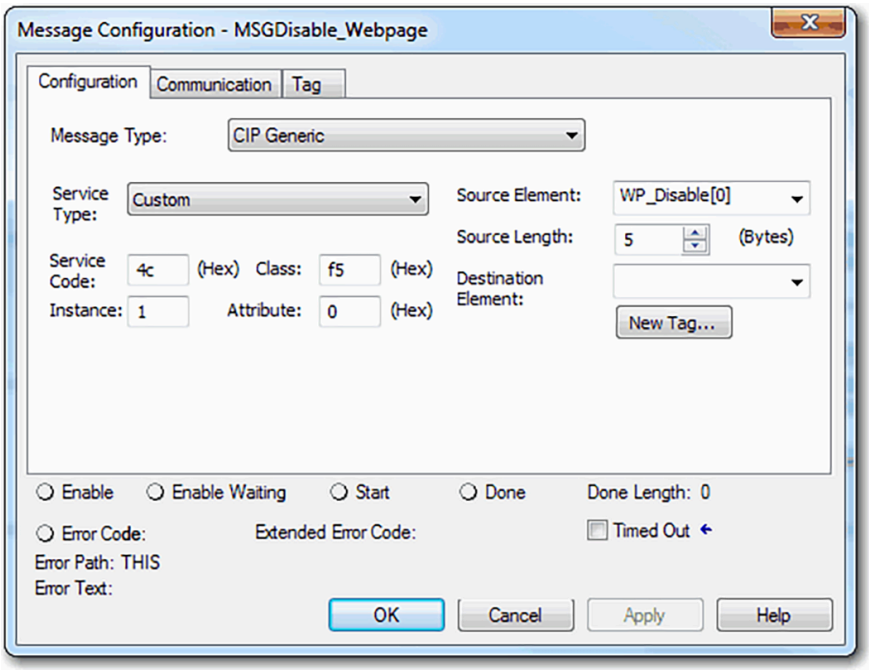
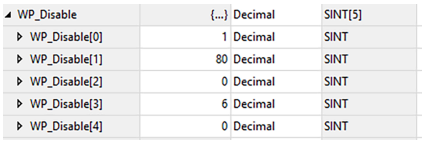


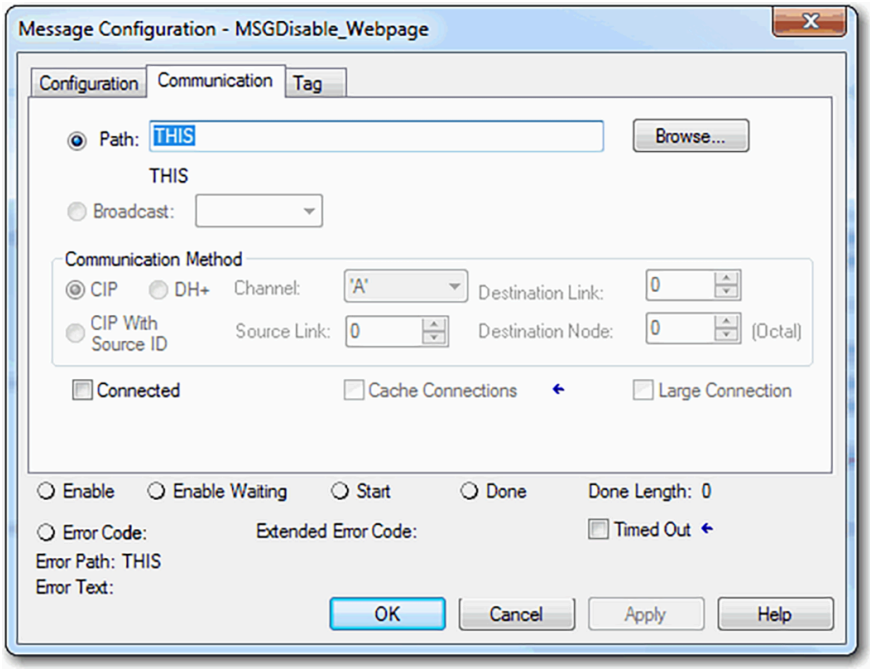
Table 47. Disable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom

Field	Description
Service Code	4c
Instance	1
Class	f5
Attribute	0
Source Element	Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Disable and must match the following graphic.  **IMPORTANT**: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not disabled.
Source Length	5

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



Use a CIP Generic MSG to Enable the Controller Webpages

1. Add an MSG instruction to your program.

   IMPORTANT: You cannot add an MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk® Security settings deny this editing option.

2. Configure the Configuration table on the Message Configuration dialog box as described in the table below.

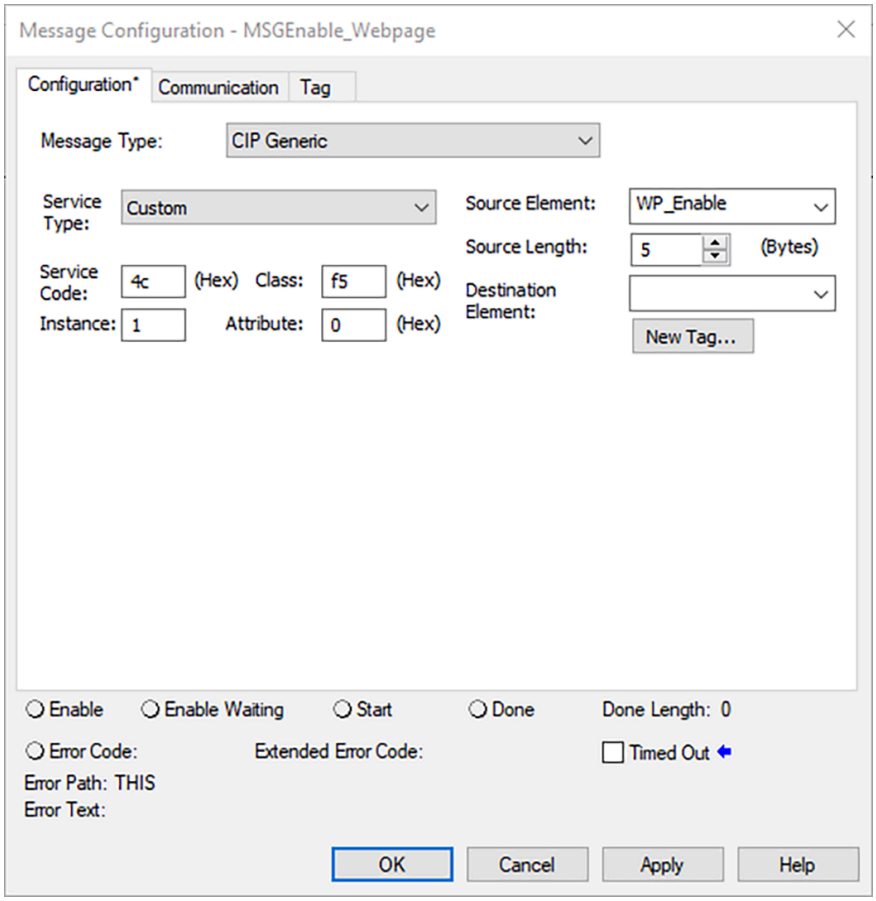
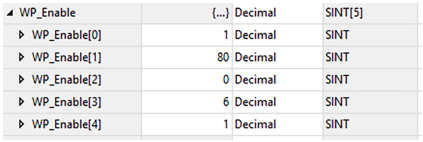


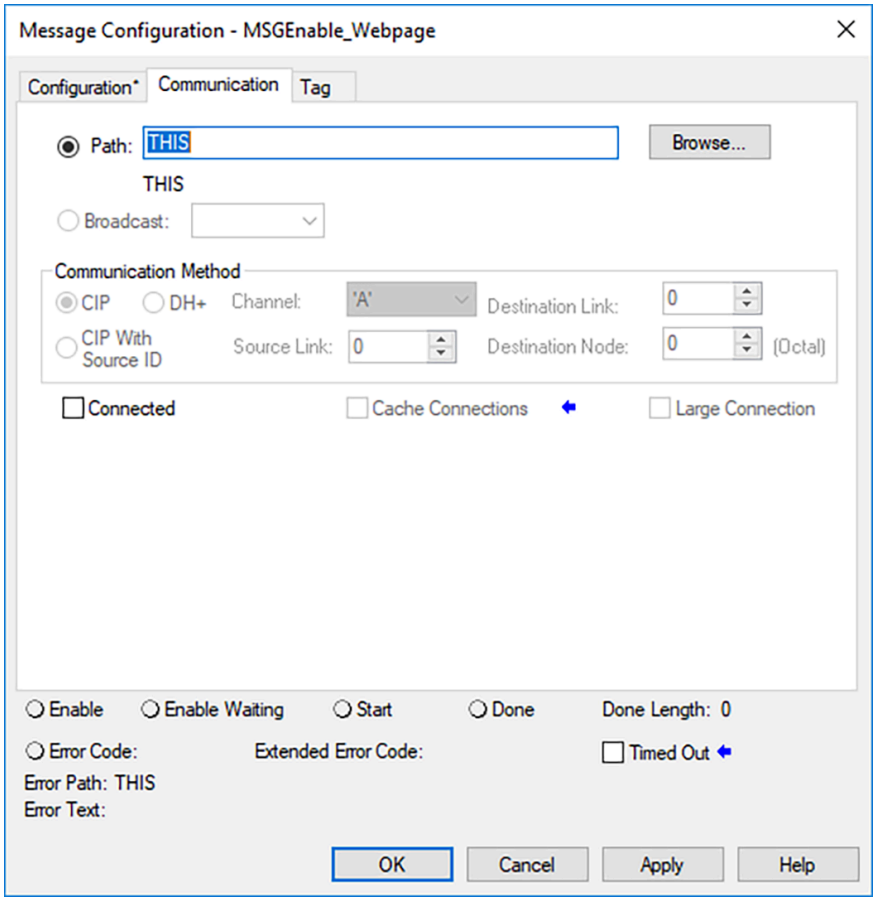
Table 48. Enable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1
Class	f5
Attribute	0
Source Element	Controller tag of SINT[5] data type.

Field	Description
	In this example, the controller tag is named WP_Enable and must match the following graphic.  **IMPORTANT**: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not enabled.
Source Length	5

3. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.



Trusted Slots on the Controller

Trusted slots help maintain network segmentation when a controller front Ethernet port is disabled, such as in redundant control systems. Trusted slots restrict communication paths through which certain operations are performed on the controller.

IMPORTANT: Trusted slots and CIP Security™ are not compatible on the same device. If both features are used on the same device, programming through the controller front Ethernet port is disabled and you are locked out of programming the controller until you perform a physical reset.

To meet IEC-62443-4-2 SL 1 certification requirements, you must not configure Trusted slots on the controller and instead use CIP Bridging Control on page 156.

Trusted slots help maintain network segmentation when the controller front Ethernet port is disabled, such as in redundant control systems. Trusted slots restrict communication paths through which certain operations are performed on the controller.

The following rules apply to Trusted slots:

- The firmware revisions of the physical modules in the Trusted slots must be compatible with the firmware revisions and electronic keying options that are configured in the I/O tree of the project. For compatibility, see Electronic Keying on page 100.
- All communication is Trusted from the module as long as there is not a fault or keying mismatch.
- If no module is configured in the I/O tree for the respective Trusted slot, then all communication is Trusted regardless of which module is physically present.

You configure Trusted slots with the parameters on the Security tab of the Controller Properties dialog box.

Restrict Communication Except Through Selected Slots

Select this checkbox to restrict communication through any slot in the chassis that is not Trusted. Clear the checkbox to allow the controller to communicate without communication restrictions.

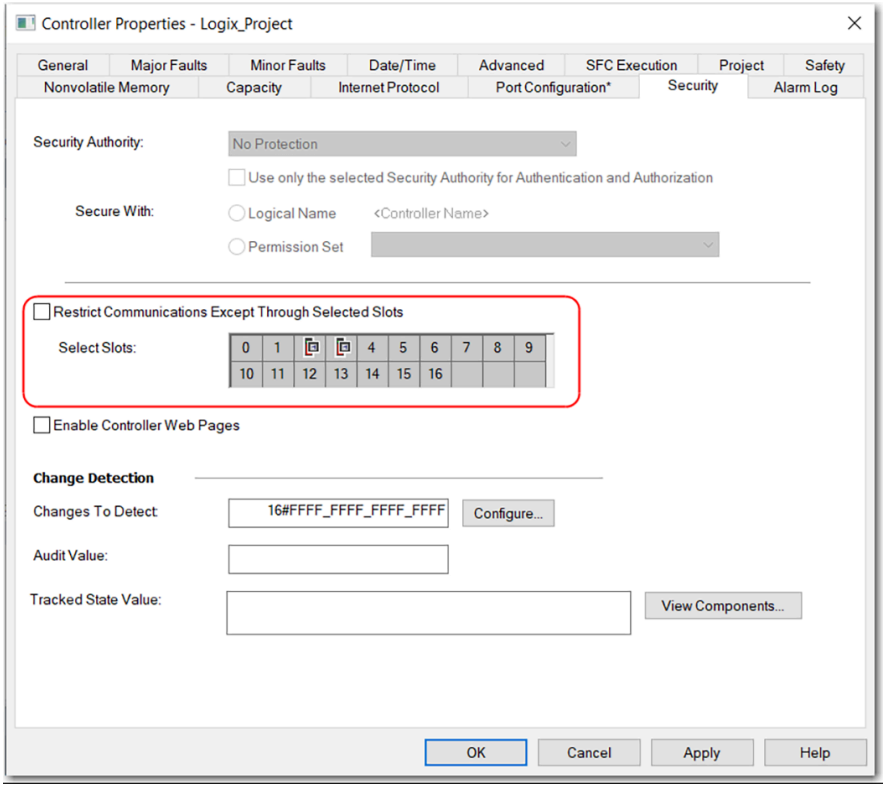
IMPORTANT: When this checkbox is selected, communication is restricted through the front Ethernet port and firmware updates are restricted to Trusted slots when using AutoFlash, or ControlFLASH Plus® software. Support is restricted for tools that require access to restricted data through Class 3 connections.

Select Slots

Only the slots that are selected under Select Slots are Trusted communication paths for the controller. The Select Slots grid configures the trusted slots for the controller. When you select the Restrict Communications Except Through Selected Slots checkbox, you must click at least one slot that is not occupied by the controller.

If the chassis size for the project is known, the number of slots equal to the chassis size appear on the dialog box. Otherwise, 17 slots (0...16) appear on the dialog box.

Figure 52. Selected Slot Options



Privacy Aspects

If configured to do so, the controller can collect the following personal data for the purpose of logging user activity:

- User name (full name and domain name)
- Workstation name
- FactoryTalk® ID

No more personal data is collected than needed and no personal data is logged by default.

IMPORTANT: The general purpose programming capabilities of the controller allow you to program the controller to collect personal data through connection to other devices and systems for any purpose. You are responsible for protecting personal data collected as a result of your applications.

Data Protection

The following provides methods to protect personal data stored by the controller through restricted access:

- CIP Security™ — To implement CIP Security™, see the CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001.
- FactoryTalk® Security — To configure FactoryTalk® Security permissions, see the Configure System Security Features User Manual, SECURE-UM001.

Data Removal

Personal data can be stored by the controller in these locations:

- Internal memory of the controller. The circular buffer of the controller only keeps a limited amount of data within the controller.
- External memory card, only if logging is configured to write to a text file on the card

IMPORTANT: Data that has been retrieved by external software is the responsibility of the respective software.

You can remove personal data by using these methods:

- Perform a factory reset on the controller to delete data from internal memory.
- Access the text file on the memory card and delete personal data.

IMPORTANT: The controller does not have secure reset functionality to make deleted data nonrecoverable. To address critical security concerns about data recovery, we recommend physically destroying a device when decommissioned.

Develop Motion Applications

The controllers support Integrated Motion on an EtherNet/IP™ network and digital drives interfaces that include connected drives. The controllers support any combination of CIP™, Virtual, and Consumed axes. You can add all axes to one Motion Group, and you can assign any combination of axes to different axis update schedules.

Table 49. Supported Axes and Drives

Controller	Total Number of Supported Axes	Support Drive Types
ControlLogix® 5580 GuardLogix® 5580	256	• Integrated Motion on an EtherNet/IP™ network drives • EtherNet/IP™ connected drives • Sercos interface connected drives. • Analog drives support ±10V analog output and can interface with various feedback devices, such as quadrature encoder, SSI, and LVDT feedback.

Rockwell Automation® recommends using the built-in EtherNet/IP port for high-performance motion applications.

For more information, see these publications:

- Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003.
- Integrated Motion on the EtherNet/IP Network Reference Manual, publication MOTION-RM003.
- SERCOS and Analog Motion Configuration and Startup User Manual, publication MOTION-UM001.

You can associate Integrated Motion axes to any appropriate drive, regardless of whether the communications path to the drive is via the embedded Ethernet port, or over the 1756 backplane via an Ethernet bridge, such as a 1756-EN2T.

The configuration process varies, depending on your application and drive selection. The following are general steps to configure a motion application.

1. Create a controller project.
2. Select the type of drive.
3. Create axis tags as needed.
4. Configure the drive.
5. Create axes as needed.

Program Motion Control

The controller provides a set of motion control instructions for your axes:

- The controller uses these instructions just like the rest of the Logix 5000® instructions.
- Each motion instruction works on one or more axes.

- You can program by using motion control instructions in these programming languages:
  - Ladder Diagram (LD)
  - Structured Text (ST)
  - Sequential Function Chart (SFC)
- Each motion instruction needs a motion control tag. The tag uses a MOTION_INSTRUCTION data type and stores the information status of the instruction.

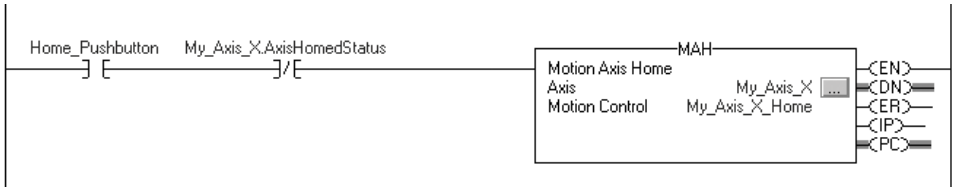
For more information, see the Logix 5000 Controller Motion Instructions Reference Manual, publication MOTION-RM002.

ATTENTION: Use each motion control tag in only one motion instruction. Unintended operation can result if you reuse the same motion control tag in other motion instructions, or if you write to any of the motion control tag elements.

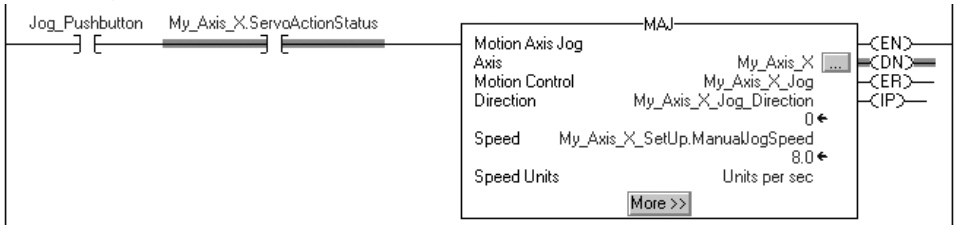
In this example, a simple ladder diagram that homes, jogs, and moves an axis.

If Initialize_Pushbutton = on and the axis = off (My_Axis_X.ServoActionStatus = off) then the MSO instruction turns on the axis.

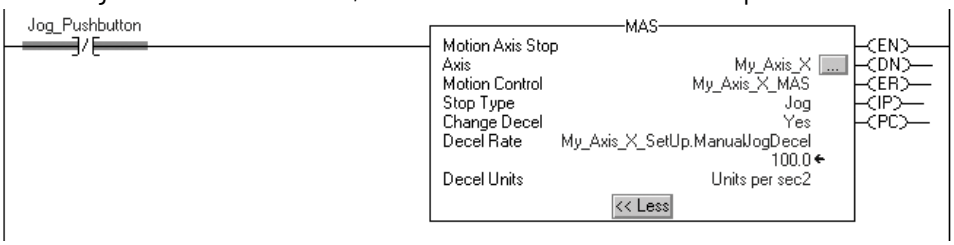
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off) then the MAH instruction homes the axis.



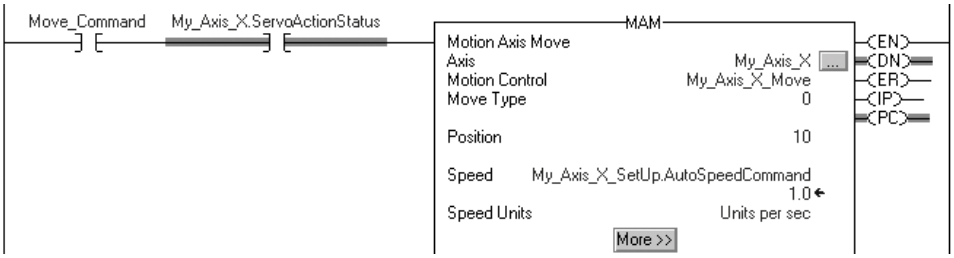
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAJ instruction jogs the axis forward at 8 units/second.



If Jog_Pushbutton = off then the MAS instruction stops the axis at 100 units/second^2. Make sure that Change Decel is Yes. Otherwise, the axis decelerates at its maximum speed.



If Move_Command = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAM instruction moves the axis. The axis moves to the position of 10 units at 1 unit/second.

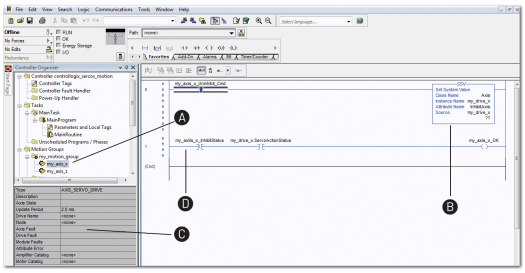


Obtain Axis Information

You can obtain axis information by using these methods:

- Double-click the axis (A) to open the Axis Properties dialog box.
- Use a Get System Value (GSV) or Set System Value (SSV) instruction (B) to read or change the configuration at runtime.
- View the QuickView pane (C) to see the state and faults of an axis.
- Use an axis tag for status and faults (D).

Figure 53. Obtain Axis Information



Troubleshoot the Controller

There are many options available to troubleshoot the controller if issues occur during normal operation.

You can use the Studio 5000 Logix Designer® application to view fault conditions in these ways:

- Module status in the I/O Configuration Tree
- Categories on I/O Module Properties Dialog
- Notification in the Tag Monitor
- Fault Information in the Controller Properties Dialog
- Ethernet Port Diagnostics
- Advanced Time Sync dialog

You can also use:

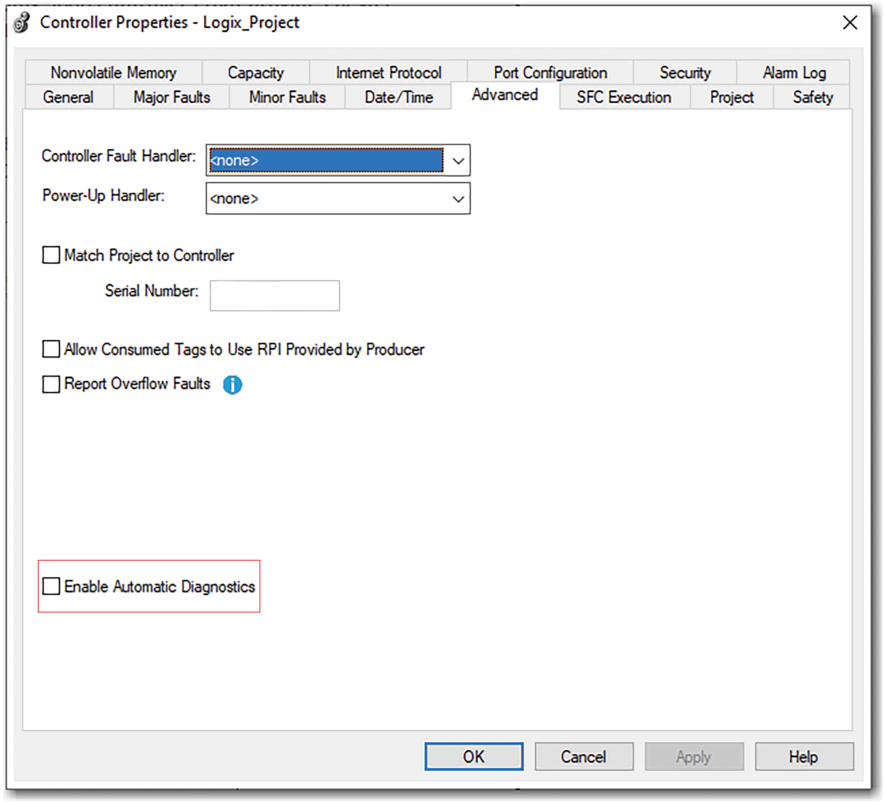
- Diagnostic information in Linx-based software
- Controller Webpages

Automatic Diagnostics

Automatic Diagnostics is a system-level feature in Logix 5000® controllers that provides device diagnostics to HMIs and other clients, with zero programming. The diagnostics include device description conditions and state events.

Automatic Diagnostics is enabled by default in controllers with firmware revision 33 or later. You can disable and enable the whole feature while online or offline from the Advanced tab on the Controller Properties dialog box. You can also disable Automatic Diagnostics for a specific device in the device's configuration.

Figure 54. Controller Properties Advanced Tab



Considerations for Communication Loss Diagnostics

The response time and diagnostic information for a loss of communication depends on the device and configuration settings.

Table 50. Connection and Device Behavior

Type of Connection	Device Behavior
Direct connection to a controller	The device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter.
No connection to a controller	Communication adapters that do not have a connection to the controller do not report communication loss diagnostics. We recommend that you configure your communications adapters for a status connection to make sure that they report any communication loss diagnostic in a timely manner.
Data connection	The device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter.
Rack-optimized connection	The device does not report communication loss diagnostics. The communication adapter reports communication loss diagnostics. A device with a rack-optimized connection has a reduced set of diagnostics as compared to a direct connection.

When enabled, the Automatic Diagnostics feature enables the following:

- Communication loss diagnostics for all devices in the controller I/O configuration.
- Device-level automatic diagnostics evaluations for all uninhibited and enabled devices.

You can disable Automatic Diagnostics for a specific device in the device configuration. The communication loss diagnostic remains active even if the device disables Automatic Diagnostics. To disable communication loss diagnostic, inhibit the device or disable Automatic Diagnostics at the controller.

Controller Diagnostics with the Logix Designer Application

A warning symbol appears in the controller organizer next to the I/O module under these conditions:

- If there are faults or other conditions in the I/O module
- If the connection to the I/O module fails while in run mode

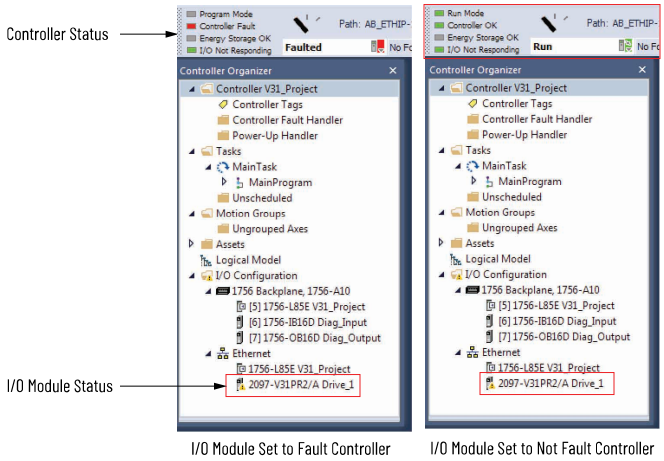
When the I/O module is configured to cause a major fault on the controller and an I/O module fault occurs, the following can result:

- Controller state displays Faulted.
- Controller status displays Controller Fault and is steady red.
- I/O module status displays I/O Not Responding and blinks green.

When the I/O module is not configured to cause a major fault on the controller and an I/O module fault occurs, the following result:

- Controller state displays the current state, for example, Rem Run.
- Controller status displays Controller OK and is steady green.
- I/O module status displays I/O Not Responding and blinks green.

Figure 55. I/O Fault on the Controller



I/O Module Set to Fault Controller I/O Module Set to Not Fault Controller

IMPORTANT: Safety Consideration

You cannot configure safety connections to automatically fault the controller

I/O Module Properties

The Module Properties dialog box for an I/O device shows fault information, such as:

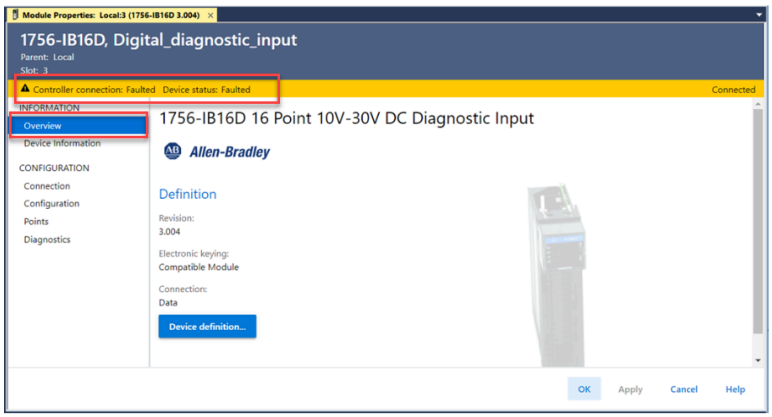
- Module state
- Fault description
- Major and minor fault descriptions

- Module's internal state
- Diagnostics information

Module Status on General Category

The General category shows a Faulted status.

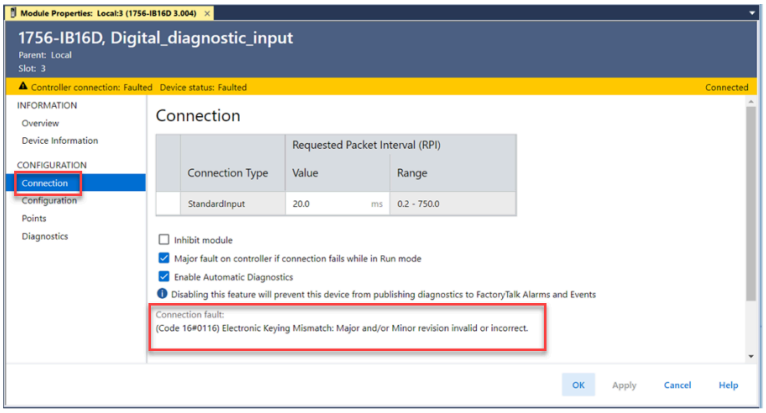
Figure 56. I/O Fault Status on Overview Category



Module Fault Description on Connection Category

The Connection category displays the module fault description that includes an error code that is associated with the specific fault type.

Figure 57. I/O fault on Connection Category



Module Fault Descriptions on Module Info Category

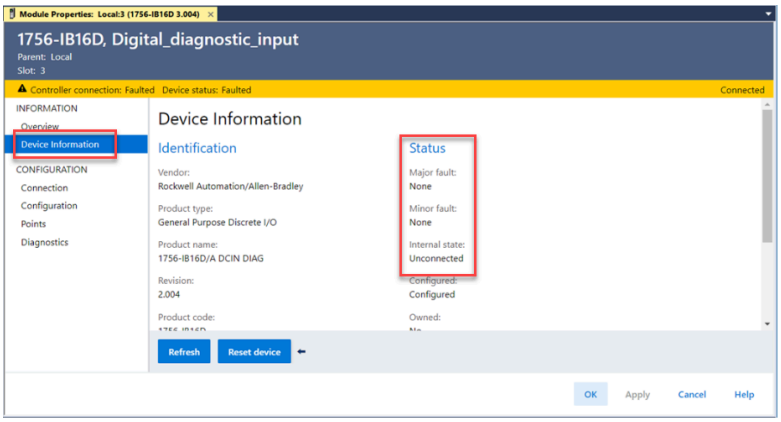
The Module Info view requires successful communication.

- If communication to the I/O module is OK, but the module itself is faulted, then the Module Info tab helps to troubleshoot the fault.
- If there is a communication fault, then the Connection Tab is more useful.

On the Module Info category, the Status section displays the following about the I/O module:

- Major and Minor Faults
- Internal State

Figure 58. I/O Fault on Device Information View



Notification in the Tag Monitor

General module faults are also reported in the Tag Monitor. Diagnostic faults are reported only in the Tag Monitor. When the Value field is set to 1, a fault is present.

Figure 59. I/O Module Fault

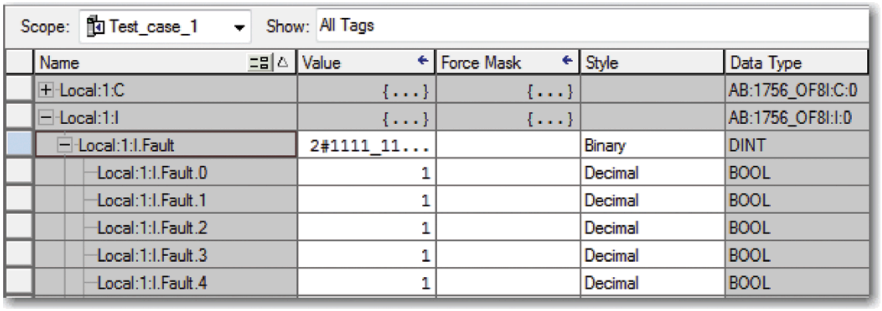
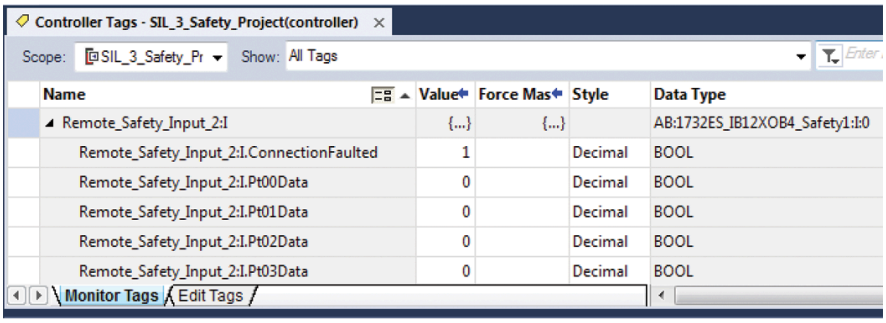


Figure 60. Safety I/O Connection Fault

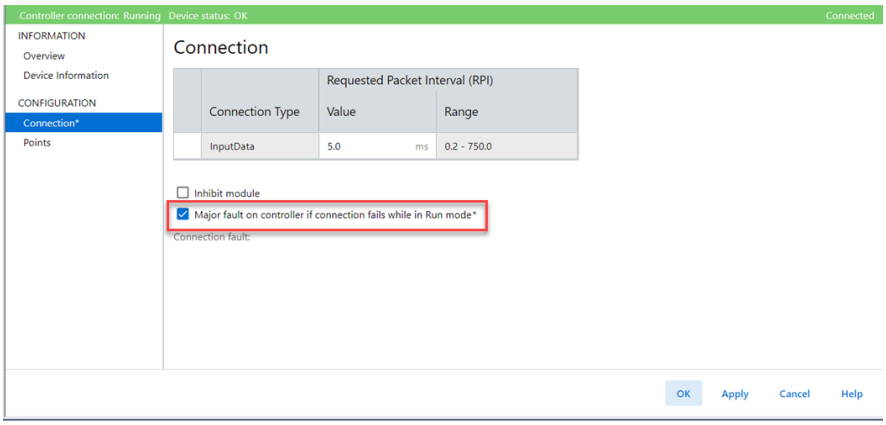


Enable Major Fault on Controller

To display recent I/O fault information on the Major Faults tab of the controller properties, you must first select Major Fault on Controller if Connection Fails While in Run Mode on the Connection view of the I/O Properties dialog box.

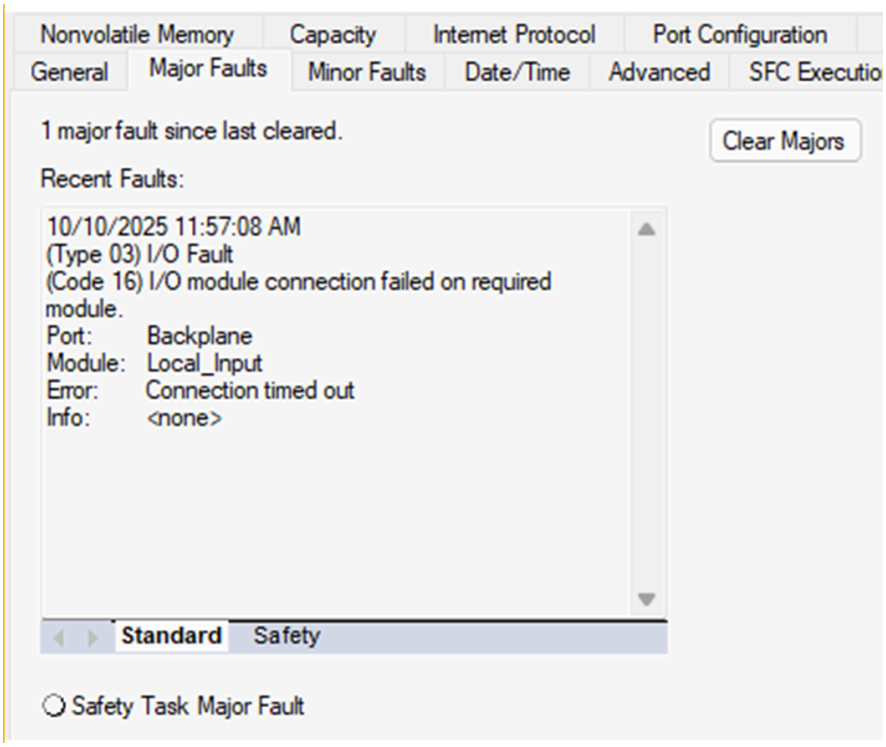
WARNING: If you select this option, a connection fault on the I/O module can cause a major fault on the controller. A major fault on the controller causes the outputs to go to their configured fault state.

Figure 61. Enable Major Fault on Controller



When you are monitoring the configuration properties of a module in the Studio 5000 Logix Designer® application and receive a communication fault message, the Major Faults tab for the controller properties indicates the type of fault under Recent Faults.

Figure 62. Major Faults Tab in Controller Properties



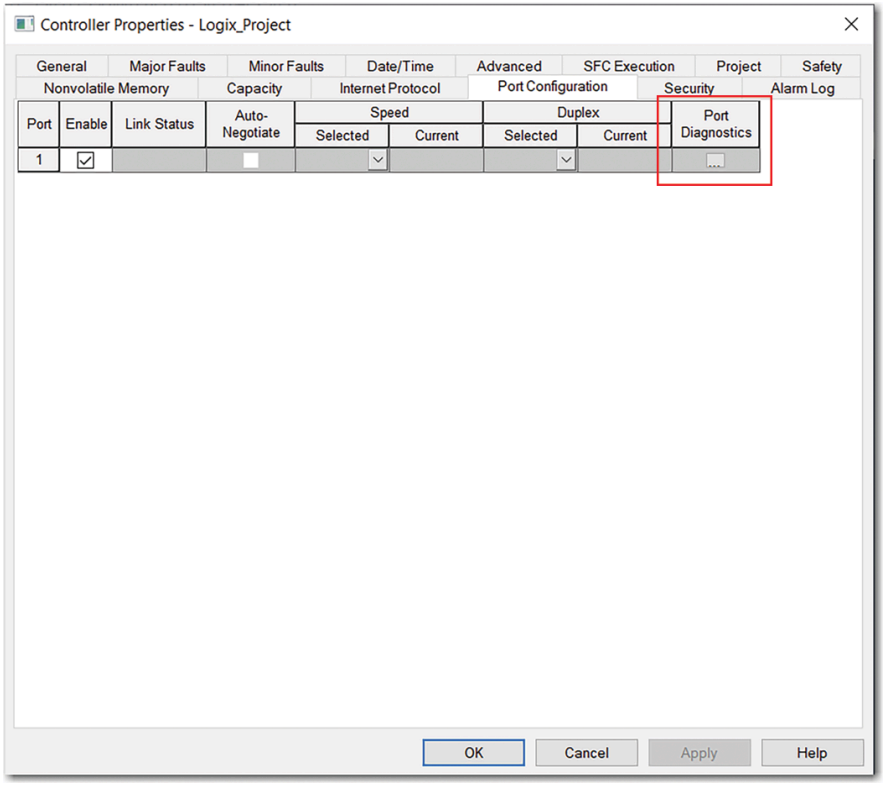
You can use the Minor Faults and Networks tabs to check for minor faults and network fault, respectively.

Port Diagnostics

When your project is online, you can view the status of the embedded Ethernet port on the controller.

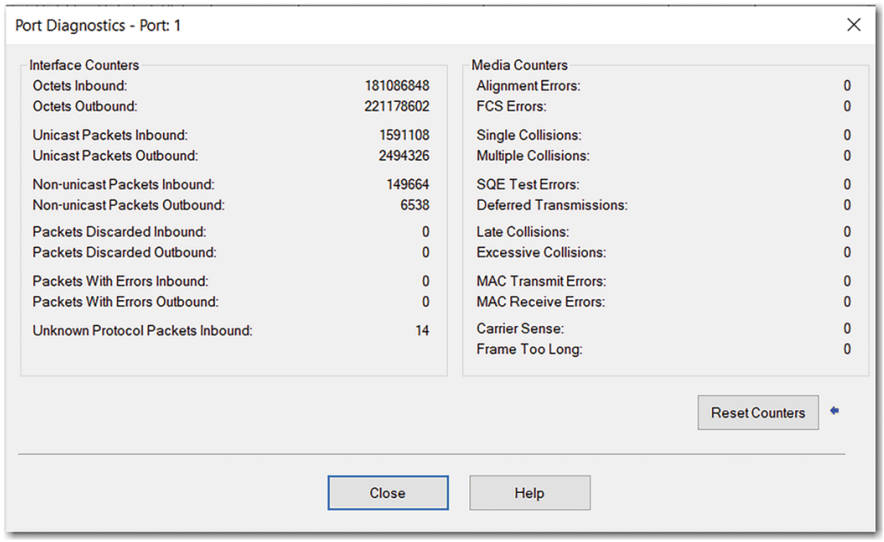
1. Access the Controller Properties.
2. On the Controller Properties dialog box, click the Port Configuration tab.
3. Click the Ellipse button in the Port Diagnostics column.

Figure 63. Ethernet Port Diagnostics



The Port Diagnostics dialog box displays diagnostic details.

Figure 64. Port Diagnostics Details



Parameters	Description
Interface Counters	The Interface Counters values have no value when you are offline or online and there is a communication error.
Octets Inbound	Displays the number of octets that are received on the interface.
Octets Outbound	Displays the number of octets that are transmitted to the interface.
Unicast Packets Inbound	Displays the number of unicast packets that are received on the interface.
Unicast Packets Outbound	Displays the number of unicast packets that are transmitted on the interface.
Non-unicast Packets Inbound	Displays the number of non-unicast packets that are received on the interface.
Non-unicast Packets Outbound	Displays the number of non-unicast packets that are transmitted on the interface.
Packets Discarded Inbound	Displays the number of inbound packets that are received on the interface but discarded.
Packets Discarded Outbound	Displays the number of outbound packets that are transmitted on the interface but discarded.
Packets With Errors Inbound	Displays the number of inbound packets that contain errors (excludes discarded inbound packets).
Packets With Errors Outbound	Displays the number of outbound packets that contain errors (excludes discarded outbound packets).
Unknown Protocol Packets Inbound	Displays the number of inbound packets with unknown protocol.
Media Counters	The Media Counters values have no value when you are offline or online and there is a communication error.
Alignment Errors	Displays the number of frames received that are not an integral number of octets in length.
FCS Errors	Displays the number of frames received that do not pass the FCS check.
Single Collisions	Displays the number of successfully transmitted frames that experienced exactly one collision.
Multiple Collisions	Displays the number of successfully transmitted frames that experienced multiple collisions.
SQE Test Errors	Displays the number of times an SQE test error message was generated.
Deferred Transmissions	Displays the number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Displays the number of times a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	Displays the number of frames for which transmission fails due to excessive collisions.
MAC Transmit Errors	Displays the number of frames for which transmission fails due to an internal MAC sub layer transmit error.
MAC Receive Errors	Displays the number of frames for which reception on an interface fails due to an internal MAC sub layer receive error.
Carrier Sense	Displays the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frame Too Long	Displays the number of frames received that exceed the maximum permitted frame size.
Reset Counters	Click Reset Counter to cause the interface and media counter values on the module to set to zero and the values on the dialog box to update to the current counter values.

Parameters	Description
	The Reset Counter appears dimmed when offline or when online and a communication error occurs.

Advanced Time Sync

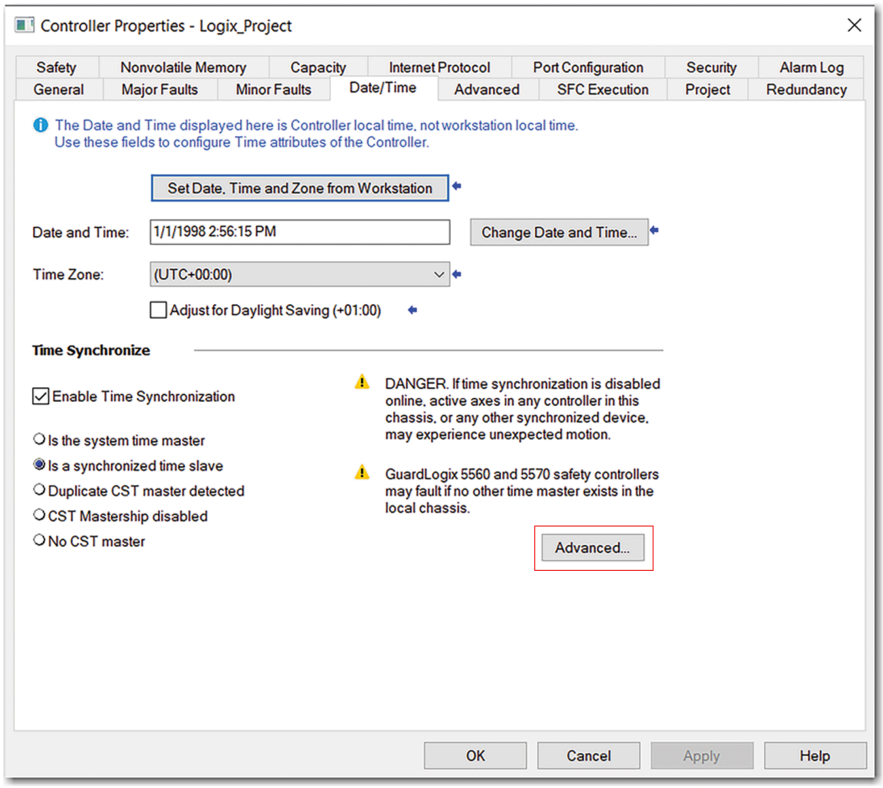
The Advanced Time Sync dialog displays information that is related to CIP Sync™ time synchronization. The information appears only if the project is online and Time Synchronization is enabled on the Date/Time tab.

IMPORTANT: Precision Time Protocol (PTP) Software

- Access to software that manages PTP on a control system network must be limited to users who are trained on the administration of industrial control system time including PTP. This includes the PTP update tool that is supplied by Rockwell Automation, or other publicly available PTP management software. Incorrect updates while a control system is running can disrupt the operation of the control system, including major faults and some devices taken offline.
- When disabling PTP on a controller, to give the controller time to process the disable, use a two-second delay before setting the WallClockTime (WCT) in the controller. Otherwise, there is a risk of the Grandmaster clock overwriting the WCT.

On the Date/Time tab, click the Advanced button.

Figure 65. Controller Properties Date/Time Tab



The Advanced Time Sync dialog box opens.

Figure 66. Advanced Time Sync

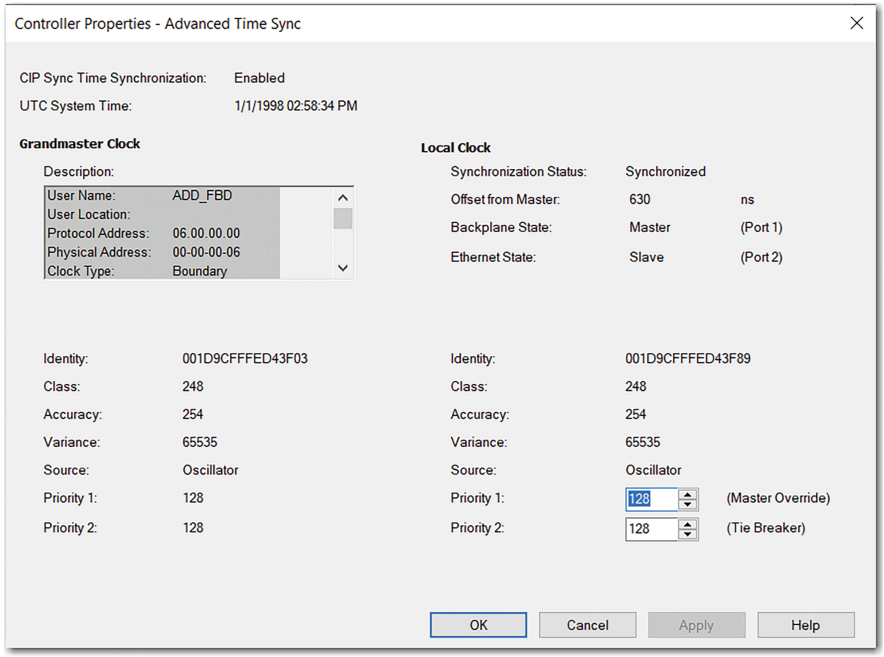


Table 51. Advanced Time Sync Parameters

Grandmaster Clock	
Description	Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified: • User Name • User Location • Protocol Address • Physical Address • Clock Type • Manufacturer Name • Model • Serial Number • Hardware Revision • Firmware Revision • Software Revision • Profile Identity • Physical Protocol • Network Protocol • Port Number Use the vertical scroll bar to view the data.
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0...255 with zero as the best clock.

Table 51. Advanced Time Sync Parameters (continued)

Grandmaster Clock	
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the Grandmaster clock. The available values are: • Atomic Clock • GPS • Radio • PTP • NTP • HAND set • Other • Oscillator
Priority 1 / Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The priority values range from 0…255. The highest priority is zero. The default value for both settings is 128.
Local Clock	
Synchronization Status	Displays whether the local clock is synchronized or not synchronized with the Grandmaster reference clock. A clock is synchronized if it has one port in the slave state and is receiving updates from the master.
Offset to Master	Displays the amount of deviation between the local clock and the Grandmaster clock in nanoseconds.
Backplane State	Displays the current state of the backplane. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Ethernet State	Displays the state of the Ethernet port. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the local clock. Values are defined from 0…255, with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the local clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the local clock. The available values are: • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP

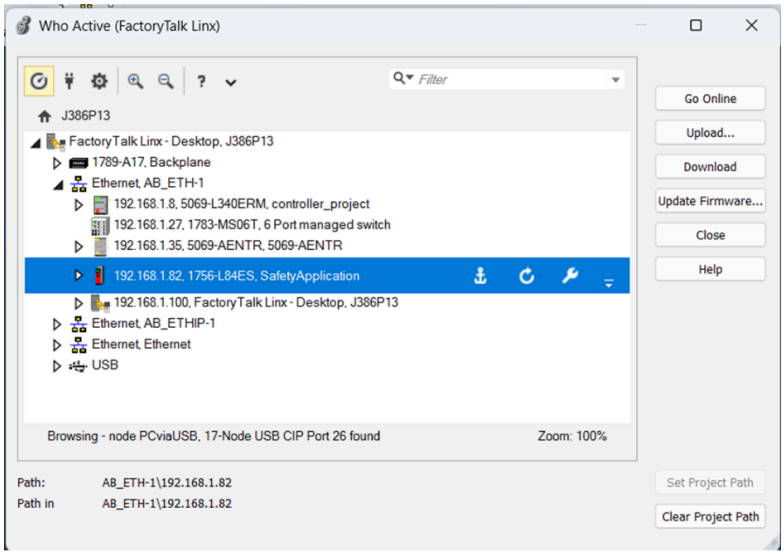
Table 51. Advanced Time Sync Parameters (continued)

Grandmaster Clock	
	• HAND set • Other • Oscillator

Controller Diagnostics with Linx-based Software

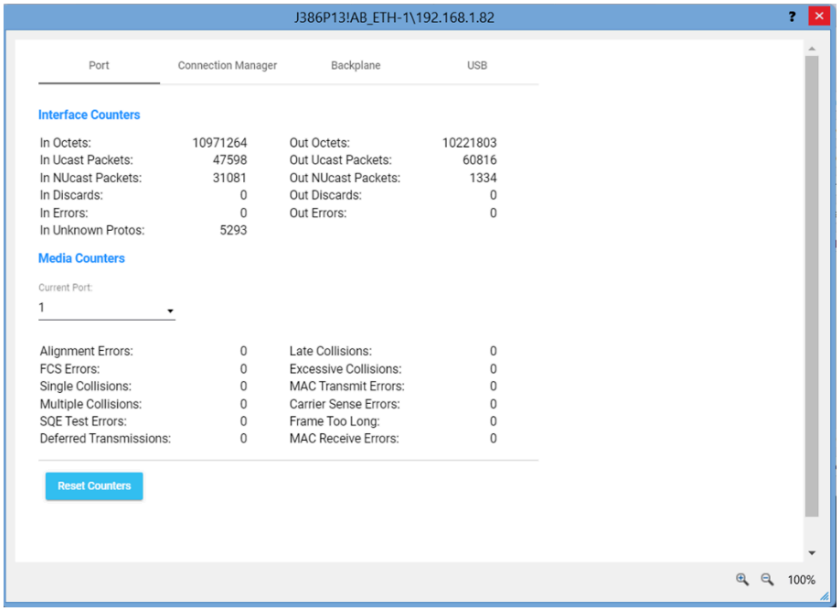
You can also view diagnostic information in Linx-based software.

1. From the Communications menu, select Who Active or Network Browser.
2. Navigate to the controller on the EtherNet/IP™ network.



3. Right-click the controller and choose Device Statistics.

The Statistics dialog box shows a variety of information.

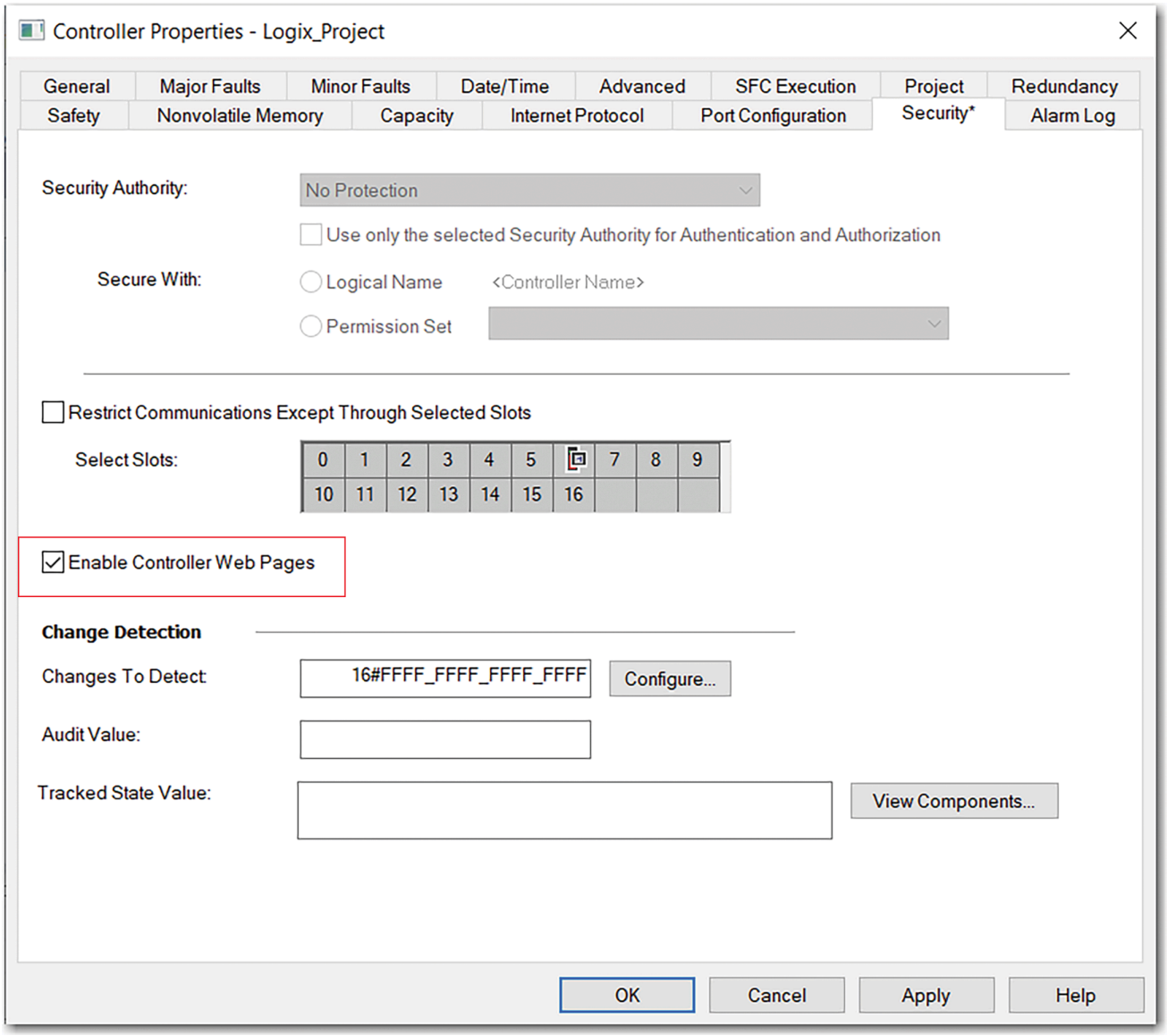


Controller Webpages

The controller provides diagnostic webpages that track controller performance, network performance, and backplane performance. Controller webpages are read-only.

IMPORTANT: Controller webpages are disabled by default with the Studio 5000 Logix Designer® application version 33 or later.

- To enable the controller webpages, select the checkbox on the Security tab of the controller properties.



- For CIP Security™ applications, you can also use FactoryTalk® Policy Manager to enable the webpages. FactoryTalk® Policy Manager overrides the Controller Properties checkbox.

To access the diagnostic webpages, follow these steps.

1. Open your web browser.
2. In the Address field, type the IP address of the controller and press Enter.
3. To access the diagnostic webpages, use the links in the left-side navigation bar. Some links are only accessible if you open the folder in which they exist.

EtherNet/IP settings and safety applications can slightly modify the web pages. In general, the web pages offer:

- Home webpage provides device information and controller status
- Faults webpage shows major and minor faults on the controller.
- Diagnostics webpages provide communications and messaging data for the controller.

- Tasks webpage shows CPU utilization of the control and communications cores and summarizes the tasks that are running in the controller.
- Browse Chassis webpage lets you view module information, backplane statistics, and connection statistics for modules in the local chassis.

Status Indicators

The controller has six status indicators and one four-character scrolling status display. The 1756-L8SP safety partner has the four-character scrolling status display and the OK status indicator.

Figure 67. Status Display and Status Indicators

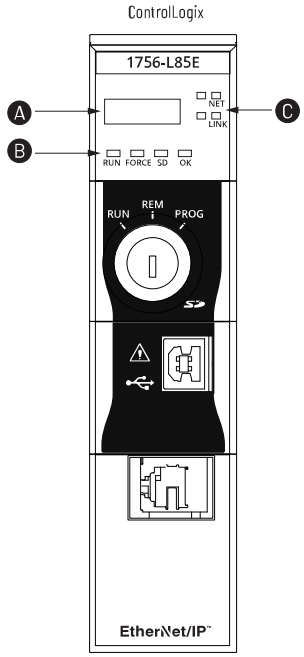
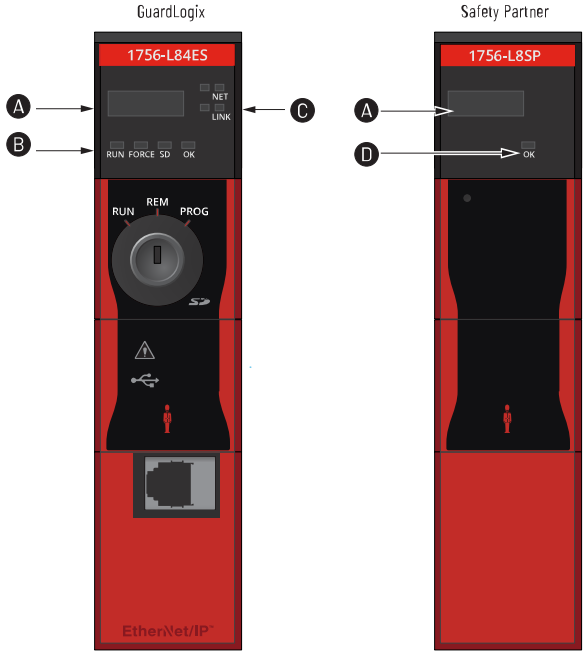


Figure 68. Status Display and Status Indicators



Item	Description
A	Four-character scrolling status display. You can disable some of these messages. See Disable the Status Display.
B	Controller status indicators.
C	EtherNet/IP™ status indicators.
D	Safety partner OK status indicator.

General Status Messages

The scrolling messages that are described in this table are typically indicated upon powerup, power down, and while the controller is running to show the status of the controller.

Table 52. Controller General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Determine if the controller is powered and determine the state of the controller
Identity Mismatch—Contact Tech Support Missing Vendor Certificate—Contact Tech Support Bad Vendor Certificate—Contact Tech Support	Beginning with firmware revision 34.011, if a firmware update identifies the controller as not authentic, the hardware is permanently disabled.
TEST	The controller is conducting power-up tests.
CHRG	The embedded energy storage circuit is charging.
PASS	Power-up tests have been successfully completed.
Saving...Do Not Remove SD Card	The controller is about to save an image to the SD card.
SAVE	A project is being saved to the SD card. Allow the save to complete before: • Removing the SD card. • Disconnecting the power. **IMPORTANT:** Do not remove the SD card while the controller is saving to the SD card. Allow the save to complete without interruption. If you interrupt the save, data corruption or loss can occur.
LOAD	A project is being loaded from the SD card. Allow the load to complete before doing the following: • Removing the SD card. • Disconnecting the power. **IMPORTANT:** Do not remove the SD card while the controller is loading from the SD card. Allow the load to complete without interruption. If you interrupt the load, data corruption or loss can occur.
UPDT	A firmware update is being conducted from the SD card upon powerup. If you do not want the firmware to update upon powerup, change the Load Image property of the controller.

Table 52. Controller General Status Messages (continued)

Message	Interpretation
Rev *XX.xxx*	The major and minor revision of the firmware of the controller.
Catalog number	The controller catalog number and series.
Link Down	The message appears when the Ethernet port does not have a connection. The message scrolls continuously during operation.
Link Disabled	The message appears when you have disabled the Ethernet port. The message scrolls continuously during operation.
DHCP- 00:00:XX:XX:XX:XX	The message appears when the controller is set for DHCP but not configured on a network. The message shows the MAC address of the controller. The message scrolls continuously during operation if no IP address is set.
Ethernet Port Rate/Duplex State	The current port rate and duplex state when the Ethernet port has a connection. The message scrolls continuously during operation.
IP address	The IP address of the controller. Appears on powerup, then scrolls continuously during operation. If the IP address is not yet set, then the MAC address appears.
Duplicate IP - 00:00:XX:XX:XX:XX	The message appears when the controller detects a device on the network that has the same IP address as the controller Ethernet port. The message shows the MAC address of the device with the duplicate IP address. The message scrolls continuously during operation.
No Project	No project is loaded on the controller. To load a project, do one of the following: • Download a project to the controller • Use an SD card to load a project to the controller
Project Name	The name of the project that is loaded on the controller.
BUSY	The I/O modules that are associated with the controller are not yet fully powered. Allow time for powerup and I/O module self-testing.
Corrupt Certificate Received	The security certificate that is associated with the firmware is corrupted. Go to rok.auto/support and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Corrupt Image Received	The firmware file is corrupted. Go to rok.auto/support and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Backup Energy HW Failure - Save Project	A failure with the embedded storage circuit has occurred, and the controller is incapable of saving the program if a powerdown occurs. If you see this message, then save your program to the SD card before you remove power and then replace the controller.
Backup Energy Low - Save Project	The embedded storage circuit does not have sufficient energy to enable the controller to save the program if a powerdown occurs. If you see this message, then save your program to the SD card before you remove power, and then replace the controller.

Table 52. Controller General Status Messages (continued)

Message	Interpretation
Flash in Progress	A firmware update that is initiated via ControlFLASH Plus®, ControlFLASH™ or AutoFlash software is in progress. Allow the firmware update to complete without interruption.
Firmware Installation Required	The controller is using boot firmware (revision 1.*xxx*) and requires a firmware update.
SD Card Locked	An SD card that is locked is installed.
SD Card Unprotected	The controller SD card has been unprotected and is available for remote read/write operations.
Download in Progress	An active download is occurring
Aborting Download	An active download is being canceled. This may be due to a user-initiated cancel, a download failure, or connection loss. After completion, the No Project status message displays.

Safety Status Messages

In addition to the general status messages, these safety messages can display as scrolling messages.

Table 53. Safety Status Messages

Message	Interpretation
No Safety Signature	Safety Task is in Run mode without a safety signature. Generate a safety signature.
Safety Unlocked	The controller is in Run mode with a safety signature but is not safety-locked. Safety-lock the controller.
Safety Partner Missing	The safety partner is missing or unavailable. Make sure that the safety partner is seated properly in the slot that is immediately to the right of the safety controller. The controller displays this message only in a SIL 3/PLe configuration.
Hardware Incompatible	ControlLogix and GuardLogix only The safety partner and primary controller hardware are incompatible. The controller displays this message only in a SIL 3/PLe configuration.
Firmware Incompatible	ControlLogix and GuardLogix only The safety partner and primary controller firmware revision levels are incompatible. Update the modules to the correct firmware revision. The controller displays this message only in a SIL 3/PLe configuration.
Safety Task Inoperable	The safety logic is invalid. For example, a mismatch occurred between the primary controller and the safety partner, a watchdog timeout occurred, or memory is corrupt.

Safety Partner Status Messages

The safety partner display can show these scrolling messages.

Table 54. Safety Partner Status Messages

Message	Interpretation
L8SP	Standard display text. If there is a major nonrecoverable fault, then the fault code scrolls across the display.
Flash in Progress	A firmware update is in progress. Allow the firmware update to complete without interruption.

Fault Messages

If the controller displays a fault, these scrolling messages can appear on the status display. For more information about how to monitor and handle major and minor controller faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication 1756-PM014.

Table 55. Fault Messages

Message	Interpretation
Major Fault T*XX:CXX message*	A major fault of Type *XX* and Code *XX* has been detected. For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, a JMP instruction is programmed to jump to an invalid LBL instruction. Major faults of Type 1, Codes 60, 61, 62 include a unique 9-character code that you can provide to Rockwell Automation® support for troubleshooting.
I/O Fault Local:*X #XXXX message*	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleName #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module is indicated with the fault code and a brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named My_Module is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleParent:X #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The parent name of the module is indicated because no module name is configured in the I/O Configuration tree of the Logix Designer application. In addition, the fault code is indicated with a brief description of the fault. For example, I/O Fault My_CNet:3 #0107 Connection Not Found indicates that a connection to a module in slot 3 of the chassis with the communication module named My_CNet is not open. Take corrective action specific to the type of fault indicated.
X I/O Faults	I/O faults are present and *X* = the number of I/O faults present. If there are multiple I/O faults, the controller indicates the first fault reported. As each I/O fault is resolved, the number of indicated faults decreases and the I/O Fault message indicates the next reported fault. Take corrective action specific to the type of fault indicated.

Major Fault Messages

The Major Fault T*XX*:C*XX* message on the controller scrolling display indicates major faults.

This topic links to Logix 5000 Controller and I/O Fault Codes and Syslog Messages, 1756-RD001; the file automatically downloads when you click the link.

For suggested recovery methods for major faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

I/O Fault Codes

The controller indicates I/O faults on the status display in one of these formats:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent:X #XXXX message*

The first part of the format is used to indicate the location of the module with a fault. How the location is indicated depends on your I/O configuration and the properties of the module that are specified in the Studio 5000 Logix Designer® application.

The latter part of the format, #XXXX message, can be used to diagnose the type of I/O fault and potential corrective actions.

This topic links to Logix 5000 Controller and I/O Fault Codes and Syslog Messages, 1756-RD001; the file automatically downloads when you click the link.

For suggested recovery methods for major faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

Controller Status Indicators

The status indicators are below the status display on the controller. They indicate the state of the controller as described in these tables.

IMPORTANT: Status indicators do not provide detailed diagnostics for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

RUN Indicator

The RUN status indicator shows the current mode of the controller.

To change the controller mode, you can use the controller switch on the front of the controller or the Controller Status menu in the Studio 5000 Logix Designer® application.

Table 56. RUN Status Indicator

State	Description
Off	The controller is in Program or Test mode.
Steady green	The controller is in Run mode.

FORCE Indicator

The Force status indicator shows if I/O forces are enabled on the controller.

Table 57. FORCE Status Indicator

State	Description
Off	No tags contain I/O force values, and I/O force values are not enabled.
Steady yellow	I/O forces enabled. If any I/O force values exist, they are active. **NOTE:** Use caution if you change any force values. In this state, the changes take effect immediately.
Flashing yellow	I/O forces exist in the application, but are not active because I/O forces are not enabled. **NOTE:** Use caution if you enable I/O forces. All existing I/O force values take effect immediately.

SD Indicator

The SD status indicator shows if the SD card is in use.

Table 58. SD Status Indicator

State	Description
Off	No activity is occurring with the SD card.
Flashing green	The controller is reading from or writing to the SD card. **NOTE:** Do not remove the SD card while the controller is reading or writing. Allow the read/write to complete without interruption. If you interrupt the read/write, data corruption or loss can occur.
Steady green	
Flashing red	The SD card does not have a valid file system.
Steady red	The controller does not recognize the SD card.

OK Indicator

The OK status indicator shows the state of the controller.

Table 59. Controller OK Status Indicator

State	Description
Off	No power is applied to the controller.

Table 59. Controller OK Status Indicator (continued)

State	Description
Flashing red	One of the following exists: • It is a new controller, out of the box, and it requires a firmware update. If a firmware update is required, the status display indicates Firmware Installation Required. To update firmware, see Use ControlFLASH Plus Software to Update Firmware on page . • A firmware update is in progress. If a firmware update is in progress, the 4-character display indicates Flash in Progress. • It is a previously used or in-use controller and a major fault has occurred. All user tasks, standard and safety, are stopped. • For details about major recoverable and nonrecoverable faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
Steady red	One of the following is true: • The controller is completing power-up diagnostics. • The charge of the capacitor in the ESM is being discharged FavoritesVersion: none upon powerdown. • The controller is powered, but is inoperable. • The controller is loading a project to nonvolatile memory. • The controller is experiencing a Hardware Preservation Fault due to a high internal module temperature. In this condition, only the status indicator receives power. Once the controller cools down to an acceptable temperature, then full power is applied.
Steady green	The controller is operating normally.

Safety Partner OK Indicator

The safety partner has an OK status indicator.

Table 60. Safety Partner OK Status Indicator

State	Description
Off	No power is applied.
Green	The safety partner is operating with no faults.
Red	One of the following is true: • The safety partner is completing power-up diagnostics. • The charge of the capacitor in the ESM is being discharged upon powerdown. • The safety partner is powered but is inoperable. • The safety partner is loading a project to nonvolatile memory. • The safety partner is experiencing a Hardware Preservation Fault due to a high internal module temperature. In this condition, only the status

Table 60. Safety Partner OK Status Indicator (continued)

State	Description
	indicator receives power. Once the safety partner cools down to an acceptable temperature, then full power is applied.
Flashing red	The controller is configured for SIL 2 operation, but a safety partner is installed.

EtherNet/IP Indicators

The EtherNet/IP status indicators show the state of the EtherNet/IP port and communication activity.

Table 61. EtherNet/IP Status Indicators

Indicator	State	Description
NET	Off	• The controller is not configured, or does not have an IP address. • The port is administratively disabled. • In a dual-port controller, the EtherNet/IP mode is Linear/DLR mode. In this case, the NET A2 indicator is off. The NET A1 indicator remains on.
	Flashing green	The controller has an IP address, but no active connections are established.
	Steady green	The controller has an IP address and at least one established active connection.
	Steady red	Duplicate IP address or invalid configuration.
LINK	Off	No activity. One of these conditions exists: • No link exists on the port. • Verify that the RJ45 cables are properly seated in the adapter and connected devices. • The port is administratively disabled. • In a dual-port controller, LINK A2 only - The controller is the active ring supervisor in a DLR network and has detected a rapid ring fault.
	Flashing green	All of these conditions exist: • The port is enabled. • A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device. • There is activity on the port.
	Steady green	On a single-port controller, a link exists on the port, but no traffic is being received. On a dual-port controller, all of these conditions exist: • The port is enabled. • A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device.

Table 61. EtherNet/IP Status Indicators (continued)

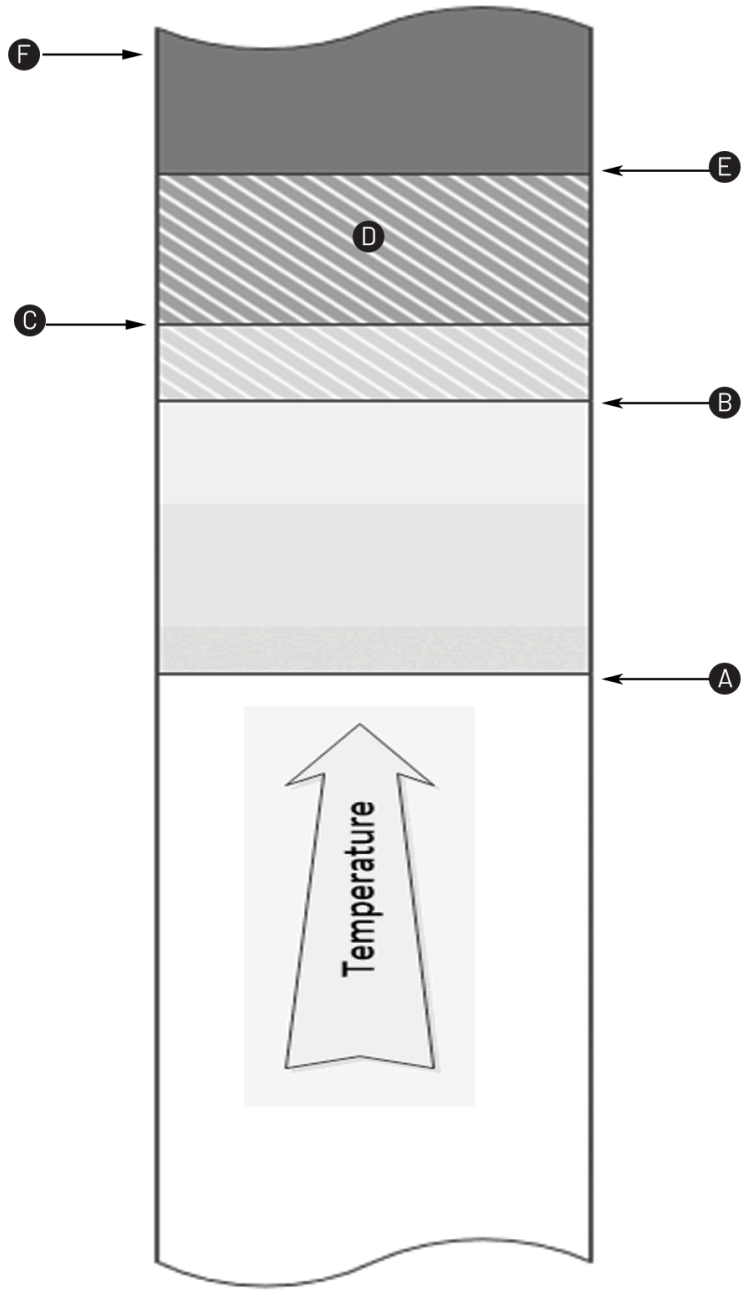
Indicator	State	Description
		• LINK A2 only - The controller is the active ring supervisor in a DLR network, and the ring is not broken. This is a normal operation. • There is no activity on the port.

Thermal Monitoring and Thermal Fault Behavior

The controllers can monitor internal module temperatures and act as the temperature increases.

IMPORTANT: If you follow the recommended limits for ambient (inlet) temperature and apply the required clearances around the chassis, the controller should not reach the initial warning (minor fault) temperature. See the 1756 ControlLogix and GuardLogix Controllers Technical Data, publication 1756-TD001.

Figure 69. Thermal Monitoring



Item	Description
A	Threshold for controller to declare a `T17:C35 Controller internal temperature is approaching operating limit' minor fault and set the Diagnostics minor fault bit. The fault is recorded in the minor fault log but is not displayed on the front panel. If the temperature returns to an acceptable range, the Diagnostics minor fault bit clears, but the minor fault record remains.
B	Threshold for the controller to declare a `CPU Temperature Fault' major recoverable fault. If a fault handler does not clear the fault, then the module enters fault mode, records the fault in the major fault log, and displays `T17:C34 CPU Temperature Fault' on the front panel.
C	Hardware Preservation Hysteresis Limit.

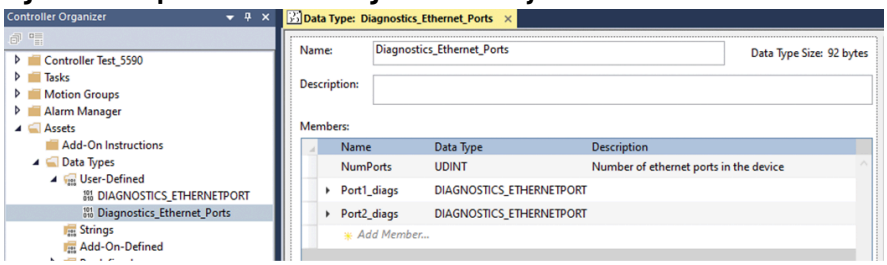
Item	Description
D	Power does not become enabled when in this range.
E	Threshold for the controller to declare a `Hardware Preservation Fault', resetting the module and disabling power. In the disabled power condition, only the OK status indicator is illuminated, and it is red. The module does not apply power until it has cooled below the Hardware Preservation Hysteresis limit. The module then enters fault mode, records the fault in the major fault log, and displays `CPU Temperature Fault' on the front panel.
F	All power to the controller is disabled except to run the red OK status indicator and monitor the temperature.

IMPORTANT: The presence of any temperature warning indicates that you must act to reduce the ambient temperature of the module. Instructions for using relay ladder logic to check for a minor fault can be found in the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication 1756-PM014. A GSV instruction can read the MinorFaultBits attribute of the FaultLog class name. If the Diagnostics minor fault bit (Bit 17) is set, then a temperature minor fault can be present. Check the Minor Faults tab of the Controller Properties dialog box in the Logix Designer application to see if the minor fault is a temperature warning.

Access Diagnostic Assembly Tags

Use diagnostic assembly tags to access controller status from the controller webpages and other diagnostic information. Each assembly has specific elements. You create UDTs and use MSG instructions to access the data in these elements.

Figure 70. Example Ethernet Ports Diagnostic Assembly



The available diagnostic assemblies include:

Table 62. Diagnostic Assemblies

Diagnostic Assembly	Description
Home	Provides device information and controller status.
Home (Safety)	Safety-related data for a safety-enabled controller.
Module Diagnostics	Module communication diagnostics.
Ethernet Statistics	Ethernet port diagnostics.
Faults	Faults data that shows major and minor faults on the controller.
OPC UA	OPC webpage data that includes number of currently used OPC UA nodes, OPC UA nodes limit, and OPC UA nodes per second statistics.
PTP	1588 PTP Time Sync webpage data.
Concurrent Connections	Concurrent Connection data information that includes Branch Failure, Failure Count, and Packets Lost.
Backplane Statistics	Diagnostics for a specific slot in a chassis.
Standard Network Diagnostics	Standard network diagnostics includes four main diagnostic assemblies for Single Port controllers, Device Level Ring (DLR), Dual-IP configuration, and PRP (Parallel Redundancy Protocol). • Single Port supports ControlLogix® 5580 controllers. • DLR supports ControlLogix® 5590 controllers, CompactLogix® 5380 controllers, and 1756-EN4TR communication modules. • Dual-IP supports ControlLogix® 5590 controllers and CompactLogix® 5380 controllers. • PRP supports 1756-EN4TR communication modules.

Create a MSG Instruction to Access a Diagnostic Assembly

Use a CIP™ Generic MSG to access diagnostic assembly data.

1. Configure the Configuration tab on the Message Configuration dialog box as described below.

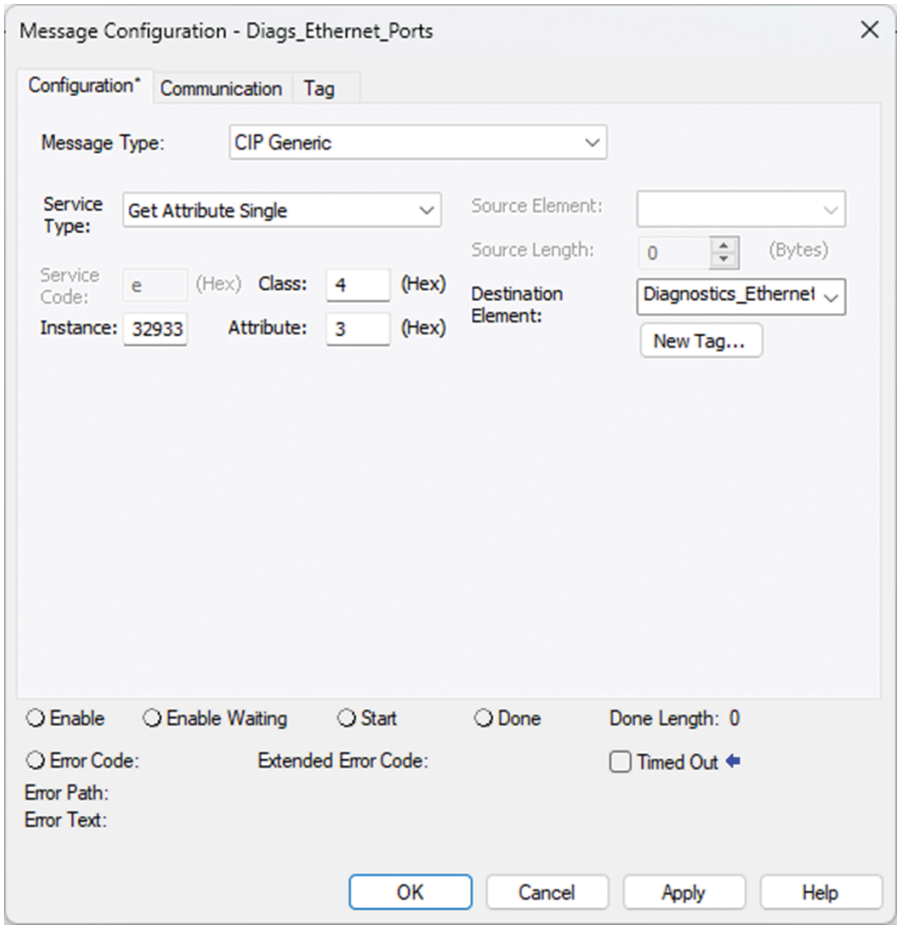
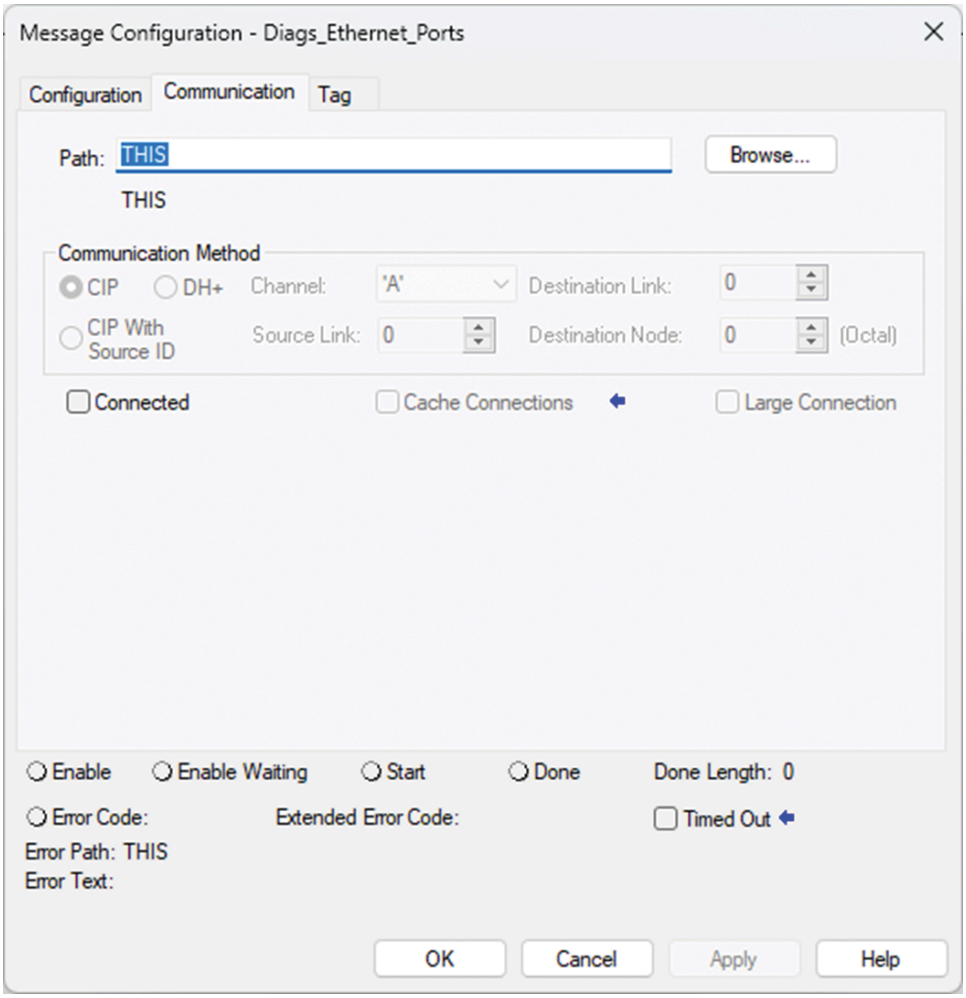


Table 63. Configure MSG Instruction

Field	Value
Message Type	CIP Generic
Service Type	Get Attribute Single
Class	4
Attribute	3
Instance	Specific to the diagnostic assembly. Must be in decimal format.
Destination Element	Controller tag of the UDT for the diagnostic assembly.

2. On the Communication tab, specify a Path of THIS for the local controller, or specify a remote controller.



Concurrent Connections Diagnostic Assembly

Concurrent Connection data information that includes Branch Failure, Failure Count, and Packets Lost.

- Instance = 32952
- Size = 12 Bytes

Table 64. Diagnostic Assembly Members

Member	Data Type	Description
BranchFailure	BOOL	This attribute indicates that one or more branches towards target(s) of any concurrent connections in which this device is a participant is not open (was not opened or timed out).
FailureCount	UDINT	This attribute is incremented every time when the Concurrent Connections Branch Failure attribute transitions from 0 to 1.
PacketsLost	UDINT	For each concurrent connection, as long as it remains open when the consumer on the branch of concurrent connection is processing the packet, it shall subtract the last received Concurrent Connection Sequence Count on this branch from the Concurrent Connection Sequence Count of this packet. If the value exceeds positive one (+1), then that value minus one is the number of concurrent connection packets that have been lost. A concurrent connection branch timeout does not cause Concurrent Connection Packets Lost to increment.

Ethernet Port Diagnostics Assembly

Ethernet Statistics webpage data.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_ETHERNETPORT user-defined data type (UDT). This data type includes the information captured for each Ethernet port. Create this UDT before you create the Ethernet Port Diagnostics UDT.

Structure for the DIAGNOSTICS_ETHERNETPORT User-defined Data Type

Table 65. Members for User-defined Data Type

Member	Data Type	Description
PortNumber	UDINT	Number of the port. Represents the instance number of the TCP/IP Interface Object.
IPAddress	USINT[4]	IP address of the port.
MacAddress	USINT[6]	Mac address of the port.
TCPConnections	UINT	TCP connections opened through the port.
CIPConnections	UINT	Total number of class 0/1 and 3 CIP connections opened through the port (sum of CIP I/O Connections attribute and CIP Explicit Connections attribute).
CIPLostPackets	UDINT	Number of lost CIP packets sent via port.
CIPTimeouts	UDINT	Number of timeouted CIP connections sent via port.
HMIPacketRate	UDINT	HMI packet rate sent via port.
IOPacketRate	UDINT	I/O packet rate sent via port.
EthernetErrors	UDINT	Number of ethernet errors in the port.
CPUUtilization	UINT	Utilization of the CPU (same for all ports).

Ethernet Port Diagnostics Assembly

- Instance = 32933
- Size = 180 Bytes

Table 66. Diagnostic Assembly Members

Member	Data Type	Description
NumPorts	UDINT	Number of ethernet ports in the device
Port1	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.
Port2	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.
Port3	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.

Table 66. Diagnostic Assembly Members (continued)

Member	Data Type	Description
Port4	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.

Home Webpage Diagnostic Assembly

Home webpage data that provides device information and controller status.

- Instance = 32930
- Size = 270 Bytes

Table 67. Diagnostic Assembly Members

Member	Data Type	Description
CatalogString	STRING_32	Textual catalog or model number.
ProductCode	UINT	Identification of a particular product of an individual vendor.
MajorRevision	USINT	Major revision of the module.
MinorRevision	USINT	Minor revision of the module.
CIPSerialNumber	UDINT	Serial number of device.
WarrantySerialNumber	STRING_32	Serial number of product warranty.
ManufactureDate	UINT	Date the product was manufactured.
ProjectName	STRING	Name of the project downloaded into the module.
StatusBits (Hidden)	UDINT	Summary status of device.
RunMode	BOOL	Indicates whether controller is in the run mode.
KeySwitchRemote	BOOL	Specifies whether the key is in the "remote" position.
IOForcesExist	BOOL	Indicates whether IO forces exists. It is true only when "Force" LED is amber or flashing.
IOForcesActive	BOOL	Indicates whether IO forces are enabled. Logix Designer labels it "Forces" / "No Forces". It is true only when "Force" LED is amber.
SDCardFault	BOOL	Specifies whether SD card fault appeared. It is true if SD LED is solid or flashing red.
SDCardActivity	BOOL	Specifies whether SD card is active. It is true if SD LED is solid or flashing green.
MajorFault	BOOL	A value that indicates whether the module has a major fault. It is bit 4.
MinorFault	BOOL	A value that indicates whether the module has a minor fault. It is bit 5.
IOFault	BOOL	A value that indicates whether the module has a IO fault.

Table 67. Diagnostic Assembly Members (continued)

Member	Data Type	Description
EnergyStorageStatus	BOOL	From LogixDesigner this is: minor_fault_bits.10 If minor_fault_bits.10 is on, depending on the controller, the battery is low or the ESM or UPS needs to be replaced or is missing.
StatusDisplayText	STRING	Scrolling string includes: • Project Name • Ethernet Address • Link State (Up Down) • Link Speed • IO Fault • Redundancy State
MajorHardwareRevision	USINT	Major revision of the module hardware.
MinorHardwareRevision	USINT	Minor revision of the hardware module.
HardwareSeries	SINT[2]	Two ASCII characters describing the hardware series. It is Rockwell extension to the Identity object.

Home (Safety) Diagnostic Assembly

Safety-related data on the Home webpage for a safety-enabled controller.

- Instance = 32931
- Size = 96 Bytes

Table 68. Diagnostic Assembly Members

Member	Data Type	Description
SafetyStatus	BOOL	SIL 2/SIL3 Status information of the safety task and the partnership between the controller and its safety partners.
SafetyLocked	BOOL	Indicates if the safety application is in the locked state.
SafetySigned	BOOL	Indicates if a Safety Signature has been created and the controller is in a protected state.
SafetySignatureID	UDINT	ID portion of the safety signature CRC over safety memory. Returns zero when no snapshot exists, or on controllers that do not support a four-byte safety signature.
SafetySignatureTimestampString	STRING	Software generated timestamp that indicates when a Safety Signature was generated. Contains the Safety Signature Timestamp String when a valid snapshot exists. Maximum length is 40 characters. Format of string is “mm/dd/yyyy, hh:mm:ss.iii <AM or PM>” where iii = milliseconds. This string is set to "Non-existing" when no snapshot exists.

Module Diagnostics Diagnostic Assembly

Module Diagnostics webpage data.

- Instance = 32932
- Size = 20 Bytes

Table 69. Diagnostic Assembly Members

Member	Data Type	Description
IOConnections	UINT	Number of I/O connections (class 0/1).
MessagingConnections	UINT	Number of messaging connections (class 3).
MaxObservedConnections	UINT	Maximum number of observed class 3 connections.
IOCommsUtilizationActual	UINT	Represents the current I/O communications utilization for I/O traffic.
IOCommsUtilizationTheoretical	UINT	Based on information agreed during Forward Open procedure. Represents the theoretical I/O communications utilization for I/O traffic.
IOPPSActual	UDINT	I/O messages packets per second.
IOPPSTheoretical	UDINT	Based on information agreed during Forward Open procedure. The theoretical value for I/O messages packets per second.

OPC UA Diagnostic Assembly

OPC webpage data that includes number of currently used OPC UA nodes, OPC UA nodes limit, and OPC UA nodes per second statistics.

- Instance = 32940
- Size = 12 Bytes

Table 70. Diagnostic Assembly Members

Member	Data Type	Description
UsedNodes	UDINT	Number of currently used OPC UA user defined nodes for a server associated with this instance.
MaxNodes	UDINT	Maximum possible number of OPC UA user defined nodes that a client can write or read from a server associated with this instance.
NodesPerSecond	UDINT	Current number of read or written scalar nodes per second. Scalar node means node with one basic type value or with one string. Vector and matrix nodes are counted as the number of its atomic elements.

PTP Diagnostic Assembly

1588 PTP Time Sync webpage data.

- Instance = 32941
- Size = 88 Bytes

Table 71. Diagnostic Assembly Members

Member	Data Type	Description
Enabled	BOOL	Is PTP enabled.

Table 71. Diagnostic Assembly Members (continued)

Member	Data Type	Description
TimeTransmitter	BOOL	Is The Grandmaster
SyncValid	BOOL	Sync status.
DomainNumber	USINT	Domain number
StepsRemoved	UINT	Steps removed.
SyncStatus	UDINT	CipSyncSynchronizationStatus. Available options are: init (0), synchronization hold timed out (1), synchronization hold (2) and synchronized (3).
UTCTime	STRING_32	SystemTime in user-friendly type. Counted using SystemTime.
SystemTime	ULINT	SystemTimeNanoseconds
OffsetFromTimeTransmitter	ULINT	Offset from master
MaxOffsetFromTimeTransmiter	ULINT	Max Offset from master.
AvgPathDelayTime	ULINT	Mean path delay to master.
SystemToLocalClockOffset	ULINT	Offset between system time and local time.

Faults Diagnostic Assembly

Faults webpage data that shows major and minor faults on the controller.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_FAULTDETAILS user-defined data type. This data type includes the information captured for each fault. Create this UDT before you create the Fault UDTs.

Structure for the DIAGNOSTICS_FAULTDETAILS User-defined Data Type

Table 72. Members of User-defined Data Type

Member	Data Type	Description
Timestamp	ULINT	The moment when the fault occurred. It's format is the UNIX timestamp in microseconds.
Code	UDINT	Fault code.
Type	UDINT	Type number of the fault code.
Description_1	STRING	Part 1 of the fault description.
Description_2	STRING	Part 2 of the fault description.

Diagnostic Faults_A Assembly

- Instance = 32934
- Size = 392 Bytes

Table 73. Diagnostic Assembly Members

Member	Data Type	Description
MajorFaultsReported	UDINT	Count of all Major Faults reported
MinorFaultsReported	UDINT	Count of all Minor Faults reported
MajorFault1	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MajorFault2	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_B Assembly

- Instance = 32935
- Size = 192 Bytes

Table 74. Diagnostic Assembly Members

Member	Data Type	Description
MajorFault3	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_C Assembly

- Instance = 32936
- Size = 384 Bytes

Table 75. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault1	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault2	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_D Assembly

- Instance = 32937
- Size = 384 Bytes

Table 76. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault3	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault4	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_E Assembly

- Instance = 32938
- Size = 384 Bytes

Table 77. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault5	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault6	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_F Assembly

- Instance = 32939
- Size = 384 Bytes

Table 78. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault7	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault68	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

ControlLogix Backplane Statistics

Diagnostics for a specific slot in a chassis.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_CHASSIS_SLOTS_DATA user-defined data type. This data type includes the information captured for each slot. Create this UDT before you create the Chassis Diagnostics UDTs.

Structure for the ControlLogix DIAGNOSTICS_CHASSIS_SLOTS_DATA User-defined Data Type

Table 79. Members of User-defined Data Type

Member	Data Type	Description
MajorRevision	UDINT	Major revision of the module in the slot (for specific module in chassis).
MinorRevision	UDINT	Minor revision of the module in the slot (for specific module in chassis).
SerialNumber	UDINT	Serial number of the module in the slot (for specific module in chassis).
Slot	USINT	Slot number (for specific module in chassis).
Status	USINT	Current status of ICP object: 0 normal communications, bit 0 set = RX Disabled, bit 1 set = Multicast RX Disabled, bit 2 set = RA/GA Miscompare
RxBadMulticastCRC	UDINT	Number of multicast frames received with bad CRC (for specific module in chassis).

Table 79. Members of User-defined Data Type (continued)

Member	Data Type	Description
RxBadMulticastCRCThreshold	UDINT	Threshold of the number of multicast frames received with bad CRC (for specific module in chassis).
RxBadCRC	UDINT	Number of frames received with bad CRC (for specific module in chassis).
RxBusTimeouts	UDINT	Number of timeouts on received frames (for specific module in chassis).
TxBadCRC	UDINT	Number of frames sent with bad CRC (for specific module in chassis).
TxBusTimeouts	UDINT	Number of timeouts on sent frames (for specific module in chassis).
TxRetryLimit	UDINT	Retry limit for sent frames (for specific module in chassis).

ControlLogix Chassis Diagnostics_A Assembly

- Instance = 32942
- Size = 444 Bytes

Table 80. Diagnostic Assembly Members

Member	Data Type	Description
ChassisSize	USINT	Size of the chassis in terms of number of slots and is programmed at time of manufacture into the rack's non-volatile storage.
Slot00	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot01	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot02	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot03	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot04	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot05	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot06	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot07	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot08	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot09	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.

ControlLogix Chassis Diagnostics_B Assembly

- Instance = 32943
- Size = 312 Bytes

Table 81. Diagnostic Assembly Members

Member	Data Type	Description
ChassisSize	USINT	Size of the rack in terms of number of slots and is programmed at time of manufacture into the rack's non-volatile storage.
Slot10	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot11	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot12	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot13	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot14	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot15	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot16	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.

Standard Network Diagnostic Assemblies

Standard network diagnostics includes four main diagnostic assemblies for Single Port controllers, Device Level Ring (DLR), Dual-IP configuration, and PRP (Parallel Redundancy Protocol).

- Single Port supports ControlLogix® 5580 controllers.
- DLR supports ControlLogix® 5590 controllers, CompactLogix® 5380 controllers, and 1756-EN4TR communication modules.
- Dual-IP supports ControlLogix® 5590 controllers and CompactLogix® 5380 controllers.
- PRP supports 1756-EN4TR communication modules.

IMPORTANT: This assembly includes six structures that are used to create user-defined data types that capture the information used in the main diagnostic assemblies. Create these UDTs before you create the main Standard Network Diagnostics UDTs.

The instance number is 210 for the main assemblies, and the device will return the assembly that matches what it is configured for (for example, DLR, PRP, Dual-IP).

Table 82. Structure of Standard Network Diagnostic Assemblies

Main Diagnostic Assemblies	StandardDiag_ConnMgr	StandardDiag_DLRSupervisor	StandardDiag_EthernetLink	StandardDiag_PRP	StandardDiag_TCP	StandardDiag_TimeSync
StandardNetworkDiagnostic_DLRSup	✓	✓	✓	–	✓	✓
StandardNetworkDiagnostic_DualIP	✓	–	✓	–	✓	✓

Table 82. Structure of Standard Network Diagnostic Assemblies (continued)

Main Diagnostic Assemblies	StandardDiag_ConnMgr	StandardDiag_DLRSupervisor	StandardDiag_EthernetLink	StandardDiag_PRP	StandardDiag_TCP	StandardDiag_TimeSync
StandardNetworkDiagnostic_L8	✓	–	✓	–	✓	✓
StandardNetworkDiagnostic_PRP	✓	–	✓	✓	✓	✓

Structures for the Standard Network Diagnostics User-defined Data Types

Use these structures to create user-defined data types that capture the information used in the main diagnostic assemblies. Create these UDTs before you create the main Standard Network Diagnostics Diagnostic Assemblies.

Structure for the StandardDiag_ConnMgr User-defined Data Type

Provides status on I/O and Explicit Messaging connections.

Table 83. StandardDiag_ConnMgr User-defined Data Type

Member	Data Type	Description
MissedIOpacketsCnt	UDINT	Cumulative count of missed IO packets.
NumIOConnection	UDINT	Number of IO connections established.
MessagesPerSecond	UDINT	Number of messages per second being processed.
IOPacketsPerSecond	UDINT	Number of IO packets per second being processed.
NumMessagingConnections	UDINT	Number of messaging connections established.
ConnectionTimeoutsCnt	UINT	Cumulative count of connection timeouts that have occurred.
CPU_Utilization	UINT	CPU utilization measured in tenths of percentage (i.e. 1000 = 100%).
IO_Utilization	UINT	IO capacity utilization measured in tenths of percentage (i.e. 1000 = 100%).
ConcurrentCommsBranchFail	BOOL	One or more concurrent communications branch is currently not transmitting/receiving data.
ConcurrentCommsConnFailCnt	UDINT	Cumulative count of concurrent communications failures.
ConcurrentCommsPacketsLostCnt	UDINT	Cumulative count of concurrent communication packets missed Read/Write.
Pad	UDINT	Reserved

Structure for the StandardDiag_DLRSupervisor User-defined Data Type

Provides status on the Device Level Ring.

Table 84. StandardDiag_DLRSupervisor User-defined Data Type

Member	Data Type	Description
Network_Status	SINT	0 = Normal; 1 = Ring Fault; 2 = Loop Detected; 3 = Partial Fault; 4 = Rapid Fault/Restore Read/Write.
Ring_Supervisor_Status	SINT	0 = Backup; 1 = Active; 2 = Non supervisor; 3 = non-DLR topology; 4 = Unsupported parameter.
Ring_Faults_Count	UINT	Cumulative count of ring faults.
Pad	SINT[4]	Reserved

Structure for StandardDiag_EthernetLink User-defined Data Type

Provides status on the Ethernet link.

Table 85. StandardDiag_EthernetLink User-defined Data Type

Member	Data Type	Description
LinkStatus	BOOL	Indicates whether or not the module is connected to an active network. 0 = inactive link; 1 = active link.
Duplex	BOOL	Indicates the duplex mode currently in use. 0 = half duplex; 1 = full duplex.
NegotiationStatus0	BOOL	Indicates the status of link auto-negotiation.
NegotiationStatus1	BOOL	Indicates the status of link auto-negotiation.
NegotiationStatus2	BOOL	Indicates the status of link auto-negotiation.
Pad	BOOL	Reserved
HardwareFault	BOOL	0 = no local hardware fault; 1 = local hardware fault.
InterfaceSpeed	UDINT	Interface speed currently in use (10, 100, 1000).
LinkDownCnt	UDINT	Link Down Counter. Counts the number of times a Link Down transition event was detected on this port.
EthernetErrors	UDINT	Sum of error counts from Interface Counters and Media Counters.

NegotiationStatus

The status is a 3-bit field, where NegotiationStatus0 is the least significant bit.

Bit	Auto-negotiation in progress.	Auto-negotiation and speed detection failed. Using default values for speed and duplex.	Auto negotiation failed but detected speed. Duplex set to default value	Successfully negotiated speed and duplex	Auto-negotiation not attempted. Forced speed and duplex
NegotiationStatus0	0	1	0	1	0
NegotiationStatus1	0	0	1	1	0
NegotiationStatus2	0	0	0	0	1

In this example, the controller tags of the destination element show that speed and duplex were successfully negotiated.

Dual_IP_Diags.EthernetPort_1.NegotiationStatus0	1	Decimal	BOOL
Dual_IP_Diags.EthernetPort_1.NegotiationStatus1	1	Decimal	BOOL
Dual_IP_Diags.EthernetPort_1.NegotiationStatus2	0	Decimal	BOOL

Structure for theStandardDiag_PRP User-defined Data Type

Provides status on the PRP ports.

Table 86. StandardDiag_PRP User-defined Data Type

Member	Data Type	Description
Warning_LAN_A	BOOL	A potential problem with the PRP port exists.
Warning_LAN_B	BOOL	A potential problem with the PRP port exists.
Pad	SINT[4]	Reserved

Structure for the StandardDiag_TCP User-defined Data Type

Provides status on the TCP/IP network interface.

Table 87. StandardDiag_TCP User-defined Data Type

Member	Data Type	Description
NonCIPMessagesPerSecond	UDINT	Non-CIP messages per second.
NumTCPConnections	UINT	Number of active TCP connections.

Structure for the StandardDiag_TimeSync User-defined Data Type

Provides status on time synchronization.

Table 88. StandardDiag_Time Sync User-defined Data Type

Member	Data Type	Description
IsSynchronized	BOOL	Local clock is synchronized with Time Transmitter.
OffsetFromTimeTransmitter	ULINT	Offset between local clock and Time Transmitter clock in nanoseconds.
GrandMasterID	SINT[8]	GrandMaster Clock Identity.

Main Standard Network Diagnostics Assemblies

Use the data types you created with the Structures for the Standard Network Diagnostics User-defined Data Types on page 227 to create these diagnostic assemblies.

StandardNetworkDiagnostic_DLRSup

- Instance = 210
- Size = 120 Bytes

Table 89. StandardNetworkDiagnostic_DLRSup Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
DLR	StandardDiag_DLRSupervisor	Provides status on the Device Level Ring.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_DualIP

- Instance = 210
- Size = 120 Bytes

Table 90. StandardNetworkDiagnostic_DualIP Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCPPort_1	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TCPPort_2	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_L8

- Instance = 210
- Size = 96 Bytes

Table 91. StandardNetworkDiagnostic_L8 Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.

Table 91. StandardNetworkDiagnostic_L8 Diagnostic Assembly (continued)

Member	Data Type	Description
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_PRP

- Instance = 210
- Size = 120 Bytes

Table 92. StandardNetworkDiagnostic_PRP Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
PRP	StandardDiag_PRP	Provides status on the PRP ports.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

Change Controller Project Type

Because safety projects have special requirements and do not support certain standard features, you must understand the behavior of the system when changing the project from standard to safety or from safety to standard.

Changing the project affects the following:

- Supported features
- Physical configuration of the project (safety partner and safety I/O)
- Controller properties
- Project components such as tasks, programs, routines, and tags
- Safety Add-On Instructions

When you change one controller type to another, the class of tags, routines, and programs remain unaltered. Any I/O devices that are no longer compatible with the target controller are deleted. If needed, the representation of the safety partner is updated to appear appropriately for the target controller.

Change from a Standard to a Safety Project

Upon confirmation of a change from a standard project to a safety project, safety components are created to meet the minimum requirements for a safety project:

- The safety task is created only if the maximum number of downloadable tasks has not been reached. The safety task is initialized with its default values.

If your project already contains 32 tasks, and you try to change from standard to a safety, the project does not convert and stays as a standard project.

- Safety components are created (such as, safety task and safety program).
- The safety project defaults to safety level SIL 2/PLd.
- A time-based safety network number (SNN) is generated for the local chassis.
- A time-based safety network number (SNN) is also generated for the embedded EtherNet/IP™ port.
- Standard features that are not supported by the safety project are removed from the Controller Properties dialog box.

Change from a Safety to a Standard Project

Upon confirmation of a change from a safety project to a standard project, some components are changed, and others are deleted, as described below:

- The safety partner is deleted from the I/O chassis, if it existed.
- Safety I/O devices and their tags are deleted.
- The safety task, programs, and routines are changed to a standard task, programs, and routines.
- All safety tags, except safety consume tags, are changed to standard tags.
- Safety consume tags are deleted.
- Safety tag mappings are deleted.
- The safety network numbers (SNN) are deleted.
- Safety-lock and safety-unlock passwords are deleted.

- If the standard project supports features that were not available to the safety project, those new features are visible in the Controller Properties dialog box.

Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

If the safety project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the project type.

History of Changes

1756-UM543S-EN-P, November 2025

Topic
Added content to the ATTENTION table in section Protect the Safety Signature
Updated the User Initiated row in the Controller Power table that explains how what happens when you insert a memory card and powerup the controller
Moved topic Trusted Slots Slots on the Controller to chapter Manage Controller Communications
Updated content in the ATTENTION table in section Develop Safety Applications
Added topic CIP Bridging Control to chapter Develop Secure Applications
Added content on how to access diagnostic assembly information

1756-UM543R-EN-P, December 2024

Change
Updated Additional Resources table
Revised Controller Redundancy section
Revised Secure Controller Systems section
Added IEC-62443-4-2 SL 1 security certification content for safety controllers
Added statement about impact of license-based source protection on download times
Added Privacy Aspects section
Added information about unique code for troubleshooting major faults Type 1, Codes 60, 61, 62

1756-UM543Q-EN-P, July 2024

Change
Updated information about system compatibility and extreme environment ratings
Added catalog numbers 1756-L81ESXT, 1756-L82ESXT, 1756-L83ESXT, 1756-L84ESXT, 1756-L8SPXT, 1756-L81E-NSEXT, 1756-L82E-NSEXT, 1756-L83E-NSEXT, 1756-L84E-NSEXT, 1756-L85E-NSEXT, 1756-L81EPXT, 1756-L83EPXT, and 1756-L85EPXT
Updated information about conformal coated products
Added recommended SD cards

1756-UM543P-EN-P, November 2023

Change
Added catalog number 1756-L85ES
Revised the Safety Signature section in Chapter 2
Updated the controller Safety tab screenshots
Updated the Safety I/O Replacements Options section
Added a statement about the status of the Enable Controller Webpages checkbox

1756-UM5430-EN-P, February 2023

Change
Updated the controller minimum requirements

1756-UM543N-EN-P, November 2022

Change
Moved information about connection reaction time limit to publication 1756-RM012
Added GuardLogix-XT™ catalog numbers
Revised ControlLogix-XT™ and GuardLogix-XT™ Controllers section
Revised information about the safety signature
Added 1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT catalog numbers
Added information about secure socket objects
Added introduction and Program Safety Applications section to Chapter 11 and moved other safety topics from Chapter 11 to publication 1756-RM012
Added information about component tracking

1756-UM543M-EN-P, May 2022

Change
Added publication to the Additional Resources table
Separated ControlLogix® and GuardLogix® K catalog numbers
Updated CIP Security™ content
Added CIP Security™ to ControlLogix® and GuardLogix® controller feature tables

Change
Added CIP Security™ considerations for the number of EtherNet/IP™ nodes
Added K controllers to the description of ControlLogix® 5580 controllers that support IEC-62443-4-2 SL 1 security requirements
Added syslog collector to controller system image
Restructured security checklists
Moved Verification of Security Implementation content to the beginning of security checklist
Changed "Studio 5000 Logix Designer® application" checklist item in Table 37 from "yes" to "may be required" for IEC-62443-4-2 SL 1 security requirements
Added FactoryTalk® Security software to Table 38 and revised details
Revised details of "Firmware update" checklist item in Table 38
Added "Syslog collector" checklist item to Table 41
Changed "Controller log" checklist item in Table 41 to "Disabled controller log auto-write" and revised details
Added information about matching firmware revisions and Trusted® slots
Changed NVS to non-volatile controller memory
Added syslog log collector to Controller Log section
Added method to disable CIP Security™ ports in FactoryTalk® Linx software
Updated general status messages for the controller

1756-UM543L-EN-P, August 2021

Change
Updated link to Logix Controller and I/O Fault Codes
Updated Conformal Coated Products statement
Updated Controller Log section
Added Controller Status messages

1756-UM543K-EN-P, August 2020

Change
Added ControlLogix® NSE, ControlLogix-XT™, and ControlLogix® Process controllers

Change
Updated safety signature definition
Updated behavior of controller status indicators while loading a project from the SD card
Added Simple Network Management Protocol (SNMP).
Added Automatic Diagnostics
Added Considerations for Communication Loss Diagnostics

1756-UM543J-EN-P, October 2019

Change
Added links to access Controller and I/O fault code information from the Knowledgebase Support Center

1756-UM543I-EN-P, March 2019

Change
Moved information on Controller and I/O fault codes to the attached spreadsheets
Added Develop Secure Applications chapter
Updated Controller webpage information

1756-UM543H-EN-P, August 2018

Change
Updated the ControlLogix® and ControlLogix-XT™ Chassis and Slots table

1756-UM543G-EN-P, July 2018

Change
Changed some remaining instances of “safety task signature” to “safety signature” throughout
Updated the Assign the Safety Network Number (SNN) section
Updated the Copy and Paste a Safety Controller Safety Network Number section
Updated the Set the SNN of a Safety I/O Device section

1756-UM543F-EN-P, February 2018

Change
Added GuardLogix® 550 controllers and Safety Information

1756-UM543E-EN-P, December 2016

Change
Updated tables with new maximum number of EtherNet/IP™ nodes that are supported in Version 30 or later
Added the 1756-IF16IH module to the list of supported HART devices

1756-UM543D-EN-P, August 2016

Change
Added the catalog numbers 1756-L81E, 1756-L82E, 1756-L84E
Added ControlFLASH™ to the Required Software section
Added the section ‘EtherNet/IP™ Network Communication Rates'
Added information on the Ethernet node counter to the section 'Nodes on an EtherNet/IP™ Network
Added the appendix ‘Security Options’

1756-UM543C-EN-P, November 2015

Change
Updated the diagram for multiple controllers in one chassis

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, 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)	Get help determining how products interact, check features and capabilities, and find associated firmware.	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 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

1756-UM543T-EN-P - December 2025
Supersedes 1756-UM543S-EN-P – November 2025