



This manual links to Logix 5000 Controller and I/O Fault Codes, publication [1756-RD001](#); download the spreadsheet now for offline access.



ControlLogix 5580 and GuardLogix 5580 Controllers

Bulletin Number 1756



Allen-Bradley

by ROCKWELL AUTOMATION

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.

	Preface	
	About This Publication	9
	Download Firmware, AOP, EDS, and Other Files	9
	Summary of Changes	9
	Additional Resources	9
	Chapter 1	
ControlLogix and GuardLogix Systems	Minimum Requirements	11
	ControlLogix Controllers	12
	ControlLogix No Stored Energy (NSE) Controllers	12
	ControlLogix XT and GuardLogix XT Controllers	12
	Process Controllers	12
	Conformal Coated Products	13
	ControlLogix Redundant Controllers	13
	ControlLogix System	13
	Standalone Controller and I/O	13
	Multiple Controllers in One Chassis	14
	Multiple Devices Connected via Multiple Networks	15
	GuardLogix System	16
	GuardLogix with Safety I/O and Integrated Safety Drives	17
	Design the System	19
	CIP Security	19
	Secure Controller Systems	19
	ControlLogix 5580 Controller Features	20
	GuardLogix 5580 Controller Features	21
	Features Supported by GuardLogix 5580 Controllers via the Safety Task	22
	Chapter 2	
Safety Concept of GuardLogix Controllers	Functional Safety Capability	23
	Safety Network Number	23
	Safety Signature	24
	Distinguish between Standard and Safety Components	24
	Controller Data-flow Capabilities	25
	Safety Terminology	26
	Chapter 3	
Connect to a Controller	Set the IP Address	27
	Requirements	27
	Other Methods to Set the IP Address	27
	Duplicate IP Address Detection	28
	Duplicate IP Address Resolution	28
	DNS Addressing	29
	Update Controller Firmware	30
	Firmware Upgrade Guidelines for Safety Controllers	30
	Determine Required Controller Firmware	31

Obtain Controller Firmware	31
Use ControlFLASH Plus or ControlFLASH Software to Update Firmware	31
Use AutoFlash to Update Firmware	32

Chapter 4

Communication Networks

Networks Available	35
EtherNet/IP Network Communication	36
EtherNet/IP Link Speeds	36
EtherNet/IP Communication Modules	39
Double Data Rate (DDR) Backplane Communication for ControlLogix Controllers	39
ControlNet Network Communication	40
GuardLogix ControlNet Example	41
ControlNet Modules	42
DeviceNet Network Communication	42
DeviceNet Bridge Module and Linking Devices	43
Connections Over DeviceNet Networks	43
Data Highway Plus (DH+) Network Communication	43
Communicate Over a DH+ Network	44
Universal Remote I/O (RIO) Communication	45
Communicate Over a Universal Remote I/O Network	46
Foundation Fieldbus Communication	47
HART Communication	48

Chapter 5

Start to Use the Controller

Create a Logix Designer Application Project	49
Additional Configuration for a GuardLogix Controller	50
Set the Safety Level for a GuardLogix Controller	50
Passwords for Safety-locking and Unlocking	51
Protect the Safety Signature in Run Mode	52
Assign the Safety Network Number (SNN)	53
Copy and Paste a Safety Controller Safety Network Number	56
Go Online with the Controller	59
Use RSWho	59
Use a Recent Communication Path	60
Additional Considerations for Going Online with a GuardLogix Controller	60
Match Project to Controller	61
Firmware Revision Matching	62
Safety Status/Faults	62
Safety Signature and Safety-locked and -unlocked Status	62
Checks for Going Online with a GuardLogix Controller	63
Download to the Controller	64
Use Who Active	64
Use the Controller Status Menu	66
Additional Considerations for Download to a GuardLogix Controller	66
Upload from the Controller	68
Use Who Active	68
Use the Controller Status Menu	69
Additional Considerations for Upload from a GuardLogix Controller	70
Choose the Controller Operation Mode	71

Use the Keyswitch to Change the Operation Mode	72
Use the Logix Designer Application to Change the Operation Mode	73
Reset Button	74
Stage 1 Reset	75
Stage 2 Reset	76
Safety Partner Reset	76

Chapter 6

Use the Secure Digital Card

Considerations for Storing and Loading a Safety Project	78
Store to the SD Card	78
Load from the SD Card	82
Controller Power-up	82
User-initiated Action	82
Other Secure Digital Card Tasks	84

Chapter 7

Manage Controller Communication

Connection Overview	85
Nodes on an EtherNet/IP Network	85
Devices Included in the Node Count	86
Devices Excluded from the Node Count	86
CIP Security Considerations	87
Controller Communication Interaction with Control Data	87
Produce and Consume (Interlock) Data	88
Requested Packet Interval (RPI) of Multicast Tags	89
Send and Receive Messages	89
Determine Whether to Cache Message Connections	90
Socket Interface	91
TLS Support	91
HTTP(S) REST API Client Support	91
Simple Network Management Protocol (SNMP)	92
Use a CIP Generic MSG to Enable SNMP on the Controller	92
Use a CIP Generic MSG to Disable SNMP on the Controller	94

Chapter 8

Standard I/O Modules

Selecting ControlLogix I/O Modules	97
Electronic Keying	97
Local I/O Modules	98
Add Local I/O to the I/O Configuration	99
Remote I/O Modules	102
Add Remote I/O to the Ethernet Port on the Controller	103
Add Remote I/O to a Local Communication Module	105
Add to the I/O Configuration While Online	108
Modules that Can be Added While Online	109
Determine When Data is Updated	109
Input Data Update Flowchart	110
Output Data Update Flowchart	111

Safety I/O Devices**Chapter 9**

Add Safety I/O Devices.....	113
Configure Safety I/O Devices.....	113
Use Network Address Translation (NAT) with CIP Safety Devices.....	115
Set the SNN of a Safety I/O Device	116
Change a Safety I/O Device SNN	117
Copy and Paste a Safety I/O Device SNN.....	118
Safety I/O Device Signature.....	120
Configuration via the Logix Designer Application.....	120
Different Configuration Owner (Data-only Connection)	121
Reset Safety I/O Device to Out-of-box Condition	121
I/O Device Address Format	122
Monitor Safety I/O Device Status.....	122
Replace a Safety I/O Device.....	122
Configuration Ownership	122
Safety I/O Replacement Options	123

Develop Standard Applications**Chapter 10**

Elements of a Control Application.....	129
Tasks	130
Task Priority	132
Programs	133
Scheduled and Unscheduled Programs.....	134
Routines	135
Parameters and Local Tags.....	136
Program Parameters	136
Programming Languages.....	137
Add-On Instructions.....	137
Extended Properties	138
Access the Module Object from an Add-On Instruction	139
Monitor Controller Status.....	140
Monitor I/O Connections	140
Determine If I/O Communication Has Timed Out	141
Determine if I/O Communication to a Specific I/O Module has Timed Out.....	141
Automatic Handling of I/O Module Connection Faults.....	141
Sample Controller Projects	142

Develop Safety Applications**Chapter 11**

Safety Overview	143
Program Safety Applications.....	144

Develop Secure Applications**Chapter 12**

Controller Security Features	146
Security Checklists.....	147
Configure Trusted Slots on the Controller	151
Restrict Communication except Through Selected Slots	151
Select Slots	152
Configure User-definable Major Faults	152

Create a Fault Routine	152
Configure the Program to Use the Fault Routine	152
Jump to the Fault Routine	153
License-based Source and Execution Protection	153
Enable License-based Protection	154
Configure Change Detection	156
Configure Component Tracking	158
Configure Controller Logging	158
Disable the Controller Ethernet Port	159
Disable the Ethernet Port on the Port Configuration Tab	159
Disable the Ethernet Port with an MSG Instruction	160
Disable the Controller CIP Security Ports	162
Use the Disable CIP Security Checkbox in FactoryTalk Linx	162
Use a CIP Generic MSG Instruction in the Logix Designer Application	163
Disable the Controller USB Port	165
Disable the Controller SD Card	166
Disable the 4-character Status Display	167
Disable All Categories of Messages	168
Disable Individual Categories of Messages	170
Disable Controller Webpages	172
Studio 5000 Logix Designer Application Version 33 or Later	172
Studio 5000 Logix Designer Application Version 32 or Earlier	172
Controller Web Page Default Settings	173
Use a CIP Generic MSG to Disable the Controller Webpages	173
Use a CIP Generic MSG to Enable the Controller Webpages	175

Chapter 13

Develop Motion Applications

Motion Overview	177
Program Motion Control	178
Obtain Axis Information	179

Chapter 14

Troubleshoot the Controller

Automatic Diagnostics	181
Considerations for Communication Loss Diagnostics	182
Controller Diagnostics with the Logix Designer Application	182
I/O Module Properties	183
Notification in the Tag Monitor	185
Enable Major Fault on Controller	185
Port Diagnostics	187
Advanced Time Sync	189
Controller Diagnostics with Linx-based Software	191
Controller Webpages	193
Home Webpage	194
Faults Webpage	195
Tasks Webpage	196
Browse Chassis Webpage	197

Status Indicators	Appendix A
	Status Display and Indicators 199
	General Status Messages..... 200
	GuardLogix Status Messages..... 201
	Safety Partner Status Messages 201
	Fault Messages..... 202
	Major Fault Messages..... 202
	I/O Fault Codes..... 203
	Controller Status Indicators..... 203
	RUN Indicator 203
	FORCE Indicator 203
	SD Indicator..... 204
	OK Indicator 204
	Safety Partner OK Indicator..... 204
	EtherNet/IP Indicators..... 205
	Thermal Monitoring and Thermal Fault Behavior 206
Change Controller Type	Appendix B
	Change from a Standard to a Safety Controller 207
	Change from a Safety to a Standard Controller 208
	Change Safety Controller Types 208
History of Changes	Appendix C
 209
	Index 213

About This Publication

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 Controller Systems Safety Reference Manual, publication 1756-RM012.

Download Firmware, AOP, EDS, and Other Files

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.

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
Added catalog number 1756-L85ES	11, 21, 39, 85
Revised the Safety Signature section in Chapter 2	24
Updated controller Safety tab screen shots	throughout
Updated Safety I/O Replacement Options section	123
Added statement about the status of the Enable Controller Web Pages checkbox	172

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
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.
Technical Data	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 ControlLogix chassis.
	Replacement door labels for the 1756 I/O modules, publication IASIMP-SP021
	Contains door labels for the 1756 I/O modules that are available to print.
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.
Technical Data	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
Technical Data	Provides specifications for ControlLogix power supplies.
	1756 ControlLogix Chassis Specifications Technical Data, publication 1756-TD006
	Provides specifications for ControlLogix chassis.

Resource		Description
Networks (ControlNet®, DeviceNet®, EtherNet/IP™)	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 network.
	ControlNet Network Configuration User Manual, publication CNET-UM001	Provides information about ControlNet networks.
	DeviceNet Media Design Installation Guide, publication DNET-UM072	Provides information about DeviceNet networks.
Safety application requirements	GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems 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.
Motion	Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003	Details how to design your ControlLogix system for Integrated Motion on the EtherNet/IP network applications.
	Integrated Motion on the EtherNet/IP Network Reference Manual, publication MOTION-RM003	Detailed information on axis control modes and attributes for Integrated Motion on EtherNet/IP networks.
	Motion Coordinate System User Manual, publication MOTION-UM002	Details how to create and configure a coordinated motion application system.
	SERCOS and Analog Motion Configuration and Startup User Manual, publication MOTION-UM001	Details how to configure a sercos motion application system.
Design Considerations	Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides information to help design and plan Logix 5000 systems.
	High Availability System Reference Manual, publication HIGHAV-RM002	Provides information to help design and plan high availability systems.
	System Security Design Guidelines Reference Manual, 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.
	FOUNDATION Fieldbus Design Considerations Reference Manual, PROCES-RM005	This document provides design choices and best practices for implementing a FOUNDATION Fieldbus network with the 1788-EN2FFR or 1788-CN2FFR linking devices.
	Using Logix 5000 Controllers as Masters or Slaves on Modbus Application Solution, publication CIG-AP129	For more information about using Modbus sample programs.
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, handle 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 on the GuardLogix safety application instruction set.
Product Certifications	Product Certifications website, rok.auto/certifications .	Provides declarations of conformity, certificates, and other certification details.

ControlLogix and GuardLogix Systems

This chapter describes features of the following ControlLogix® 5580 and GuardLogix® 5580 controllers.

Controller Type	Cat. No.
Standard controllers	1756-L81E, 1756-L82E, 1756-L83E, 1756-L84E, 1756-L85E
Standard controllers with conformal coating	1756-L81EK, 1756-L82EK, 1756-L83EK, 1756-L84EK, 1756-L85EK
No Stored Energy (NSE) controllers	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE
ControlLogix-XT™ controllers	1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT
Process controllers	1756-L81EP, 1756-L83EP, 1756-L85EP
GuardLogix controllers	1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L85ES ⁽¹⁾ , 1756-L8SP
GuardLogix XT controllers	1756-L81EXTS, 1756-L82EXTS, 1756-L83EXTS, 1756-L84EXTS, 1756-L8XTSP
GuardLogix controllers with conformal coating	1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8SPK

(1) Supported by Studio 5000 Logix Designer® version 36 or later.

Minimum Requirements

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers have these minimum requirements:

- ControlLogix chassis, series C (series B chassis function within a derated temperature range)
- ControlLogix chassis 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 connections or safety logic are required for your application, then you must use any GuardLogix 5580 controller.
- GuardLogix project editing requires Studio 5000 Logix Designer Professional, Full Edition, or a licensed GuardLogix Safety Editor.

ControlLogix Controllers

The controllers are available with different functionality based on your application.

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 μ J or less in 40 seconds.

If your application requires the NSE controller to deplete its residual stored energy to 400 μ J 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 μ J 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.

ControlLogix XT and GuardLogix XT Controllers

The ControlLogix XT and GuardLogix XT controllers function in the 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.

The ControlLogix 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.

Conformal Coated Products



ATTENTION: ControlLogix 5580 controllers that are listed on [page 11](#) that end with a 'K' or 'XT' are shipped with port protection plugs installed to provide a layer of protection from corrosive atmospheres. Port plugs must remain installed in unused ports at all times during storage and operation for the product to meet its corrosive atmosphere rating. If temporary access is required, plugs can be removed, and should be reinserted after temporary access is complete.

ControlLogix Redundant Controllers

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 System Reference Manual, publication [HIGHAV-RM002](#)
- ControlLogix 5580 Redundant Controller User Manual, publication [1756-UM015](#)

ControlLogix System

Applies to these controllers:

ControlLogix 5580

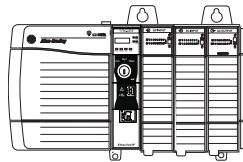
The ControlLogix system is chassis-based, which provides options for configuring a variety of communications and I/O capabilities. The ControlLogix controllers support multiple programming languages that enable sequential, process, motion, and drive control.

A variety of 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 assembled in one chassis.

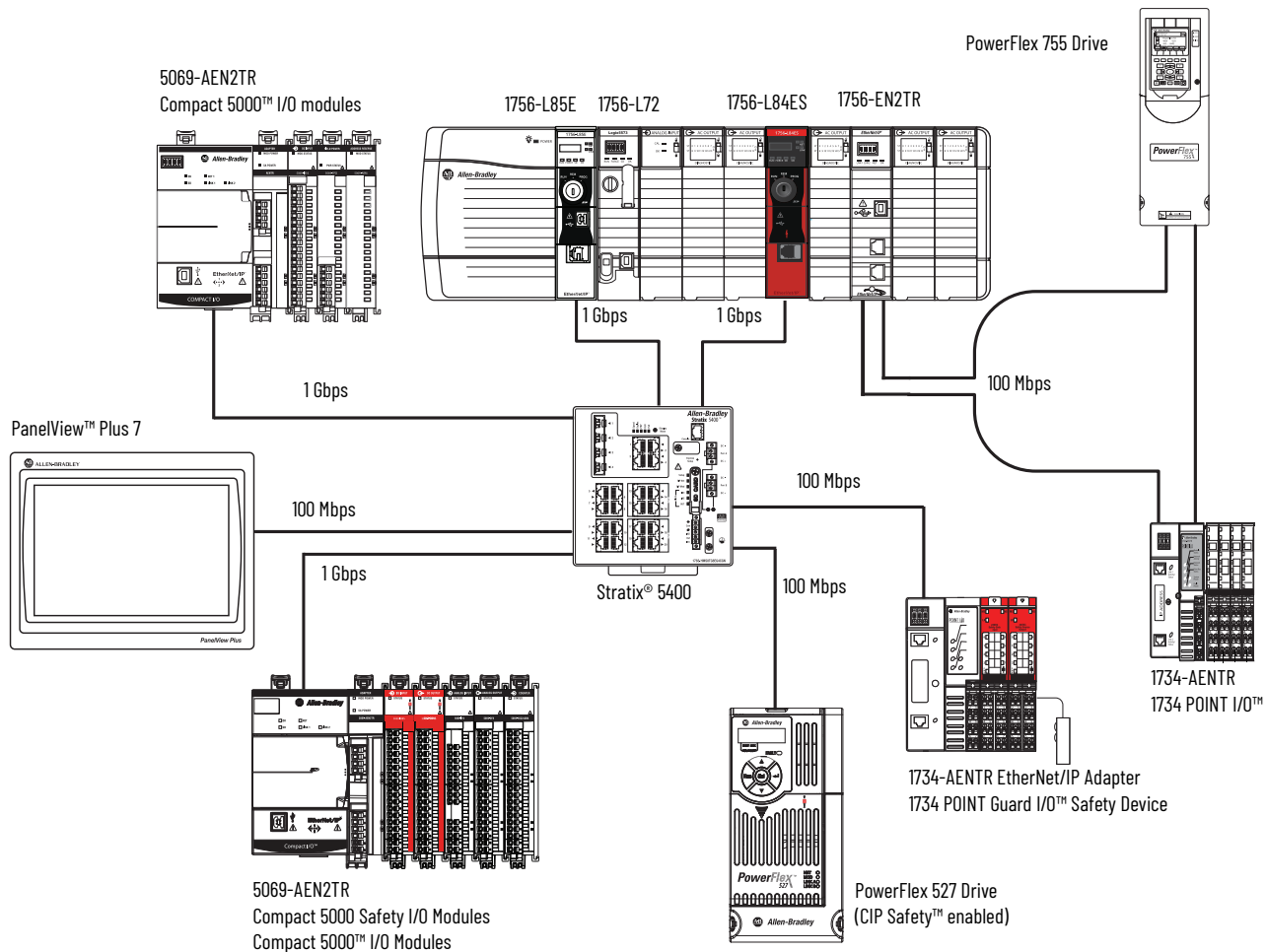
Figure 1 - Standalone Controller and I/O



Multiple Controllers in One Chassis

You can use multiple controllers in one ControlLogix chassis. This example shows a ControlLogix 5580 controller (slot 0) connected directly to the EtherNet/IP™ network, a ControlLogix 5570 controller (slot 1) connected to the network through a 1756-EN2TR module (slot 7), and a 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

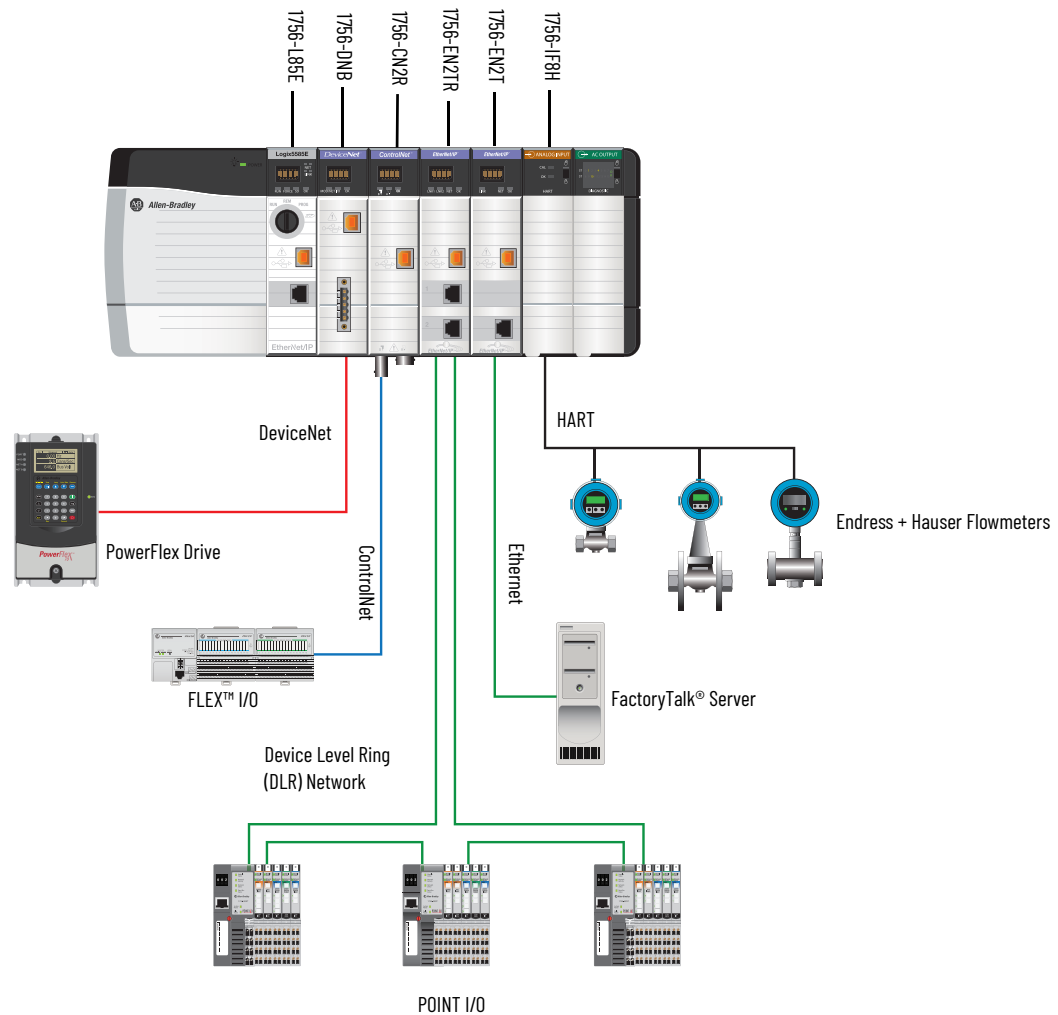
You cannot bridge through the Ethernet (front) port of another controller to add remote I/O.

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 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

Applies to these controllers:

GuardLogix 5580

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).

For a GuardLogix controller, you can interface to local standard I/O in the backplane via standard tasks while you interface with remote safety I/O through the EtherNet/IP port.

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 installed, you can achieve SIL 3/PLe (Category 4) capability.

IMPORTANT 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)

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 key switch 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.

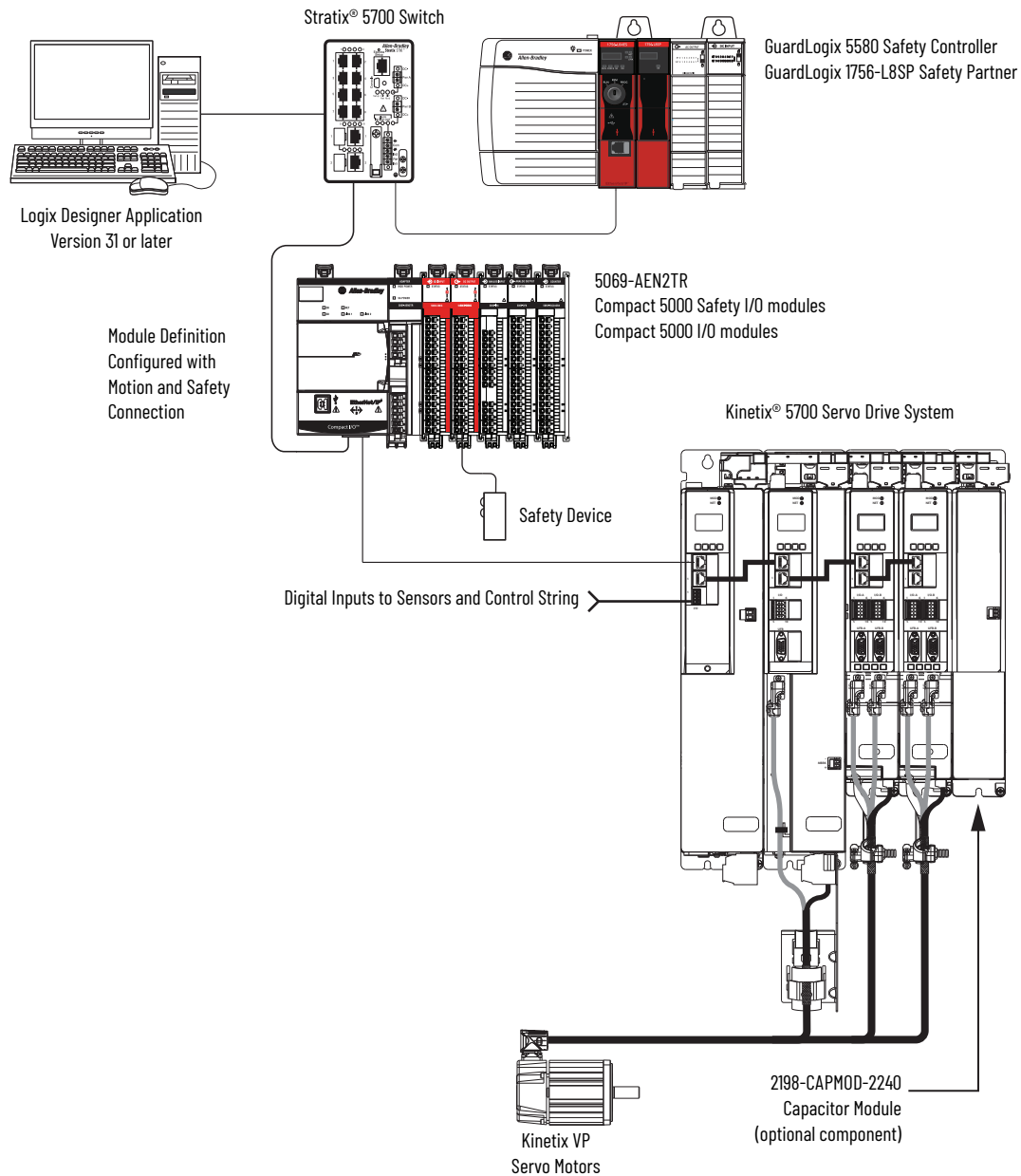
For information on Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

GuardLogix with Safety I/O and Integrated Safety Drives

In this example, a single 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.

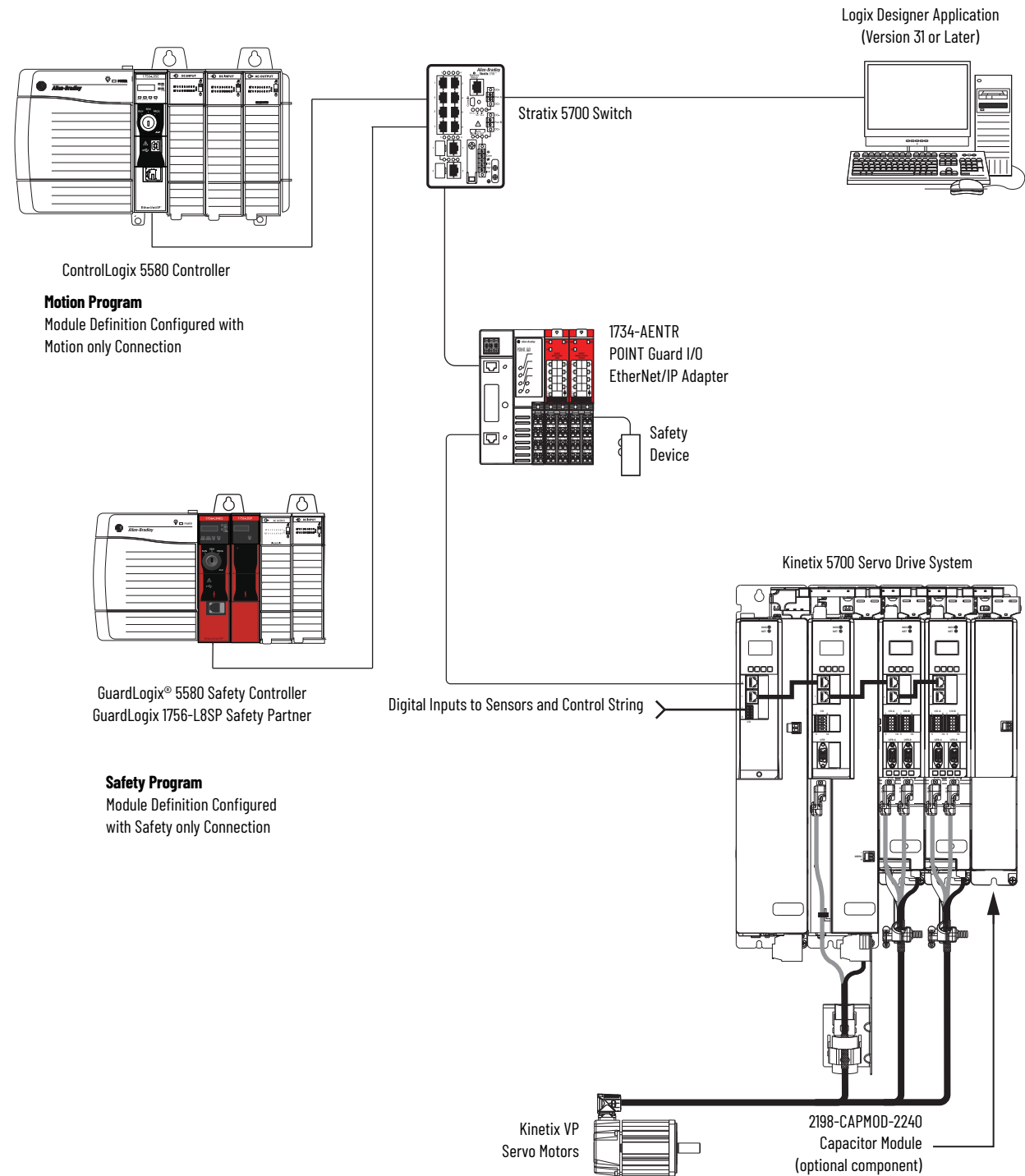
Figure 4 - Motion and Safety Configuration (Single Controller)



In this 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 the motion-only connection can be made by either a standard or a safety controller.

Figure 5 - Motion and Safety Configuration (Multiple Controllers)



Design the System

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 have 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](#)

CIP Security

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 CIP Security:

- FactoryTalk® Policy Manager software (includes FactoryTalk System Services, version 6.20 or later)
- FactoryTalk Linx software, version 6.11 or later (lets workstation software communicate securely using CIP Security)
- Studio 5000 Logix Designer application, version 31 or later

This application is required to interface with CIP Security-enabled Logix controllers. The minimum application version varies by controller product family.

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:

- The website is available at: <https://www.rockwellautomation.com/en-us/capabilities/industrial-security/security-products/cip-security.html>.
- CIP Security with Rockwell Automation Products Application Technique, publication [SECURE-AT001](#).

Secure Controller Systems

The ControlLogix 5580 controller, firmware revision 32, supports IEC-62443-4-2 SL 1 requirements. For security features and system requirements, see [Develop Secure Applications on page 145](#).

ControlLogix 5580 Controller Features

[Table 1](#) lists the system, communication, and programming features available with ControlLogix 5580 controllers.

Table 1 - ControlLogix 5580 Controller Features

Feature	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, max ⁽¹⁾	60 nodes ⁽³⁾ 100 nodes ⁽⁴⁾	80 nodes ⁽³⁾ 175 nodes ⁽⁴⁾	100 nodes ⁽²⁾ 250 nodes ⁽⁴⁾	150 nodes ⁽³⁾ 250 nodes ⁽⁴⁾	300 nodes ⁽⁵⁾
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	<ul style="list-style-type: none"> • EtherNet/IP • ControlNet • DeviceNet • Data Highway Plus™ • Remote I/O • SynchLink™ • Third-party process and device networks 				
CIP Security	See CIP Security on page 19 .				
Controller tasks	<ul style="list-style-type: none"> • 32 tasks • 1000 programs/task • Event tasks: all event triggers 				
Integrated motion	<ul style="list-style-type: none"> • Integrated Motion on the EtherNet/IP network • Sercos interface⁽⁶⁾ • Analog options⁽⁶⁾: <ul style="list-style-type: none"> - Encoder input - Linear displacement transducer (LDT) input - Serial Synchronous Input (SSI) 				
Programming languages	<ul style="list-style-type: none"> • Ladder Diagram (LD) • Structured Text (ST) • Function Block Diagram (FBD) • Sequential Function Chart (SFC) 				

(1) A node is an EtherNet/IP device that you add directly to the I/O configuration and counts toward the controller node limits.

(2) Logix Designer application versions 28 and 29.

(3) Logix Designer application version 29.

(4) Logix Designer application version 30 or later.

(5) Logix Designer application version 28 or later.

(6) Logix Designer application version 31 or later.

GuardLogix 5580 Controller Features

[Table 2](#) lists the system, communication, and programming features available with GuardLogix 5580 controllers.

Table 2 - GuardLogix 5580 Controller Features

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 ⁽¹⁾
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, max	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	<ul style="list-style-type: none"> EtherNet/IP (1756-EWEB cannot be used for safety connections) Support for Network address translation (NAT) ControlNet DeviceNet Data Highway Plus Remote I/O SynchLink Third-party process and device networks 				
CIP Security	See CIP Security on page 19 .				
Controller tasks	<ul style="list-style-type: none"> 31 standard tasks, 1 safety task 1000 programs/task Event tasks: all event triggers 				
Integrated motion	Integrated motion is supported in standard task only. <ul style="list-style-type: none"> Integrated Motion on the EtherNet/IP network Sercos interface Analog options: <ul style="list-style-type: none"> Encoder input Linear displacement transducer (LDT) input Serial Synchronous Input (SSI) 				
Programming languages	<ul style="list-style-type: none"> For the safety task, GuardLogix controllers support Ladder Diagram only. For standard tasks, GuardLogix controllers support: <ul style="list-style-type: none"> Ladder Diagram (LD) Structured Text (ST) Function Block Diagram (FBD) Sequential Function Chart (SFC) 				
Integrated safety	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Data access control Firmware supervisor Secure Digital (SD) card Safety Connections Standard Connections 				

⁽¹⁾ Supported by Logix Designer version 36 or later.

Features Supported by GuardLogix 5580 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 this table.

Table 3 - Safety Task Features

Feature	Studio 5000 Logix Designer Application, 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 ⁽¹⁾	—	X
Function block diagrams (FBD)	—	X
Integrated motion	X ⁽²⁾	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
Online export of program components	X	X
Sequential function chart (SFC) routines	—	X
Structured Text (ST)	—	X

(1) 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.

(2) Limited to the use of Drive Safety Instructions with Kinetix 5700 ERS4 drives.

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 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.

Safety Concept of GuardLogix Controllers

Functional Safety Capability

Applies to these controllers:

GuardLogix 5580

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 the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [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

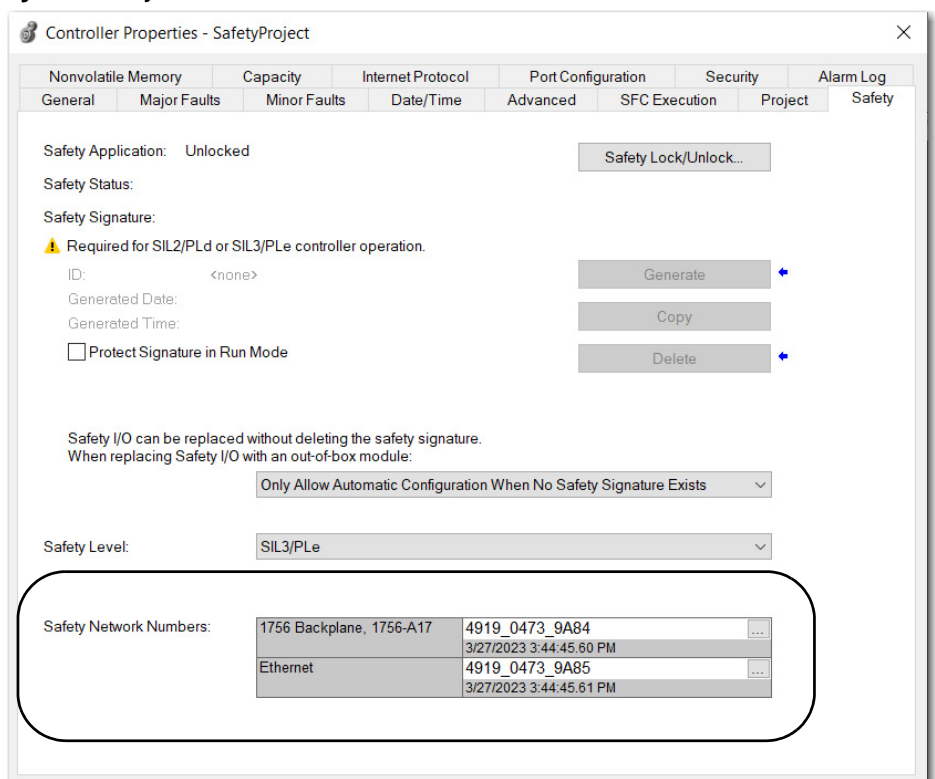
The safety network number (SNN) uniquely identifies CIP Safety™ subnets within a routable safety network. The combination of the SNN + Node Address uniquely identifies each CIP Safety port on each device in the routable safety network. GuardLogix 5580 controllers require two SNNs:

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

For an explanation of SNNs, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

To assign SNNs, see [Assign the Safety Network Number \(SNN\) on page 53](#).

Figure 6 - Safety Network Numbers



Safety Signature

The GuardLogix system uses a safety signature to verify 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 ID--A 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.

Figure 7 - Safety Signature

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

For details about the safety signature, safety signature elements, and how to generate the safety signature and the Safety Signature report, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

Distinguish between Standard and Safety Components

Slots of a GuardLogix system chassis that are not used by the safety function can be populated with other ControlLogix® modules that are certified to the Low Voltage and EMC Directives. See the Rockwell Automation Product Certifications page ([rok.auto/certifications](#)) to find the CE certificate for the ControlLogix Product Family, and determine the modules that are certified.

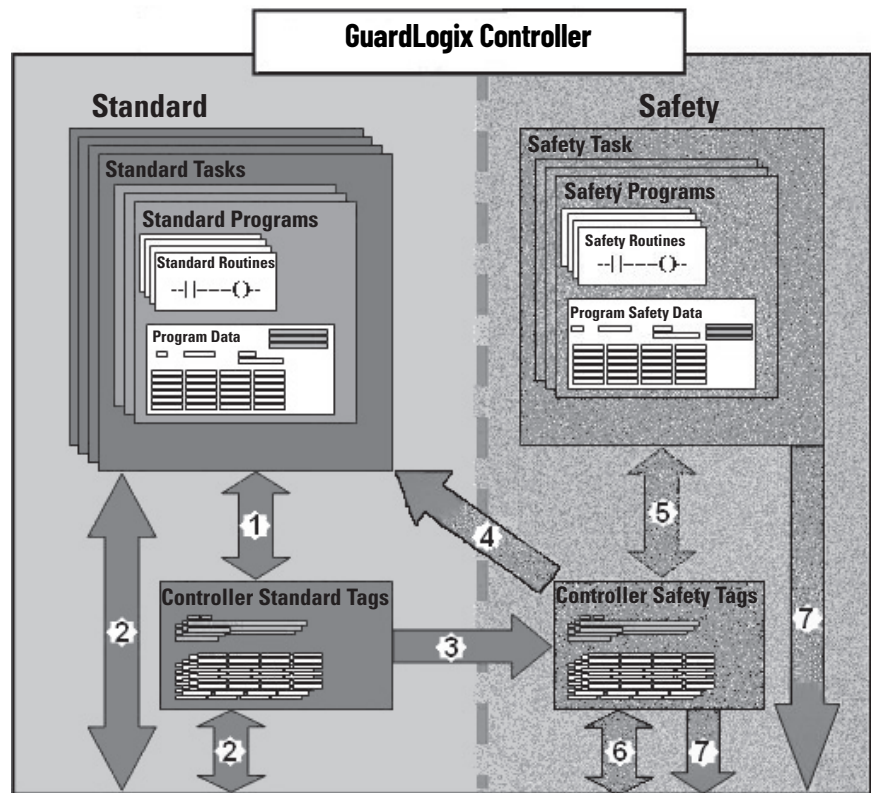
You must create and document a clear, logical, and visible distinction between the safety and standard portions of the controller project. As part of this distinction, the Studio 5000 Logix Designer® application features safety identification icons to identify the safety task, safety programs, safety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

The following illustration explains the standard and safety data-flow capabilities of the GuardLogix controller.

Figure 8 - Data-flow Capabilities



No.	Description
1	Standard tags and logic behave the same way that they do in a standard ControlLogix controller.
2	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.
3	GuardLogix controllers 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 in to 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 must not be used to control a SIL 2/PLD or SIL 3/PLC output directly.
4	Controller-scoped safety tags can be read directly by standard logic.
5	Safety tags can be read or written by safety logic.
6	Safety tags can be exchanged between safety controllers over Ethernet or ControlNet® networks, including 1756 and 5069 GuardLogix controllers.
7	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/PLC data.

Safety Terminology

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

Table 4 - 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.
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 a Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Before you can connect to the controller through the Ethernet or USB port, you must configure the EtherNet/IP™ or USB driver in Linux-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.

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

Set the IP Address

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.

Requirements

To set the IP address, have the following:

- EtherNet/IP or USB drivers 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

Other Methods to Set the IP Address

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

- BOOTP/DHCP utility
- RSLinx® Classic software
- Studio 5000 Logix Designer® application

For more information on how to use these methods, see 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 solid 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.

Duplicate IP Address Detection Conditions	Resolution Process
<ul style="list-style-type: none"> • Both devices support duplicate IP address detection. • Second device is added to the network after the first device is operating on the network. 	<ol style="list-style-type: none"> 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. See the EtherNet/IP Network Device User Manual, publication ENET-UM006.
<ul style="list-style-type: none"> • Both devices support duplicate IP address detection • Both devices were powered up at approximately the same time. 	<p>Both EtherNet/IP devices enter Conflict mode. To resolve this conflict, follow these steps:</p> <ol style="list-style-type: none"> 1. Assign a new IP address to the controller. Set the Network IP Address with the BootP DHCP EtherNet/IP Commissioning Tool. See the EtherNet/IP Network Device User Manual, publication ENET-UM006. 2. Cycle power to the other device.
One device supports duplicate IP address detection and a second device does not	<ol style="list-style-type: none"> 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. See the EtherNet/IP Network Device User Manual, publication ENET-UM006.

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.

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	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)
------------------	---

IMPORTANT	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.
------------------	---

Update Controller Firmware

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

To update your controller firmware, complete these tasks:

- [Determine Required Controller Firmware](#)
- [Obtain Controller Firmware](#)
- [Use ControlFLASH Plus or ControlFLASH Software to Update Firmware](#) or [Use AutoFlash to Update Firmware](#)

Firmware Upgrade Guidelines for Safety Controllers

IMPORTANT Safety Consideration

You cannot update a controller that is safety locked.

The IEC 61508 functional safety standard requires impact analysis before upgrading or modifying 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 of the 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 GuardLogix controller systems are certified for use in safety applications. As part of the certification process, Rockwell Automation tests the safety-related firmware functions (for example 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 upgrade.
 - 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 re-generate the safety signature as part of the firmware upgrade process. Use the online and offline edit process described in the safety reference manual for your controller.

For more controller-specific information, see the GuardLogix 5580 and Compact GuardLogix 5380 Safety Reference Manual, publication [1756-RM012](#).

IMPORTANT GuardLogix 5580 controllers have a different compiler than earlier controllers. You must revalidate that applications on earlier controllers compile correctly on GuardLogix 5580 controllers.

For product change management guidelines and definitions of how Rockwell Automation manages product versions, see System Security Design Guidelines Reference Manual, publication [SECURE-RM001](#).

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 identified during the impact analysis and determine what additional testing is necessary.
3. Perform the online and offline edit process 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.

Determine Required Controller Firmware

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

The firmware major revision level must match the software major version level. For example, if the controller firmware revision is 31.xxx, you must use Logix Designer application, version 31.

IMPORTANT Safety Consideration
For a GuardLogix® 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:

- Firmware is packaged as part of the Studio 5000 Logix Designer application installation.

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. For more information, see the next bullet.

- From the Rockwell Automation Product Compatibility and Download Center (PCDC). You can check for available 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 PCDC at rok.auto/pcdc.

Use ControlFLASH Plus or ControlFLASH Software to Update Firmware

For information on how to download, install, and use ControlFLASH Plus or ControlFLASH™ software, see:

- ControlFLASH Plus Quick Start Guide, publication [CFP-QS001](#)
- ControlFLASH Firmware Upgrade Kit User Manual, publication [1756-UM105](#)

Use AutoFlash to Update Firmware

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

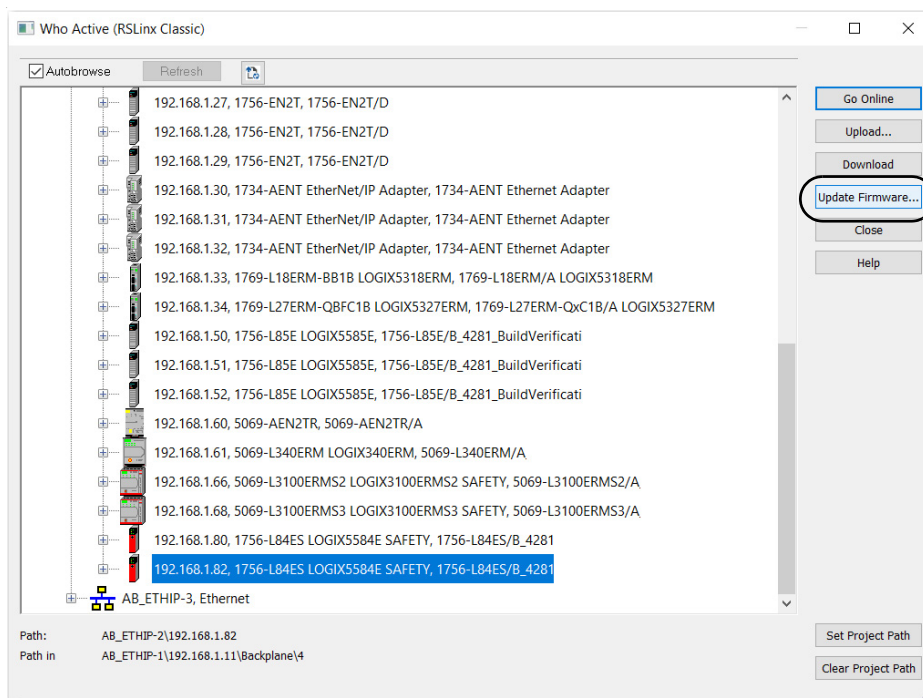


ATTENTION: If the Secure Digital Card is locked and set to load on power-up, then this update can be overwritten by firmware on the SD card.

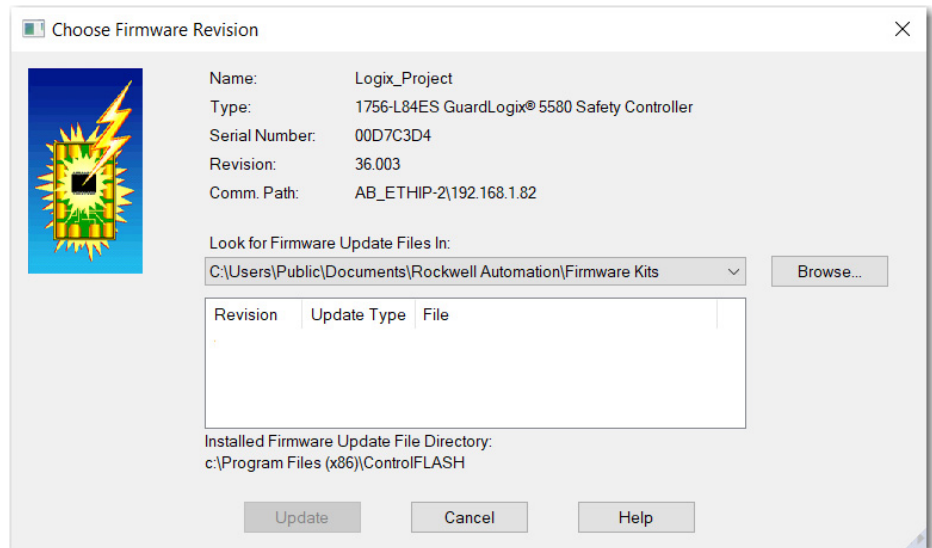
1. Verify that the network connection is made and your network driver is configured in Linx-based communication software.
2. Use the Logix Designer application to create a controller project.
3. On the Path bar, click Who Active.



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



5. On the Choose Firmware Revision dialog box, browse to the location of the firmware files (C:\Program Files (x86)\ControlFLASH).
6. Select the firmware revision, and click Update.



7. On the Confirmation dialog box, click Yes.
8. On 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 progress dialog box closes.

Notes:

Communication Networks

Several communication networks are available.

Networks Available

[Table 5](#) describes typical application features that are used with ControlLogix® and GuardLogix® systems, and lists the networks available to support such application features.

Table 5 - Applications and Supported Networks

Application Features	ControlLogix and GuardLogix Supported Networks for Standard Communications	GuardLogix Supported Networks for CIP Safety™ Communications
Integrated Motion ⁽¹⁾	EtherNet/IP™	EtherNet/IP
Time synchronization	EtherNet/IP	EtherNet/IP
Control of distributed I/O	<ul style="list-style-type: none"> EtherNet/IP DeviceNet® ControlNet® Foundation Fieldbus HART Universal remote I/O 	Time synchronization does not use the safety protocol.
Produce/consume data between controllers	<ul style="list-style-type: none"> EtherNet/IP ControlNet 	<ul style="list-style-type: none"> EtherNet/IP ControlNet
Messaging to and from other devices, including access to the controller via the Studio 5000 Logix Designer® application	<ul style="list-style-type: none"> EtherNet/IP ControlNet DeviceNet (only to devices) Data Highway Plus™ (DH+™) DH-485 	Messaging does not use the safety protocol.

(1) The controllers also support analog and Sercos motion interfaces. For more information, See [Develop Motion Applications on page 177](#).

For more information about using EtherNet/IP modules, see these publications:

- EtherNet/IP Modules in Logix 5000 Control Systems User Manual, publication [ENET-UM001](#)
- EtherNet/IP Communication Modules in 5000 Series Systems, publication [ENET-UM004](#)

For more information about network design, see these publications;

- Ethernet Design Considerations Reference Manual, publication [ENET-RM002](#).
- ControlNet Network Configuration User Manual, publication [CNET-UM001](#)
- DeviceNet Media Design Installation Guide, publication [DNET-UM072](#)
- FOUNDATION Fieldbus Design Considerations Reference Manual, publication [PROCES-RM005](#)

EtherNet/IP Network Communication

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The EtherNet/IP network offers a full suite of 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 well-accepted standards provides the capability that is required to support information data exchange and control applications.

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

EtherNet/IP Link Speeds

The controller supports 10 Mbps/100 Mbps/1 Gbps EtherNet/IP link speeds.

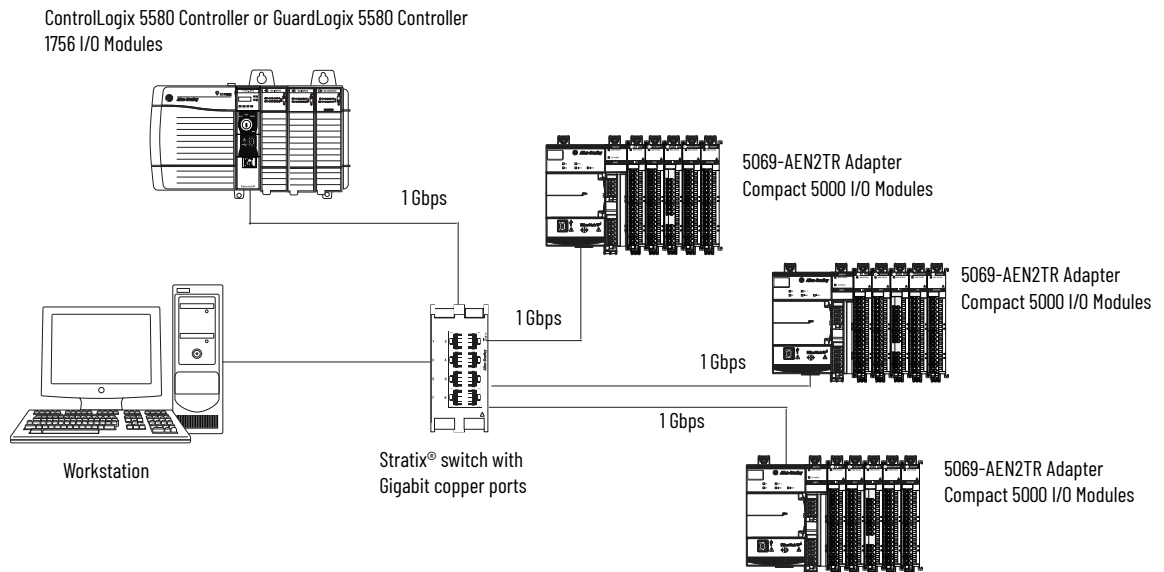
Network performance in a the controller system is optimal if the 1 Gbps link speed is used. However, legacy Ethernet devices do not support the 1 Gbps link speed. Instead, they support a maximum rate of 100 Mbps.

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.

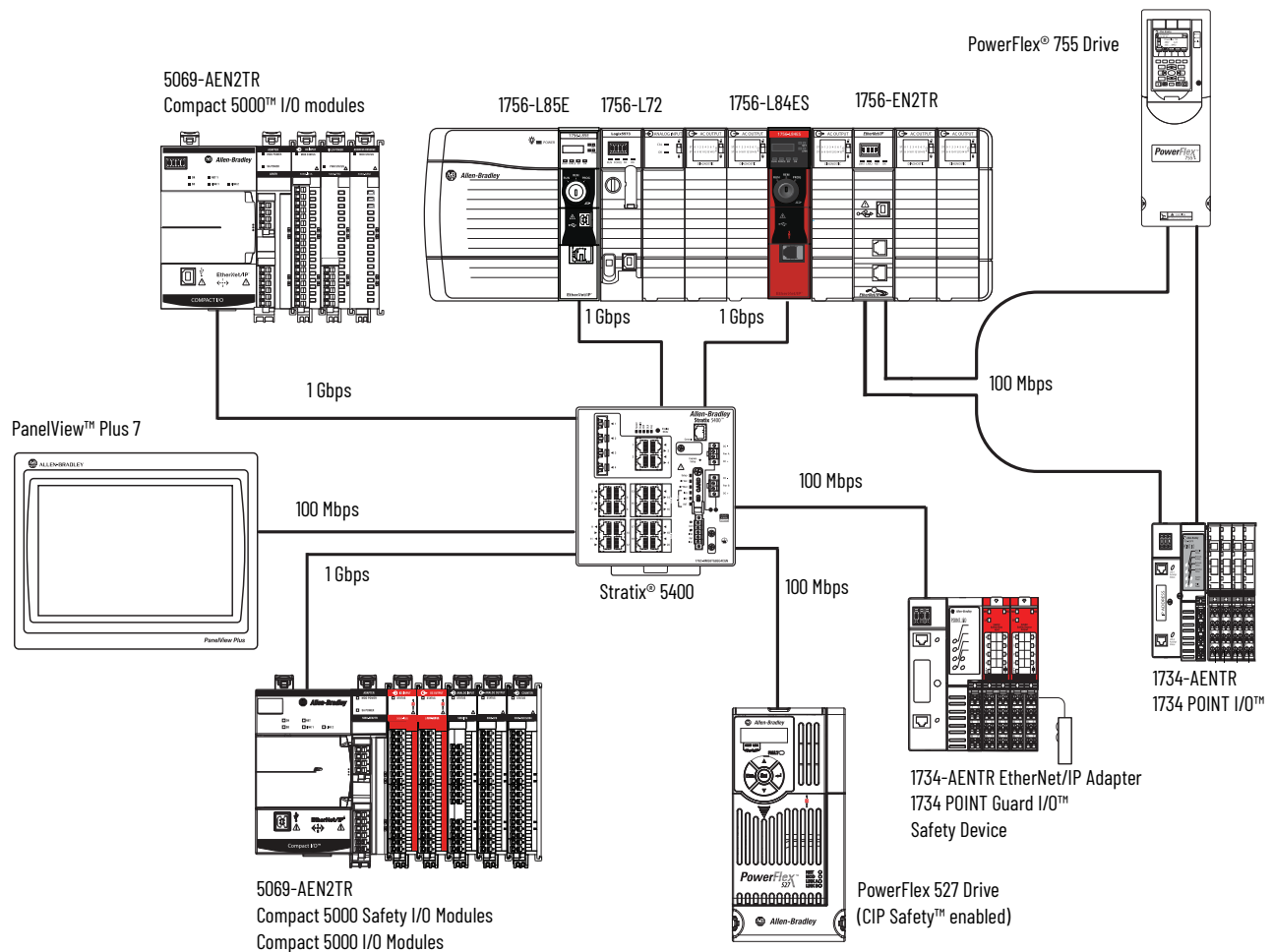
When you design a controller system and consider using the 1 Gbps rate on the controller, remember the following:

- You can use the 1 Gbps link 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.

Figure 9 - 1 Gbps EtherNet/IP Network Example



- You can use the 1 Gbps link 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 link speeds within a single DLR ring or linear network.

IMPORTANT

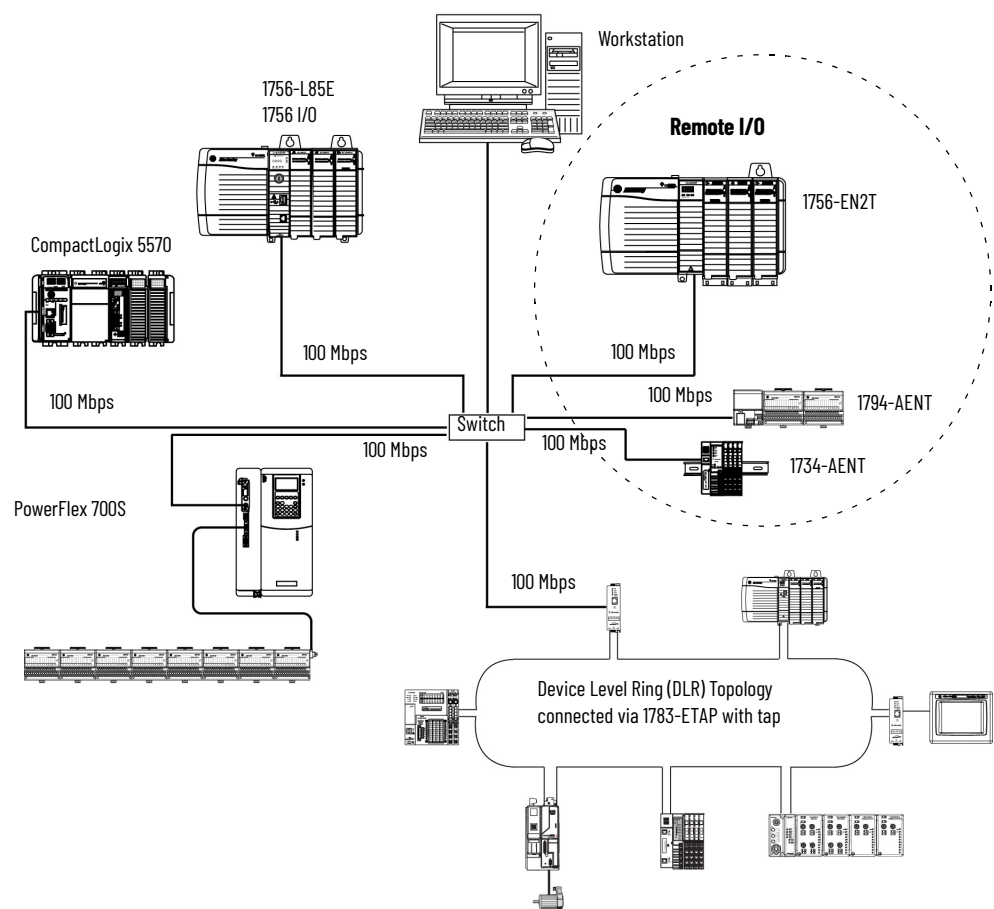
Do not use different link speeds on device ports in the same EtherNet/IP network without a managed switch.

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 5580/GuardLogix 5580 Controllers
- CompactLogix™ 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.

Figure 10 - 100 Mbps EtherNet/IP Network Example With An Unmanaged Switch



EtherNet/IP Communication Modules

For EtherNet/IP network communication, you have several modules to choose from. [Table 6](#) lists modules and their primary features.

For more information, see the 1756 ControlLogix Communication Modules Specifications Technical Data, publication [1756-TD003](#).

Table 6 - EtherNet/IP Communication Modules

Module	Is used to
1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EP, 1756-L81ES, 1756-L81ESK, 1756-L81EXT, 1756-L81EXTS, 1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82ES, 1756-L82ESK, 1756-L82EXT, 1756-L82EXTS, 1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EP, 1756-L83ES, 1756-L83ESK, 1756-L83EXT, 1756-L83EXTS, 1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84ES, 1756-L84ESK, 1756-L84EXT, 1756-L84EXTS, 1756-L85E, 1756-L85ES, 1756-L85EK, 1756-L85E-NSE, 1756-L85EP, 1756-L85EXT	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • 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 link speeds.
1756-EN2T, 1756-EN2TK, 1756-EN2TXT	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • Communicate with distributed I/O modules and other EtherNet/IP devices. • Bridge 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	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Support communication for a single-fault tolerant Device Level Ring (DLR) network. • Support a linear topology. • 1756-EN2TRXT operates in extreme environments with -25...70 °C (-13...158 °F) temperatures.
1756-EN2F, 1756-EN2FK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Connect fiber media by an LC fiber connector on the module.
1756-EN2TP, 1756-EN2TPK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Support Parallel Redundancy Protocol (PRP).
1756-EN3TR, 1756-EN3TRK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2TR modules. • Extended Integrated Motion on EtherNet/IP network. • Support as many as 128 motion axes.
1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN3TR modules. • Support as many as 256 motion axes. • Support a 1 Gbps communication rate. • Help to secure access to a control system from within the plant network.
1756-ENBT, 1756-ENBTK	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • Communicate with distributed I/O modules and other EtherNet/IP devices. • Bridge messages over an EtherNet/IP network.
1756-EN2TSC	<ul style="list-style-type: none"> • Perform the same functions as a 1756-ENBT module with twice the capacity for more demanding applications. • Help to secure access to a control system from within the plant network.
1756-EWEB, 1756-EWEBK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-ENBT modules. • Provide 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.

Double Data Rate (DDR) Backplane Communication for ControlLogix Controllers

The controllers provides double data rate capabilities across the ControlLogix backplane.

ControlNet Network Communication

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 dependable, synchronized, and coordinated real-time performance.

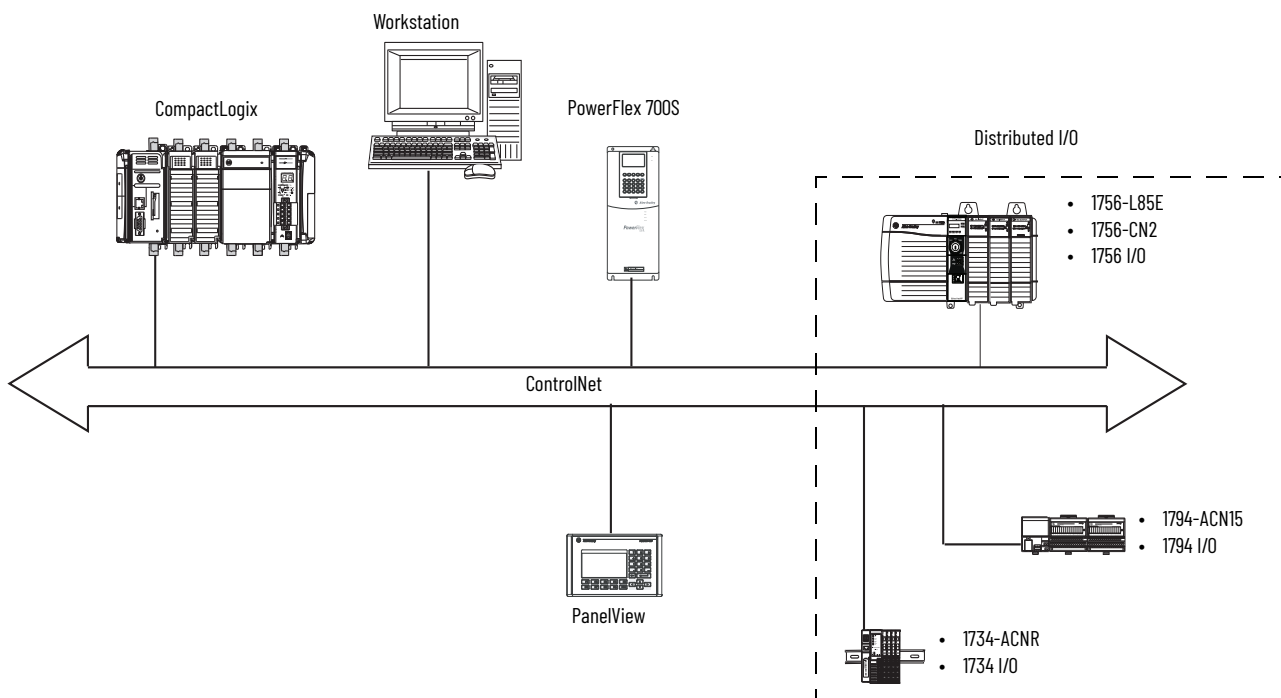
The ControlNet network often functions as the following:

- 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 example in [Figure 11](#), these actions occur via 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.

Figure 11 - ControlNet Network Overview



GuardLogix ControlNet Example

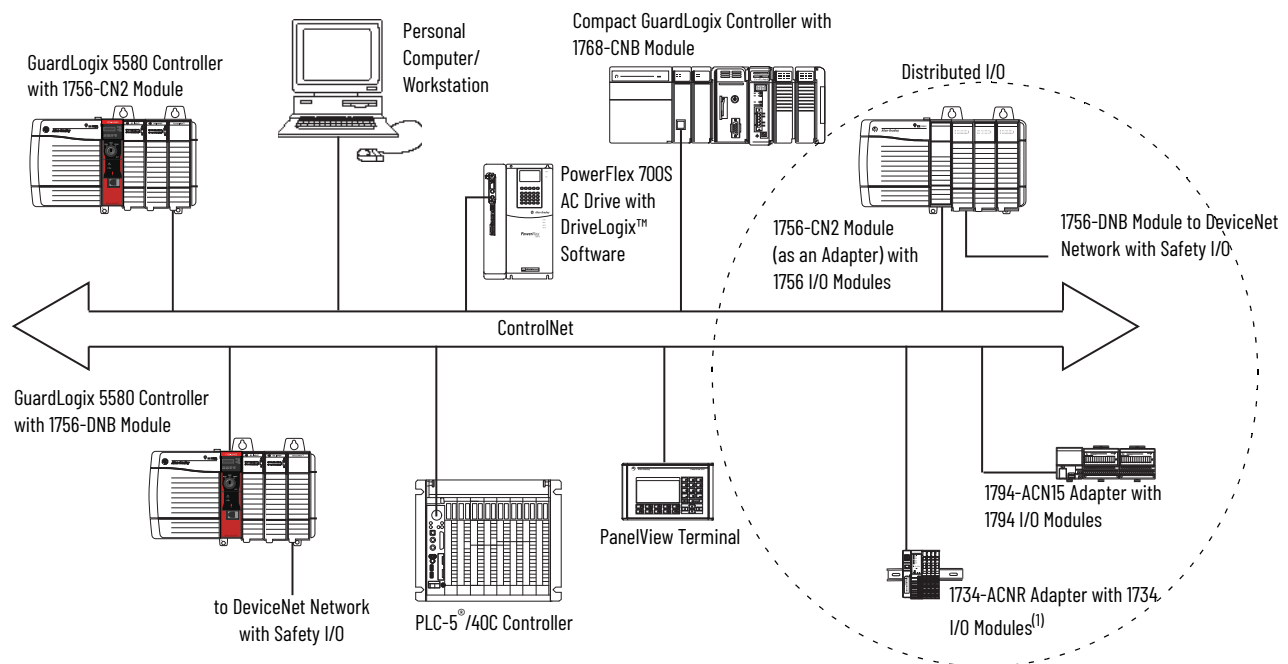
The ControlNet communication modules provide the following:

- 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.

Figure 12 - ControlNet Communication Example



(1) The 1734-ACN adapter does not support POINT Guard I/O Safety modules.

ControlNet Modules

[Table 7](#) lists the available ControlNet modules and their primary features.

Table 7 - ControlLogix ControlNet Modules

Module	System	Is used to
1756-CN2, 1756-CN2K	ControlLogix GuardLogix	<ul style="list-style-type: none">• Perform the same functions as a 1756-CNB module.• Provide twice the capacity for more demanding applications.
1756-CN2R, 1756-CN2RK, 1756-CN2RXT	ControlLogix GuardLogix	<ul style="list-style-type: none">• Perform the same functions as a 1756-CN2 module.• Support redundant ControlNet media.• 1756-CN2RXT operates in extreme environments with -25...70 °C (-13...158 °F) temperatures.
1756-CNB, 1756-CNBK	ControlLogix	<ul style="list-style-type: none">• Control I/O modules.• Communicate with other ControlNet devices (messages).• Share data with other Logix 5000™ series controllers (produce/consume).• Bridge ControlNet links to route messages to devices on other networks.• Standard connections only.
1756-CNBR, 1756-CNBRK	ControlLogix	<ul style="list-style-type: none">• Perform the same functions as a 1756-CNB module.• Support redundant ControlNet media.• Standard connections only.

For more information about using ControlNet modules, see ControlNet Modules in Logix 5000 Control Systems User Manual, publication [CNET-UM001](#).

DeviceNet Network Communication

Applies to these controllers:

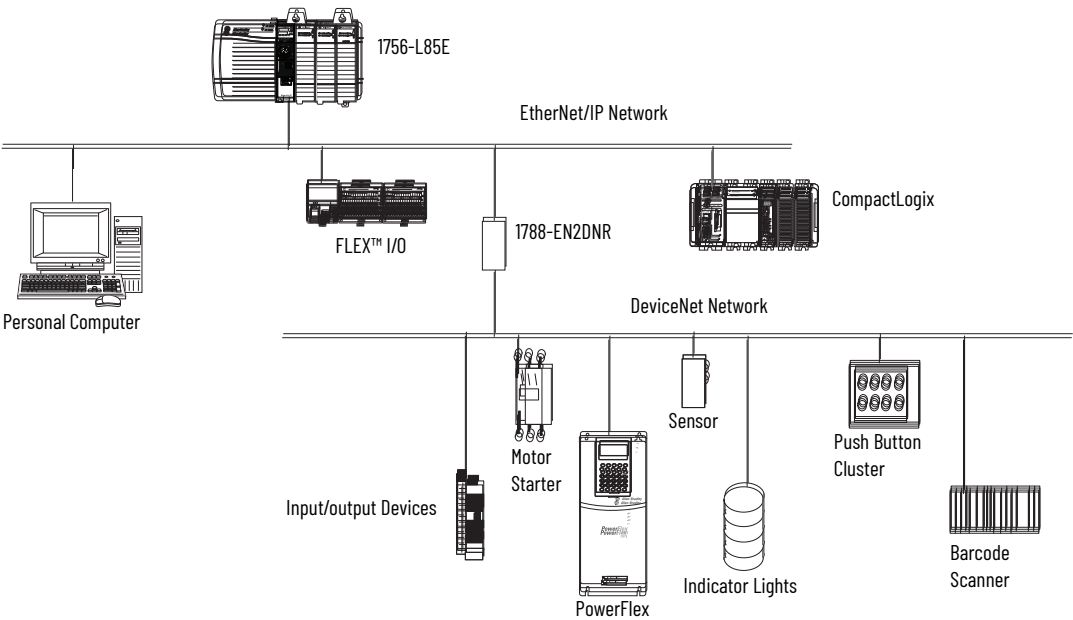
ControlLogix 5580

GuardLogix 5580

The DeviceNet network uses the Common Industrial Protocol (CIP) to provide the control, configuration, and data collection capabilities for industrial devices. The DeviceNet network uses the proven Controller Area Network (CAN) technology, which lowers installation costs and decreases installation time and costly downtime.

A DeviceNet network provides access to the intelligence present in your devices by letting you connect devices directly to plant-floor controllers without having to hard-wire each device into an I/O module.

Figure 13 - ControlLogix DeviceNet Network Overview



In this example, the 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](#).

DeviceNet Bridge Module and Linking Devices

[Table 8](#) lists the available DeviceNet bridge and linking devices that can be used with the DeviceNet network.

Table 8 - DeviceNet Communication Modules and Capabilities

Module/Device	System	Is used to
1756-DNB, 1756-DNBK	ControlLogix GuardLogix	<ul style="list-style-type: none"> Control I/O modules. Communicate with other DeviceNet devices (via messages).
1788-EN2DNR	ControlLogix	Link an EtherNet/IP network to a DeviceNet network.
1788-CN2DN	ControlLogix	Link a ControlNet network to a DeviceNet network.

Connections Over DeviceNet Networks

The ControlLogix controller requires two connections for each 1756-DNB module. One connection is for module status and configuration. The other connection is a rack-optimized connection for the device data.

For DH+ network communication, you have two module options for use in the ControlLogix chassis. [Table 9](#) lists the DH+ modules and capabilities.

Table 9 - DH+ Modules and Capabilities

RIO Module	Is used to
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Performs the same functions as a 1756-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 the ControlLogix 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:

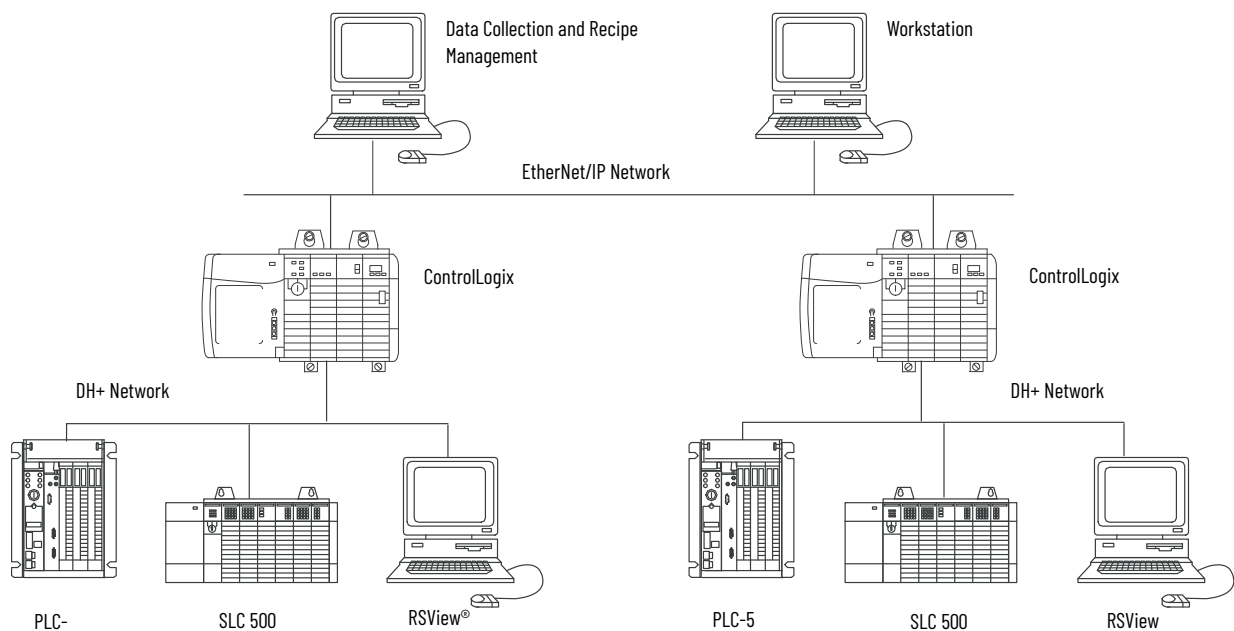
- Channel A supports 57.6 Kbps, 115.2 Kbps, and 230.4 Kbps.
- Channel B supports 57.6 Kbps and 115.2 Kbps.

Data Highway Plus (DH+) Network Communication

Applies to these controllers:

ControlLogix 5580

Figure 14 - ControlLogix DH+ Network Communication Example



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.

For more information to configure and use a DH+ network via the 1756-DHRIO or 1756-DHRIOXT module, see the Data Highway Plus-Remote I/O Communication Interface Module User Manual, publication [1756-UM514](#).

Universal Remote I/O (RIO) Communication

Applies to these controllers:

ControlLogix 5580

For universal remote I/O communication, you have three module options for use in the ControlLogix chassis. [Table 10](#) lists the RIO modules and capabilities.

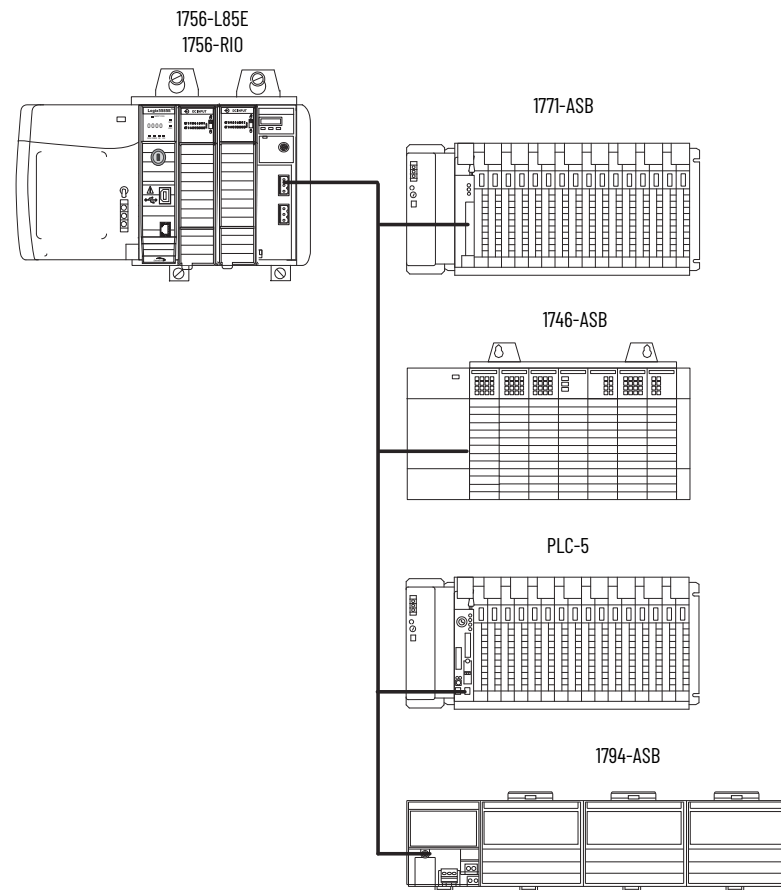
Table 10 - RIO Modules and Capabilities

RIO Module	Is used to
1756-RIO, 1756-RIOK	<ul style="list-style-type: none"> Function as an RIO scanner and adapter. Support connections to 32 racks in any combination of rack size or block transfers. Update data to the ControlLogix controller by using scheduled connections. Use for standard communications only.
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> Function as an 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	<ul style="list-style-type: none"> Performs the same functions as a 1756-DHRIO module. Operates in extreme environments with -25...+70 °C (-13...+158 °F) temperatures. Use for standard communications only.

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

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

Figure 15 - ControlLogix Universal Remote I/O Communication Example



Communicate Over a Universal Remote I/O Network

For the controller to control I/O over a universal remote I/O network, you must complete these tasks.

1. Configure the remote I/O adapter.
2. Lay out the remote I/O network cable.
3. Connect the remote I/O network cable.
4. Configure the scanner channel.

For more information to configure a remote I/O network with the 1756-RIO, 1756-DHRIO, or 1756-DHRIOXT modules, see these publications:

- Data Highway Plus-Remote I/O Communication Interface Module User Manual, publication [1756-UM514](#)
- ControlLogix Remote I/O Communication Module User Manual, publication [1756-UM534](#)

As you design your remote I/O network, remember the following:

- All devices that are connected to a remote I/O network must communicate by using the same communication rate. These rates are available for remote I/O:
 - 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.

Foundation Fieldbus Communication

Applies to these controllers:

ControlLogix 5580

Foundation Fieldbus is an open interoperable fieldbus that is designed for process control instrumentation. The Foundation Fieldbus devices that are described in [Table 11](#) can be connected to the ControlLogix controller via another network as shown in the following example.

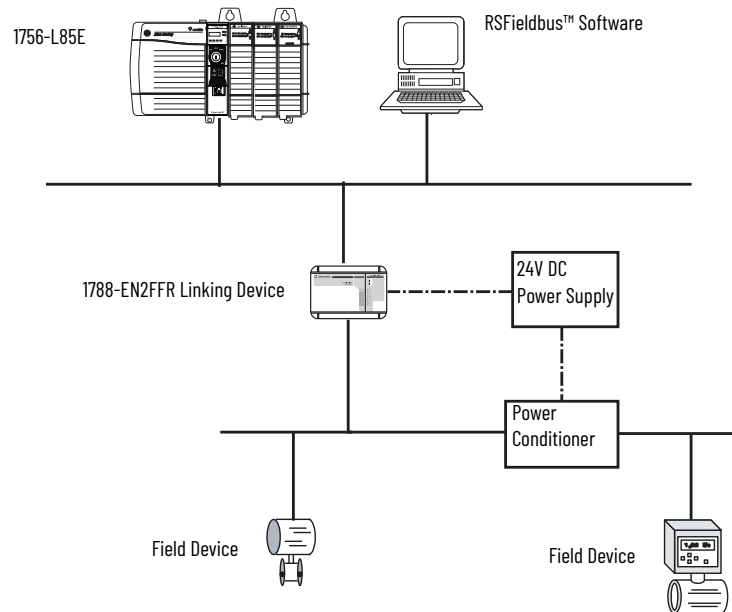
Table 11 - Foundation Fieldbus Devices and Capabilities

Fieldbus Device	Is used to
1788-EN2FFR	<ul style="list-style-type: none"> Bridge an EtherNet/IP network to Foundation Fieldbus. Connect via a low-speed serial (H1) and high-speed Ethernet (HSE) network connections. Access devices directly via an OPC server. Use for standard communications only.
1788-CN2FFR	<ul style="list-style-type: none"> Connect via low-speed serial (H1) connections. Bridge a ControlNet network to a Foundation Fieldbus. Support redundant ControlNet media. Use for standard communications only.

Foundation Fieldbus distributes and executes control in the device. The Foundation Fieldbus linking device does the following:

- Bridges from an EtherNet/IP network to an H1 connection
- Accepts HSE or EtherNet/IP messages and converts them to the H1 protocol

Figure 16 - Foundation Fieldbus Example



For more information about using the Foundation Fieldbus devices available from Rockwell Automation, see these publications:

- EtherNet/IP and ControlNet to FOUNDATION Fieldbus Linking Device User Manual, publication [1788-UM057](#)
- FOUNDATION Fieldbus Design Considerations Reference Manual, publication [PROCES-RM005](#)

HART Communication

Applies to these controllers:

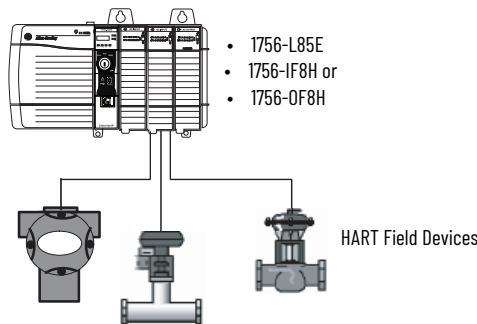
ControlLogix 5580

HART (Highway Addressable Remote Transducer) is an open protocol that is designed for process control instrumentation.

Device	Is used to
1756 analog HART I/O modules: 1756-IF8H, 1756-IF8HK 1756-IF8IH 1756-IF16H, 1756-IF16HK 1756-IF16IH 1756-OF8H, 1756-OF8HK 1756-OF8IH	<ul style="list-style-type: none">• Act as HART master to allow communication with HART field devices.• Interface directly with field devices (through built-in HART modems), which mitigates the need for external hardware and more wiring.• Provide access to more field device data, including voltage and current measurements.• Directly connect asset management software to HART devices.• Support differential wiring for environments where improved noise immunity is needed (input modules).• Use for standard communications only.
ProSoft interface MVI56-HART	<ul style="list-style-type: none">• Acquire data or control applications with slow update requirements, such as a tank farm.• Does not require external hardware to access HART signal.• Does not provide a direct connection to asset management software.• Use for standard communications only.

The HART protocol combines digital signals with analog signals to ready the digital signal for the Process Variable (PV). The HART protocol also provides diagnostic data from the transmitter.

Figure 17 - HART Protocol Example



For more information about using the HART I/O modules, see the ControlLogix HART Analog I/O Modules User Manual, publication [1756-UM533](#).

For more information about the ProSoft HART interface, see the ProSoft Technologies website at <http://www.prosoft-technology.com>.

Start to Use the Controller

Create a Logix Designer Application Project

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Create a controller project by using the Studio 5000 Logix Designer® application.

1. Create a new project and select the controller.
2. Define the properties of the controller:
 - Choose the major revision of firmware for the controller.
 - Choose the chassis size.
 - Choose the slot for the controller.
 - Choose a security authority option.

For detailed information on security, refer to the Logix 5000 Controllers Security Programming Manual, publication [1756-PM016](#).

- Enter a description of the project.
3. Click Finish.

New Project

1756-L85E ControlLogix® 5580 Controller
SafetyProject

Revision: 36

Chassis: 1756-A10 10-Slot ControlLogix Chassis

Slot: 0

Security Authority: No Protection

☐ Use only the selected Security Authority for authentication and authorization

Secure With: ☒ Logical Name <Controller Name> ☐ Permission Set

Description:

Redundancy: ☐ Enable

Cancel Back Next Finish

Additional Configuration for a GuardLogix Controller

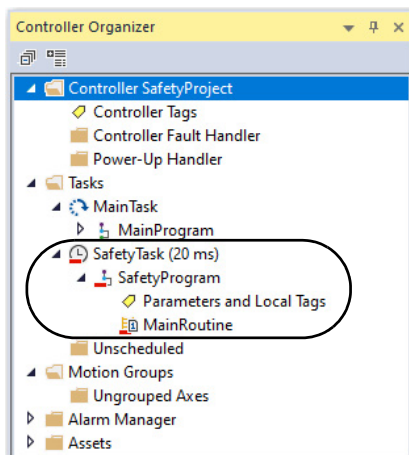
Applies to these controllers:

GuardLogix 5580

GuardLogix® controllers require additional configuration after you create the project. These topics describe how to configure your controller.

For a GuardLogix controller, the Logix Designer application creates a safety task and a safety program. A main Ladder Diagram safety routine 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.



Set the Safety Level for a GuardLogix Controller

The safety level declares to the Logix Designer application 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 required for an application is based on a required risk assessment performed by the customer.
- The safety level achieved is determined by conformance to Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements.

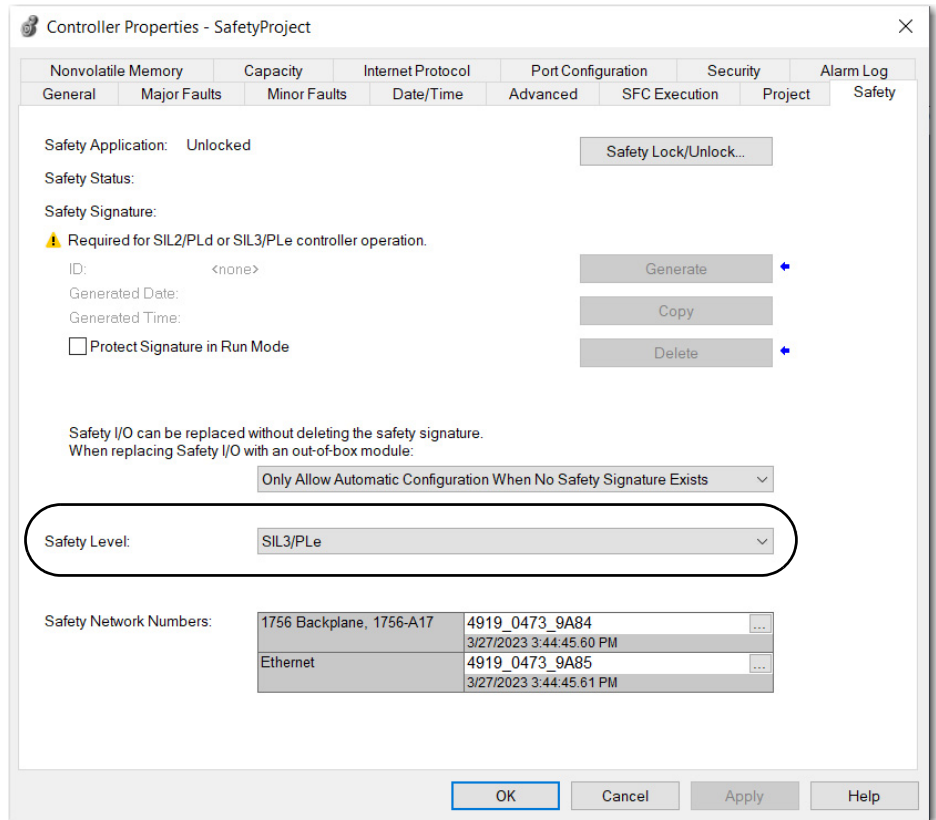
See the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

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 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 steps 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.

For information on how to set passwords, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

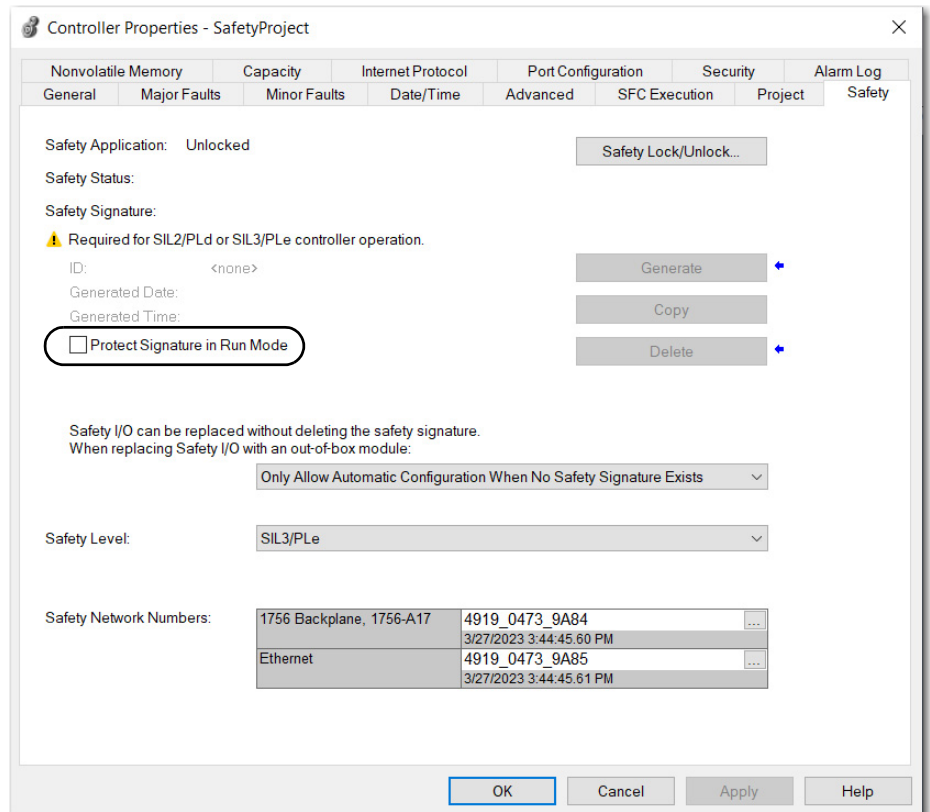
Protect the Safety Signature in Run Mode

You can 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.

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.
4. Click OK.



Assign the Safety Network Number (SNN)

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/IP™ 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.

Rockwell Automation recommends 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 Controller Systems 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.

For an explanation on the Safety Network Number, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

The SNN can be software-assigned (time-based) or user-assigned (manual). These two formats of the SNN are described in the following sections:

- [Automatic Assignment of Time-based SNN on page 54](#)
- [Manual Assignment of SNN on page 54](#)

Automatic Assignment of Time-based SNN

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 18 - Time-based Format

Manual Assignment of SNN

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.

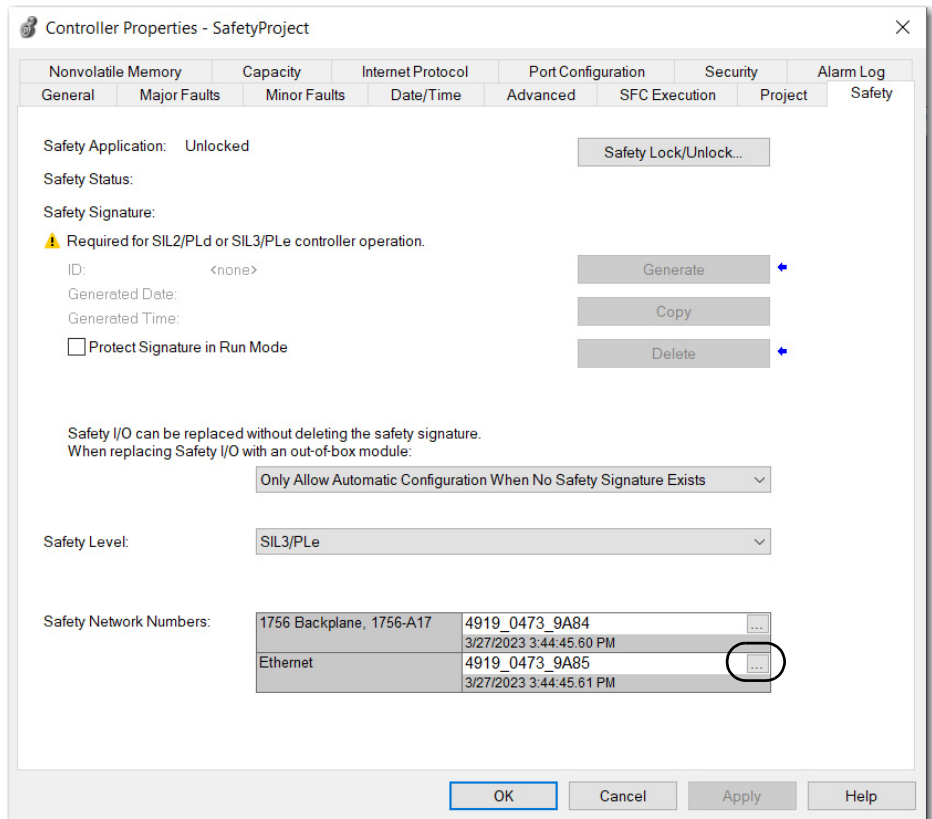
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

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 a manual assignment:

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  to the right of the safety network number for the port that you want to change.



Controller Properties - SafetyProject


Nonvolatile Memory Capacity Internet Protocol Port Configuration Security Alarm Log


General Major Faults Minor Faults Date/Time Advanced SFC Execution Project Safety

Safety Application: Unlocked Safety Lock/Unlock...


Safety Status:

Safety Signature:

 Required for SIL2/PLd or SIL3/PLe controller operation.


ID: <none> Generate 


Generated Date: Copy

Generated Time: Delete 



☐ Protect Signature in Run Mode

Safety I/O can be replaced without deleting the safety signature.
When replacing Safety I/O with an out-of-box module:

Only Allow Automatic Configuration When No Safety Signature Exists 

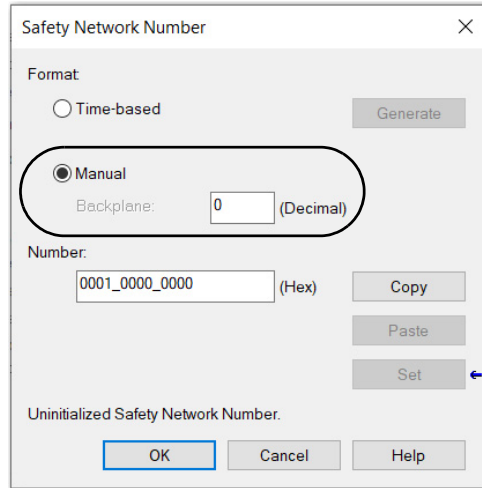
Safety Level: SIL3/PLe 

Safety Network Numbers:

1756 Backplane, 1756-A17	4919_0473_9A84 3/27/2023 3:44:45 60 PM	
Ethernet	4919_0473_9A85 3/27/2023 3:44:45 61 PM	

OK Cancel Apply Help

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





The dialog box is titled "Safety Network Number". It has a "Format" section with two radio buttons: "Time-based" and "Manual". The "Manual" radio button is selected and circled. Below it is a "Backplane:" label followed by a text box containing "0" and the label "(Decimal)". Below that is a "Number:" label followed by a text box containing "0001_0000_0000" and the label "(Hex)". To the right of the "Number:" text box are three buttons: "Copy", "Paste", and "Set". The "Set" button is circled. At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

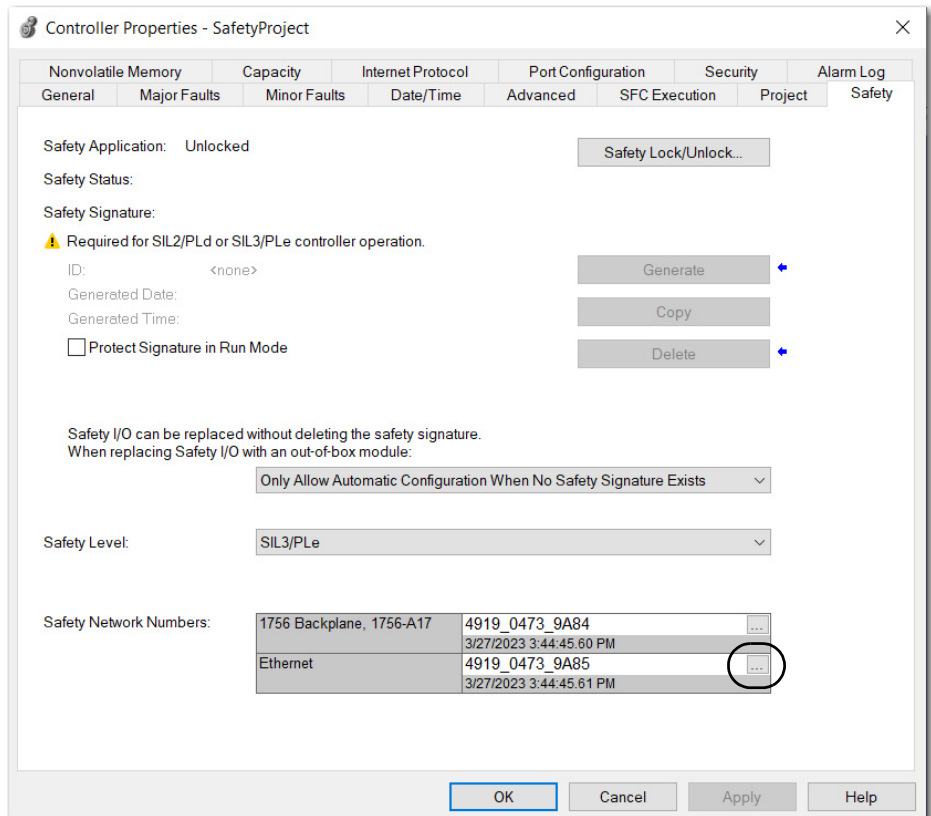
- Click OK.

Copy and Paste a Safety Controller Safety Network Number

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

Copy a Safety Controller SNN

- On the Online toolbar, click the Controller Properties icon .
- On the Controller Properties dialog box, click the Safety tab.
- On the Safety tab, click  to the right of the safety network number.



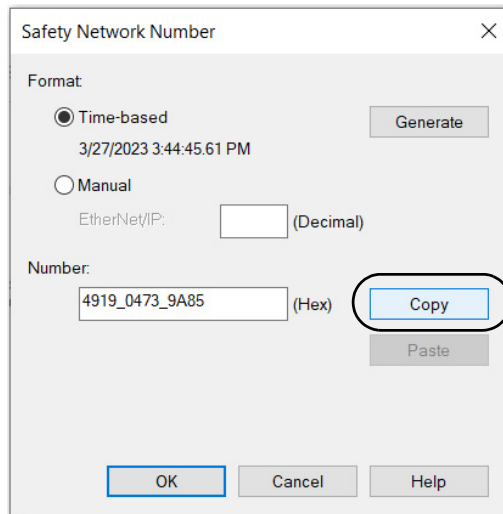
The dialog box is titled "Controller Properties - SafetyProject". It has a tabbed interface with tabs: "Nonvolatile Memory", "Capacity", "Internet Protocol", "Port Configuration", "Security", and "Alarm Log". The "Security" tab is selected. Below the tabs are several sections:

- Safety Application:** Unlocked. A button "Safety Lock/Unlock..." is to the right.
- Safety Status:**
- Safety Signature:**
 - A warning icon and text: "Required for SIL2/PLd or SIL3/PLe controller operation."
 - ID:** <none>. A button "Generate" is to the right.
 - Generated Date:**
 - Generated Time:**
 - ☐ Protect Signature in Run Mode. A button "Delete" is to the right.
- Safety I/O can be replaced without deleting the safety signature.**
 - When replacing Safety I/O with an out-of-box module:
 - Only Allow Automatic Configuration When No Safety Signature Exists (dropdown menu)
- Safety Level:** SIL3/PLe (dropdown menu)
- Safety Network Numbers:**

1756 Backplane, 1756-A17	4919_0473_9A84	...
	3/27/2023 3:44:45 60 PM	
Ethernet	4919_0473_9A85	...
	3/27/2023 3:44:45 61 PM	



At the bottom of the dialog box are four buttons: "OK", "Cancel", "Apply", and "Help".

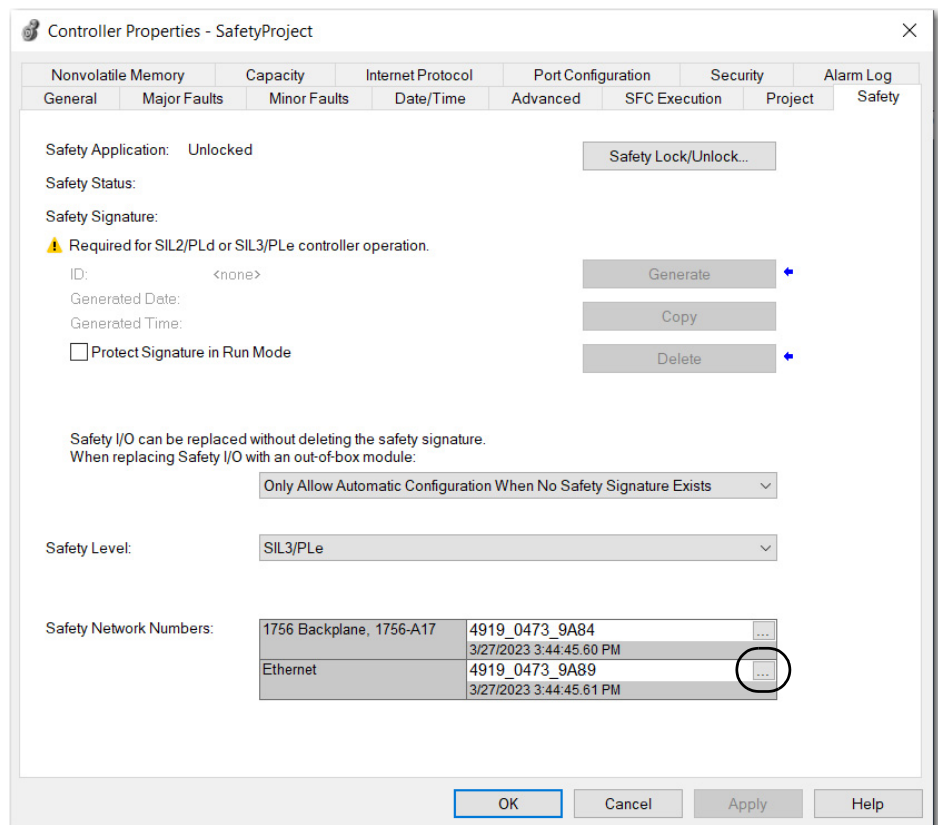
- On the Safety Network Number dialog box, click Copy and then OK.



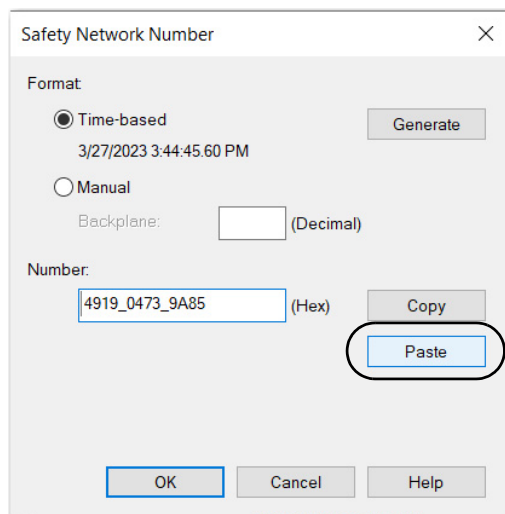
- On the Controller Properties dialog box, click OK.

Paste a Safety Controller SNN

- On the Online toolbar, click the Controller Properties icon .
- On the Controller Properties dialog box, click the Safety tab.
- On the Safety tab, click  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.

Go Online with the Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

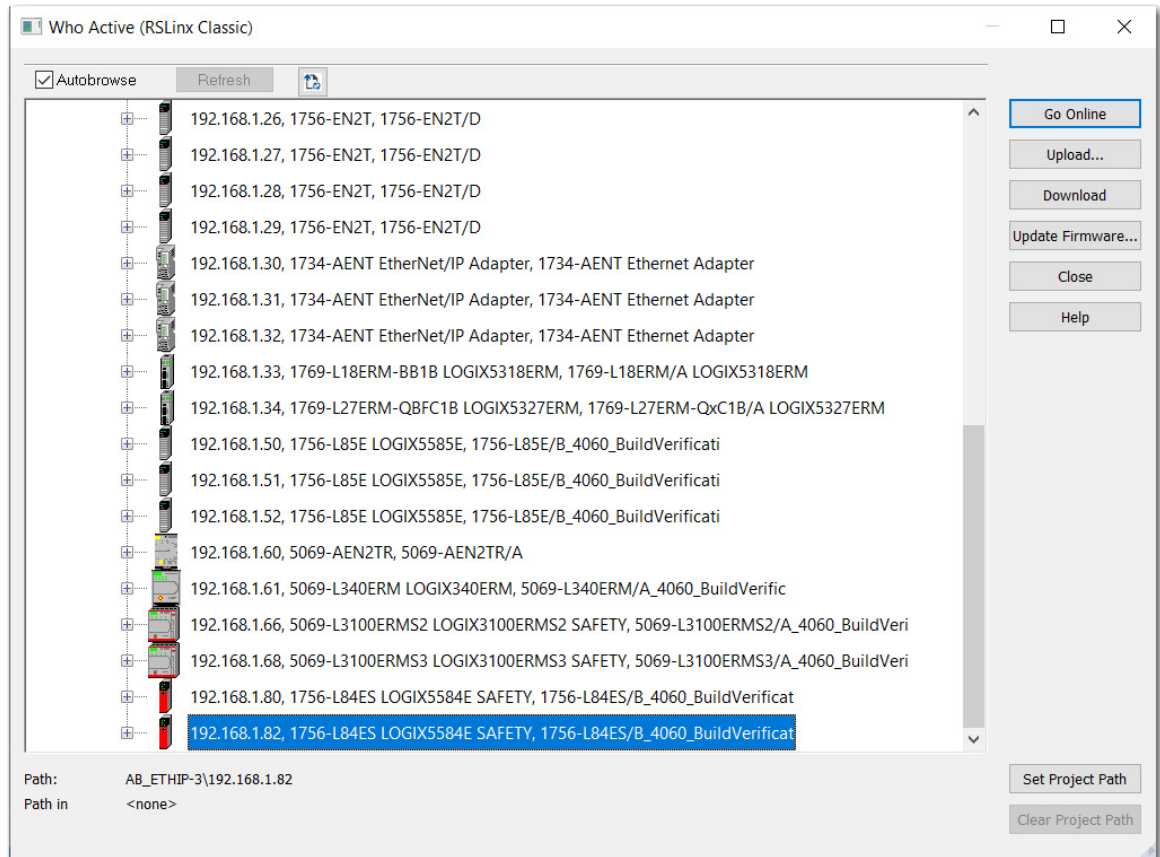
To go online with the controller, you must first specify a communication path in the Logix Designer application.

Use RSWho

1. Open or create a Logix Designer application project.
2. In the application, click RSWho.



3. Expand the communication path and select the controller.



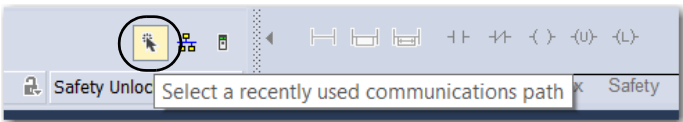
4. To store the path in the project file, click Set Project Path.
If you store the project path in the project, then you do not have to choose the path each time you go online.
5. After choosing the communication path, click Go Online in the Who Active dialog box.
Go Online will use the highlighted node in the Who Active tree, regardless of the setting for Path in Project. For more information on the Who Active dialog box, see the Logix Designer Online Help.

See [Additional Considerations for Going Online with a GuardLogix Controller on page 60](#).

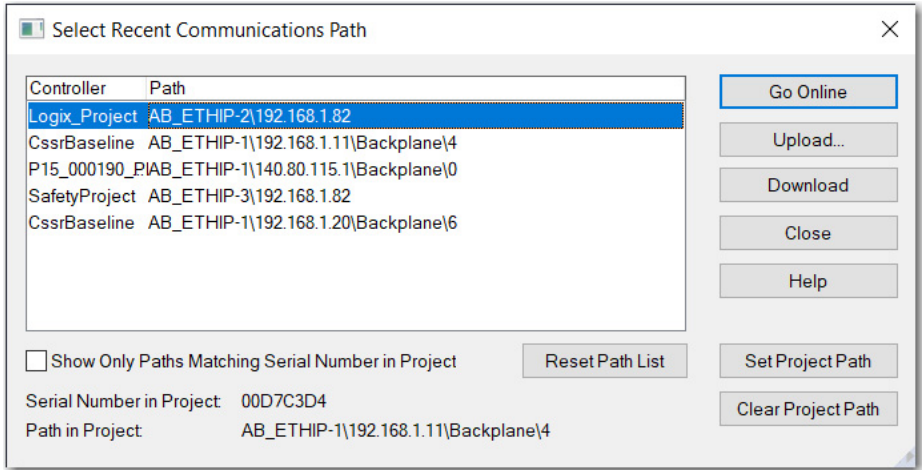
Use a Recent Communication Path

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.



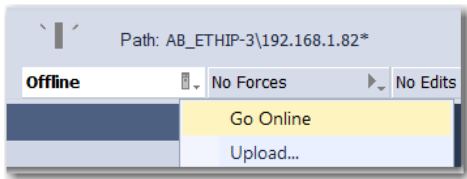
2. On the Select Recent Communications Path dialog box, choose the path.



3. To store the path in your project, click Set Project Path.
4. Click Go Online.

For more information on the Select Recent Communications Path dialog box, see the Logix Designer Online Help.

Once you have established a communication path, then you can choose Go Online from the Controller Status menu when you are working in the project.



See [Additional Considerations for Going Online with a GuardLogix Controller on page 60](#).

Additional Considerations for Going Online with a GuardLogix Controller

Applies to these controllers:

GuardLogix 5580

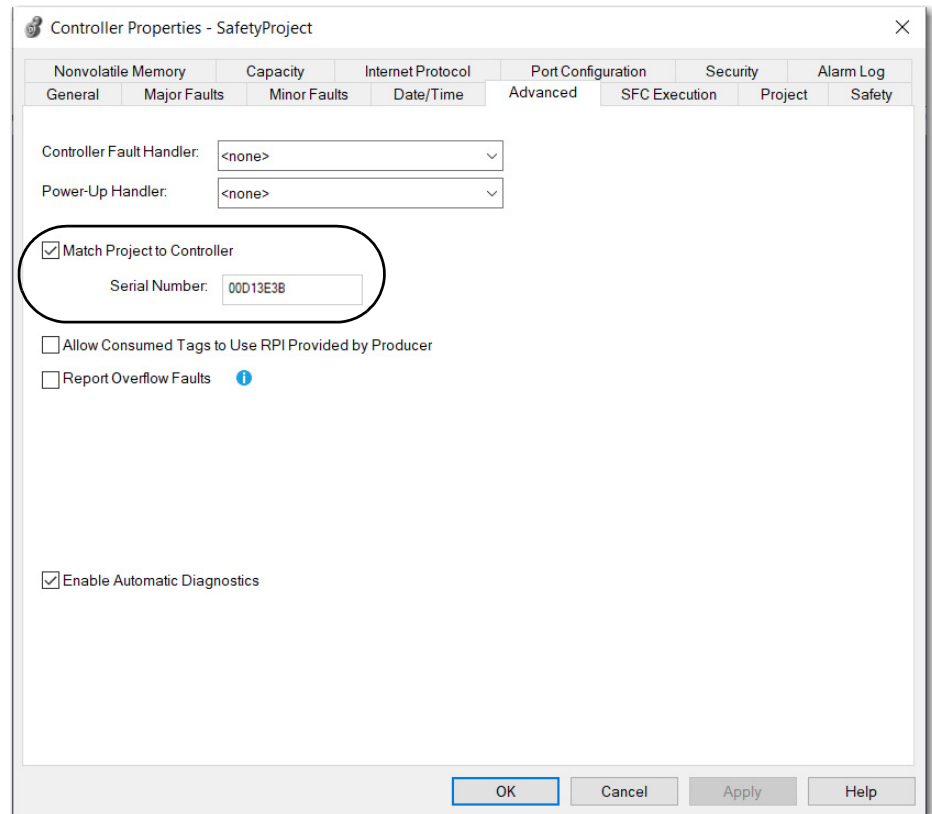
The Logix Designer application determines whether you can go online with a target controller based on whether the offline project is new or whether changes occurred in the offline project. If the project is new, you must first download the project to the controller. If changes occurred to the project, 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 Project to Controller Match feature, 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.

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 located on the Advanced tab of the Controller Properties dialog box.

Figure 19 - Match Project to Controller



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.

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 upgrade kit. An upgrade kit ships on a supplemental DVD along with the Studio 5000® environment.



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

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 prior to 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 or not a download can proceed.

Table 12 - Effect of Safety-lock and Safety Signature on Download Operation

Safety-lock Status	Safety Signature Status	Download Functionality
Controller safety-unlocked	Safety signature in the offline project matches the safety signature in the controller.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.
Controller safety-locked	Safety signatures match.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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 GuardLogix Controller

For a safety project, the Logix Designer application checks for the following:

- Do the offline project and controller serial numbers match (if Project to Controller Match is selected)?
- 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 13 - Connect to the Controller with a Safety Project

If the software indicates	Then
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.

Download to the Controller

Applies to these controllers:

ControlLogix 5580

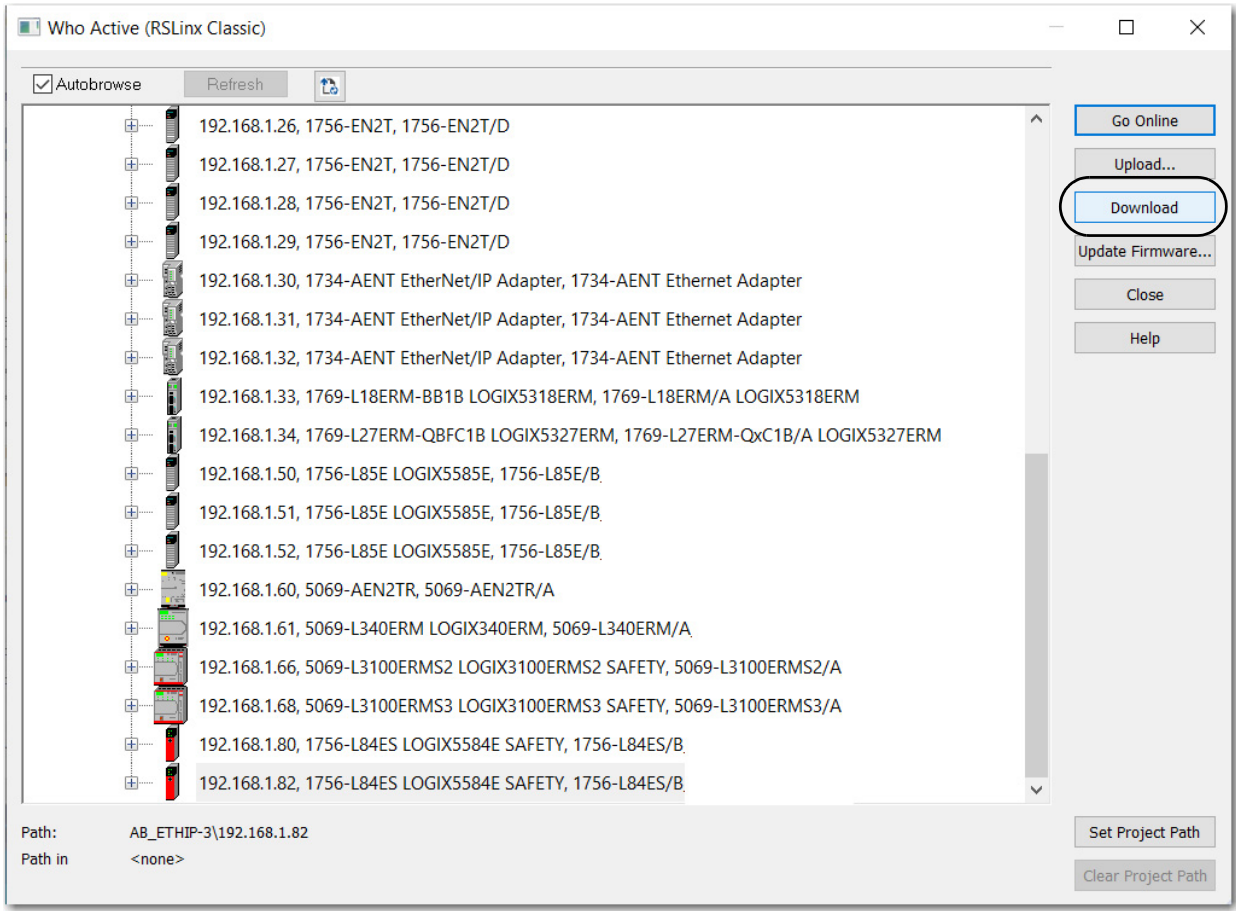
GuardLogix 5580

When you download a project to the controller, it copies the project from the Logix Designer application onto the controller.

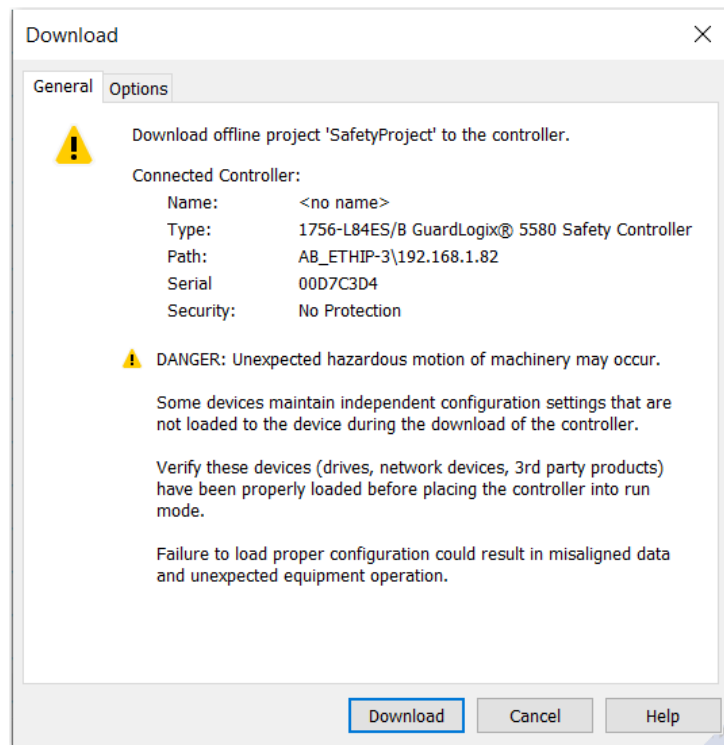
Use Who Active

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

1. After choosing the communication path, click Download in the Who Active dialog box.



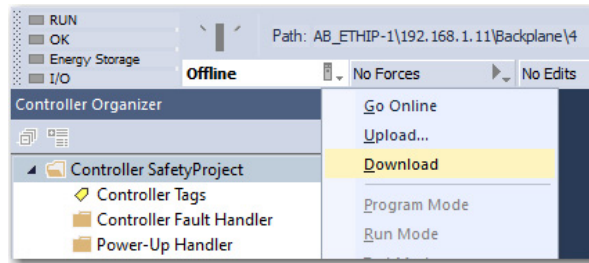
2. After reading the warnings in the Download dialog box, click Download.



Use the Controller Status Menu

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

Figure 20 - Download via the Controller Status Menu



After the download completes, the project name appears on the scrolling status display.

Additional Considerations for Download to a GuardLogix Controller

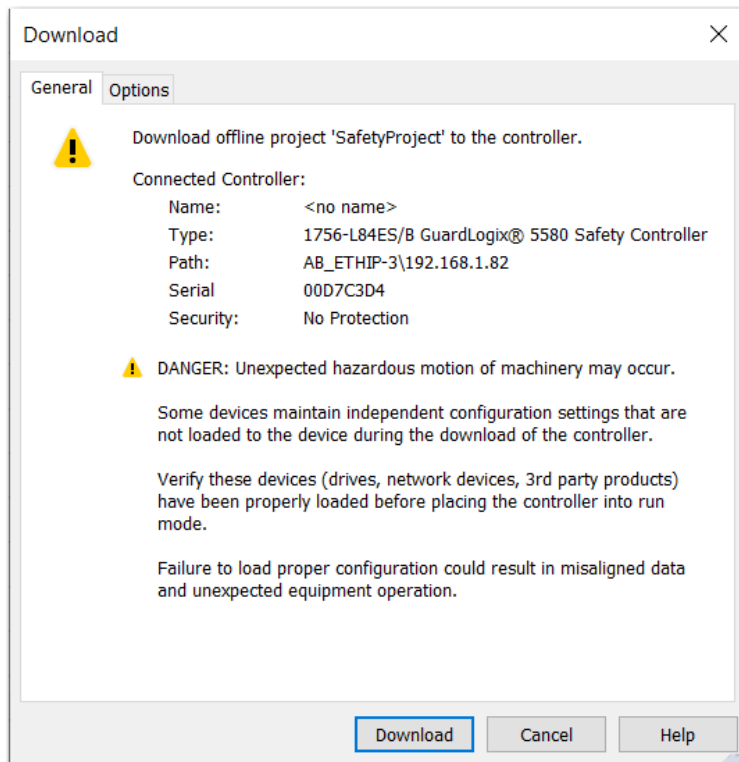
Applies to these controllers:

GuardLogix 5580

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

- Controller serial number (if project to controller match is selected)
- Firmware major and minor revisions
- Safety status
- Safety signature (if one exists)
- Safety-lock status
- Safety Partner (if one exists). The Logix Designer application 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 appears. Click Download.



The Logix Designer application displays status messages in the download dialog, progress screen, and the Errors window.

If the software indicates:	Then:
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.	<ul style="list-style-type: none"> 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.
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.

Upload from the Controller

Applies to these controllers:

ControlLogix 5580

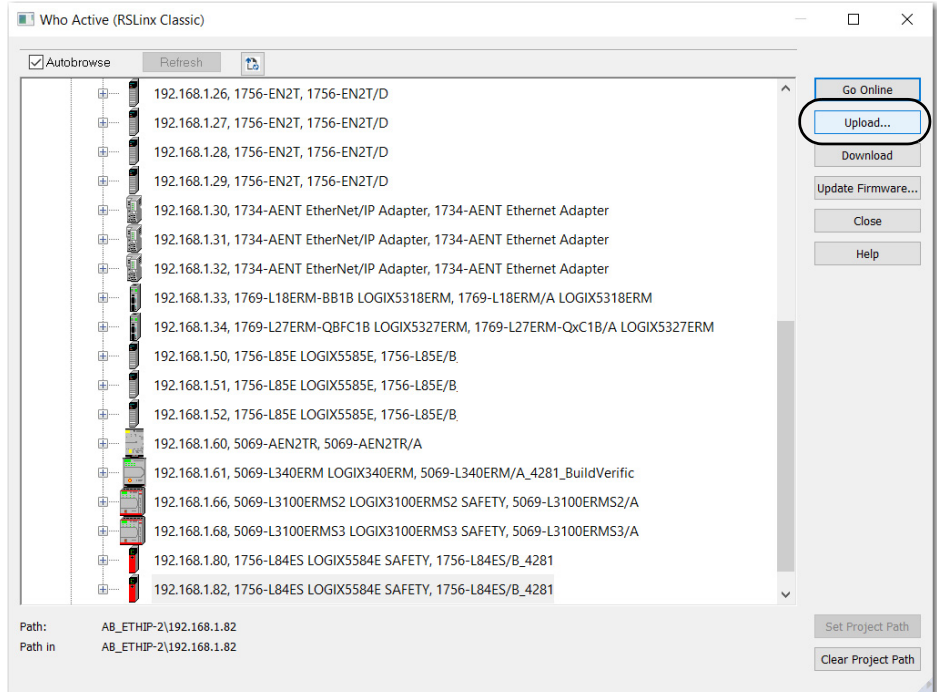
GuardLogix 5580

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

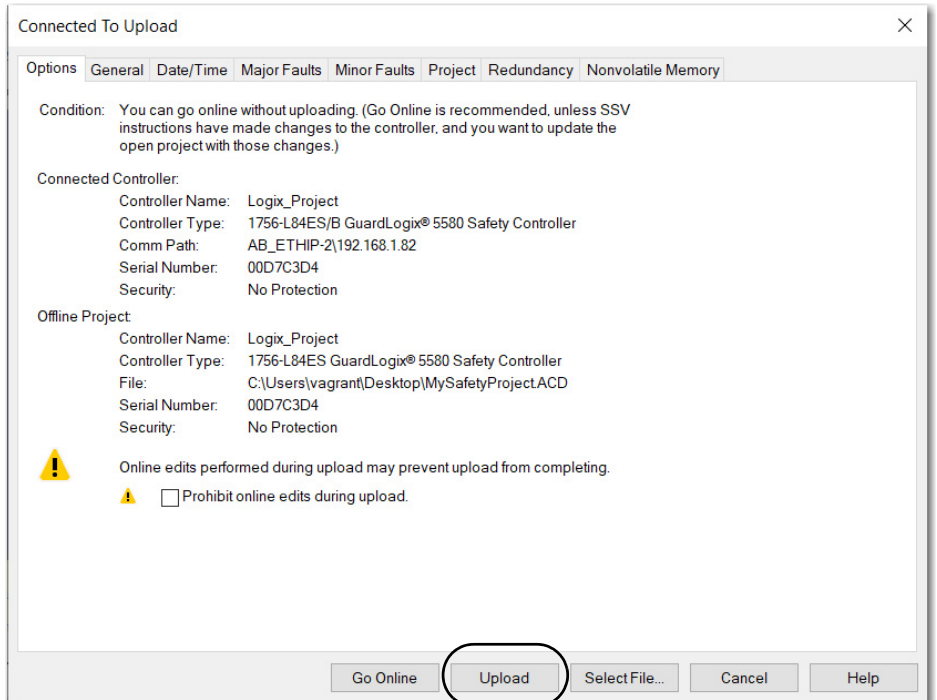
Use Who Active

You can use the features of the Who Active dialog box to upload from your controller after you have set the communication path. Complete these steps to upload from the controller.

1. After choosing the communication path, click Upload on the Who Active dialog box.



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



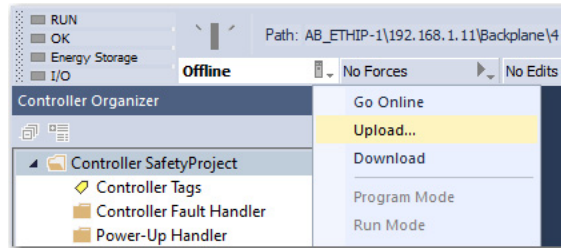
For more information on the Connected To Upload dialog box, see the online Help.

Use the Controller Status Menu

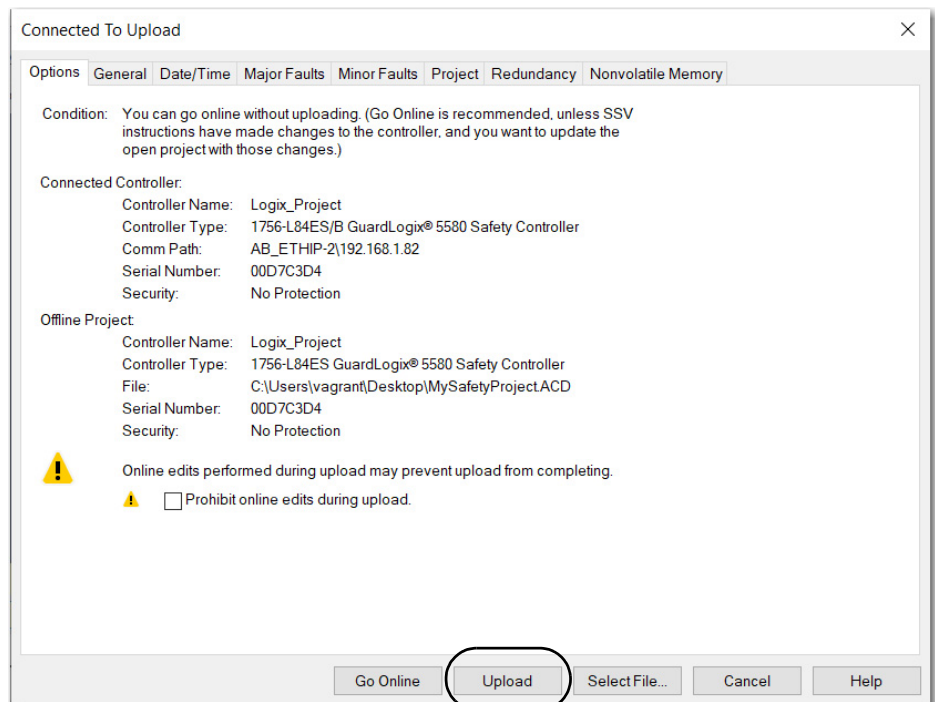
After you have chosen a communication path in the Logix Designer application, you can use the Controller Status menu to upload from the controller.

1. From the Controller Status menu, choose Upload.

Figure 21 - Upload via the Controller Status Menu



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



Additional Considerations for Upload from a GuardLogix Controller

Applies to these controllers:
GuardLogix 5580


For a safety project, the 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.

 Prior to 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.


Choose the Controller Operation Mode

Use this table as a reference when determining your controller operation mode.

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Keyswitch Position ⁽¹⁾	Available Controller Modes	In this mode you can:	In this mode you cannot:	 ATTENTION:
RUN	Run mode —The controller is actively controlling the process/machine. Projects cannot be edited in the Logix Designer application when in Run mode.	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Turn outputs to their configured state for Program mode Change the mode of the controller via the Logix Designer application Download a project Schedule a ControlNet® network While online, edit the project 	Run mode is used only when all conditions are safe.
REM	Remote Run mode —This mode is identical to Run mode except you can edit the project online, and change the controller mode through the Logix Designer application.	<ul style="list-style-type: none"> Turn outputs to the state commanded by the logic of the project. Execute (scan) tasks Change the mode of the controller via the Logix Designer application While online, edit the project Send messages Send and receive data in response to a message from another controller Produce and consume tags 	<ul style="list-style-type: none"> Turn outputs to their configured state for Program mode Download a project Schedule a ControlNet network 	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.
	Remote Program mode —This mode functions like Program mode, except you can change the controller mode through the Logix Designer application.	<ul style="list-style-type: none"> Turn outputs to their configured state for Program mode Change the mode of the controller via the Logix Designer application 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 	<ul style="list-style-type: none"> Turn outputs to the state commanded by the logic of the project. Execute (scan) tasks 	Outputs are commanded to their Program mode state, which can cause a dangerous situation.
	Remote Test mode —This controller 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. Output modules are commanded to their Program mode state (on, off, or hold).	<ul style="list-style-type: none"> Turn outputs to their configured state for Program mode Execute (scan) tasks Change the mode of the controller via the Logix Designer application While online, edit the project Send messages Send and receive data in response to a message from another controller Produce and consume tags 	<ul style="list-style-type: none"> Turn outputs to the state commanded by the logic of the project. Download a project Schedule a ControlNet network Send messages 	
PROG	Program mode —This controller mode does not execute code or control I/O, but editing operations are available. Output modules are commanded to their Program mode state (On, Off, or Hold). In this position, controller modes cannot be changed through the Logix Designer application.	<ul style="list-style-type: none"> Turn outputs to their configured state 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 	<ul style="list-style-type: none"> Turn outputs to the state commanded by the logic of the project. Execute (scan) tasks Change the mode of the controller via the Logix Designer application Send messages 	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.

(1) Moving the keyswitch from Run to Remote leaves the controller in the Remote Run mode, while moving the switch from Program to Remote leaves the controller in the Remote Program mode. You cannot choose Remote Test mode by the keyswitch alone, it is only available via the Logix Designer application.

Use the Keyswitch to Change the Operation Mode

To change the operation mode, use the controller keyswitch, catalog number 1756-KY1. The controller keyswitch provides a mechanical means to enhance controller and control system security. You must physically move the keyswitch on the controller to change its operating mode from RUN, to REM, or to PROG.

When the keyswitch on the controller is set to RUN mode, features like online editing, program downloads, and firmware updates are prohibited. See [Choose the Controller Operation Mode on page 71](#) for a complete list of prohibited features.

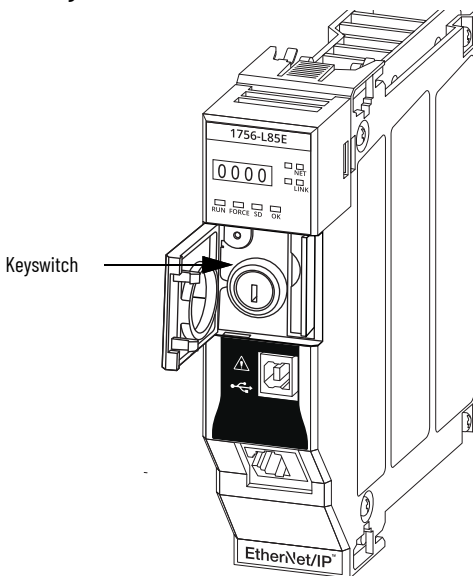
The physical keyswitch can complement other authorization and authentication methods that similarly control user-access to the controller, such as the FactoryTalk® Security service.

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

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

The keyswitch on the front of the controller can be used to change the controller to one of these modes:

- Run (RUN)
- Remote (REM)
- Program (PROG)



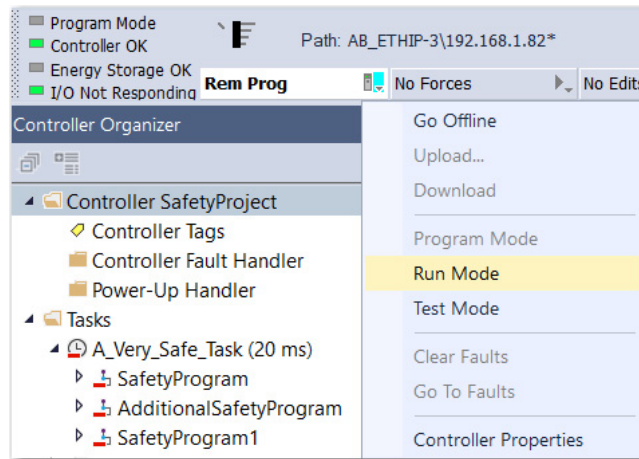
Use the Logix Designer Application to Change the Operation Mode

When you are online with the controller, and the controller keyswitch is set to Remote (REM or the center position), then you can use Logix Designer to change the operation mode.

The Controller Status menu lets you specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

Figure 22 - Operation Mode



For this example, the controller keyswitch is set to Remote mode. If your controller keyswitch is set to Run or Program modes, the menu options change.

Reset Button

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

You can reset the ControlLogix® and GuardLogix controllers, and the 1756-L8SP 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 GuardLogix 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:

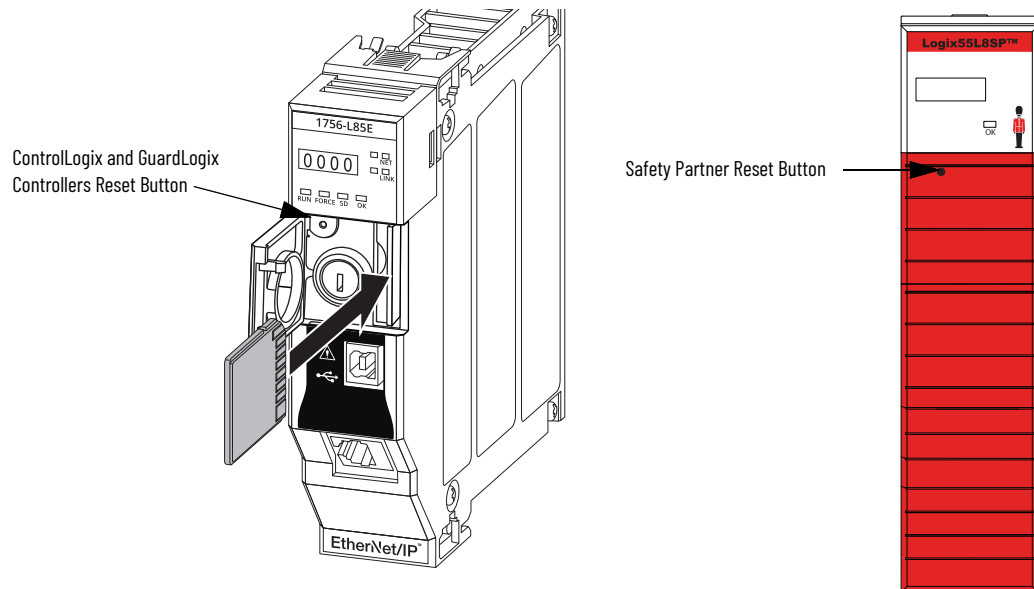
- A Stage 1 reset clears the application program and memory, but retains the IP address and all network settings. A stage 1 reset occurs only if the controller contains a user application. See [Stage 1 Reset on page 75](#).
- A Stage 2 reset returns the controller to out-of box settings (including firmware), 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. See [Stage 2 Reset on page 76](#).

The Safety Partner reset returns the safety partner to out-of box settings (including firmware). See [Safety Partner Reset on page 76](#).

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.



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 Wall Clock Time to default parameters.
- Resets the controller to begin the controller start up process.
- Prevents the controller from loading firmware or software from the SD card on this first start up after the reset, regardless of the setting on the SD card, and without modifying the SD card contents (the write-protect setting is irrelevant). An SD card will reload (if configured to do so) 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 an SD 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 Logix Designer application project to the controller in these ways:

- Download the project from the Logix Designer application - For more information, see [Download to the Controller on page 64](#)
- 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 (the 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 start up process.
- There will be no entries in the controller log after a Stage 2 reset, but saved logs on the SD card remain.

Follow these steps to perform a Stage 2 reset.

1. Power down the controller.
2. Remove the key from the keyswitch.
3. Open the front door on the controller.
4. Remove the SD 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, Factory Default.
8. After Factory Default appears, release the reset button.
9. On your workstation, delete all of the files on the SD card.
10. Power down the controller.
11. Reinstall the SD card.
12. Powerup the controller.
13. Verify that the controller is at firmware revision 1.x, and the controller is set to DHCP.

After a Stage 2 reset is performed, you must complete these tasks to use the controller again:

- Configure the Ethernet ports, set the desired EtherNet/IP mode, and set the controller IP address configuration. For more information, see [Connect to a Controller on page 27](#).
- Update the firmware revision - For more information, see [Update Controller Firmware on page 30](#).
- Download a Logix Designer application project to the controller in one of these ways:
 - Download the project from the Logix Designer application - For more information, see [Download to the Controller on page 64](#).
 - 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.

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 Secure Digital Card

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers ship with a Secure Digital (SD) card installed. We recommend that you leave the SD 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 SD cards available from Rockwell Automation:

- 2 GB SD card, catalog number 1784-SD2
- CodeMeter CmCard SD, 4 GB, catalog number 9509-CMSDCD4 (when license-based source protection and execution protection features are enabled)

While other SD 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.

SD 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 ControlLogix® 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 SD card matches the project in the controller memory at that time. Changes that you make after you store the project are not reflected in the project on the SD card.

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

IMPORTANT

Do not remove the SD 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 solid green.

If an SD 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 SD card.

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

Considerations for Storing and Loading a Safety Project

Applies to these controllers:

GuardLogix 5580

Only GuardLogix® 5580 controllers support safety projects. ControlLogix 5580 controllers do not support safety projects.

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 SD card.

If no application project exists in the controller, you can save only the firmware of the safety controller if a valid partnership exists. 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 an SD card, Rockwell Automation recommends you select Program (Remote Only) as the Load mode, that is, the mode that the controller enters after a project is loaded from the SD card.

IMPORTANT

To prevent the firmware stored on the SD card from overwriting newly-updated firmware:

- The update process first checks the load option on the SD 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 SD card is locked, the load option does not change, and the firmware that is stored on the SD card can overwrite the newly-updated firmware.

Store to the SD Card

Applies to these controllers:

ControlLogix 5580

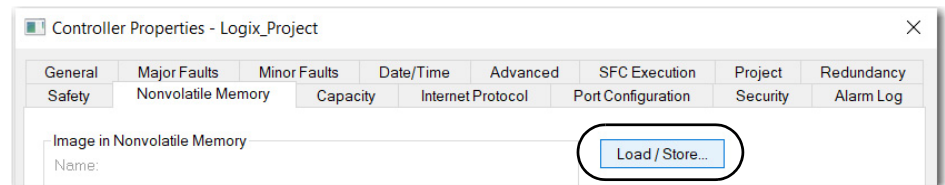
GuardLogix 5580

We recommend that you back up your Logix Designer project to an SD card on a regular basis.

If a major nonrecoverable fault occurs that removes the program from the controller memory, the backup copy on the SD card can be automatically restored to the controller to quickly resume normal controller operation.

To store a project to the SD 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. On the Nonvolatile Memory tab, click Load/Store.



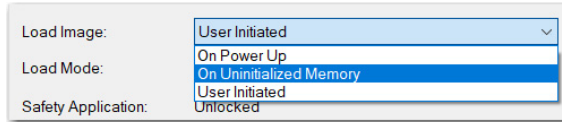
If Load/Store is dimmed (unavailable), verify the following:

- The controller is in Program mode or Remote Program mode
- You have specified the correct communication path.
- The SD card is installed.
- The SD card is unlocked. The locked status appears in the bottom-left corner of the Nonvolatile memory/Load Store dialog box.

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

Nonvolatile memory not present.

4. In the Load Image field, select a setting according to your application requirements.



This table describes the Load Image options.

If you want to load the project	Then select this Load Image option	Notes	Safety Considerations
Whenever you turn on or cycle power	On Power Up	<ul style="list-style-type: none"> 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 Studio 5000 Logix Designer® application to load the project. 	For a safety application, On Power Up loads whether or not the controller is safety-locked or there is a safety signature.
Whenever there is no project in the controller and you turn on or cycle chassis power	On Uninitialized Memory	<ul style="list-style-type: none"> If the project has been cleared from memory, this option loads the project back into the controller on power up. The controller updates the firmware on the controller, if required. The application project stored in nonvolatile memory 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. 	The controller also updates the firmware on the safety partner, if required.
Only through the Logix Designer application	User Initiated	If the controller type as well as 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.	<ul style="list-style-type: none"> 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 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. IMPORTANT: 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 required, the application 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 prevent the firmware stored on the SD card from overwriting newly updated firmware:

- The update process first checks the load option on the SD 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 SD card is locked, the load option does not change, and the firmware that is stored on the SD card can overwrite the newly updated firmware.

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

IMPORTANT Safety Consideration

Rockwell Automation recommends that you use Program (Remote Only), when you set the Load Mode for a safety application project.

6. 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

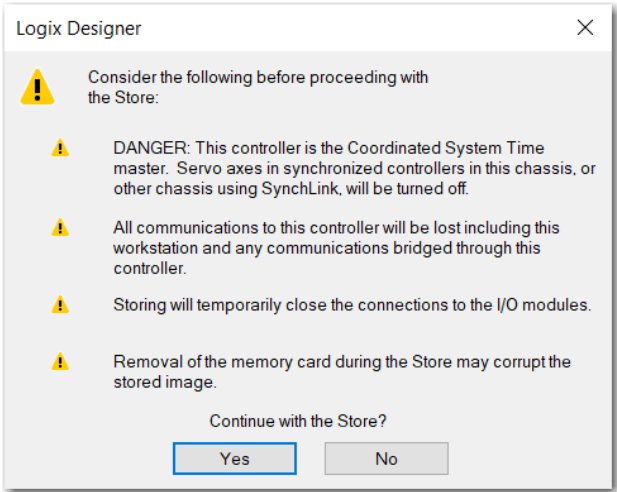
Some Safety I/O devices do not support the Firmware Supervisor feature. For example, Safety I/O devices on DeviceNet® networks and POINT Guard I/O™ modules do not support the Firmware Supervisor feature.

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

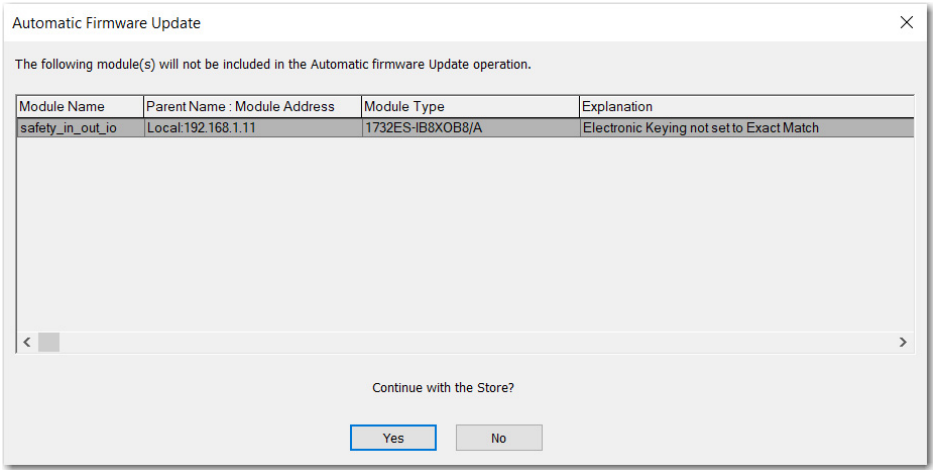
Setting	Description
Disable	<ul style="list-style-type: none">Disables any automatic firmware updates.This item only appears in the menu when you initially save the image.
Enable and Store Files to Image	<ul style="list-style-type: none">Enables automatic firmware updates for I/O devices in the configuration 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 will participate in the Automatic Firmware Update process.⁽¹⁾
Disable and Delete Files from Image	<ul style="list-style-type: none">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 image.This item only appears in the menu on subsequent saves of the image.

(1) The devices that are used with this option must support the revision of firmware being updated to.

7. Click Store.
8. 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 SD 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 solid green.

- On the Automatic Firmware Update dialog box, click Yes.
The project is saved to the SD card as indicated by the controller status indicators.

These indications show the store status

- While the store is **in progress**, the following occurs:
- OK indicator is flashing green
 - SD indicator 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 following occurs:
- 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 SD Card

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

IMPORTANT

With the SD card and brand new, out-of-box controllers:

- If you insert an SD card with an image into a brand new, out-of-box controller (firmware 1.x), then at power-up the controller automatically updates the firmware up to the version of firmware that is stored on the SD card. The update happens regardless of the Load Image setting in the image on the SD 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 an SD card to a controller in one of the following ways:

- [Controller Power-up](#)
- [User-initiated Action](#)



You can always use the Logix Designer application to load the project.

Controller Power-up

This table shows what happens at power up when you insert an SD 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 non-volatile memory is not valid ⁽¹⁾	Firmware > 1.x and internal non-volatile memory is valid ⁽¹⁾
User Initiated	Loads Firmware Only ⁽²⁾	Does Nothing	Does Nothing
On Power Up	Loads both Firmware and Application	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application 	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application
On Uninitialized Memory	Loads both Firmware and Application ⁽²⁾	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application 	Does Nothing

(1) "Valid" includes the No Project condition.

(2) Indicates change in behavior from ControlLogix 5570 and older controllers.

User-initiated Action

IMPORTANT

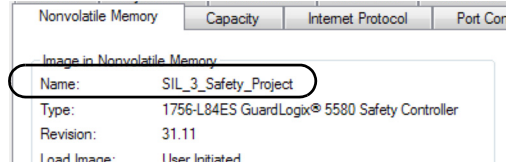
For an out-of-box controller that uses firmware revision 1.xx, you must manually update the controller to the required firmware revision before you can load a project on the controller.

You must complete the following before you can upload a project to the controller from the SD 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. Open the Controller Properties, and click the Nonvolatile Memory tab.
2. On the Nonvolatile Memory tab, verify that the project listed is the project that you want to load.



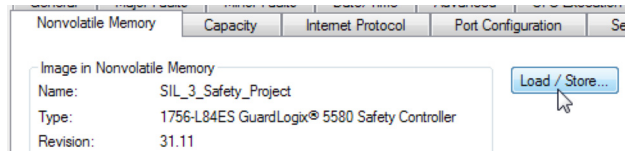
If no project is stored on the SD card, a message in the lower-left corner of the Nonvolatile Memory tab indicates that an image (project) is not available.

 No image in the nonvolatile memory.



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](#).

3. 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.
- Verify that the controller is not in Run Mode.

4. Click Load.



After you click Load, the project loads 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.

These indications show the load status

Controller	SD Indicator	OK LED on Controller	4-Character Display Message
ControlLogix 5580 controller when restoring firmware or project	Flashing Green	Solid Red	"LOAD", then followed by "UPDT"
GuardLogix 5580 SIL 2 controller when restoring firmware or project	Flashing Green	Solid Red	"LOAD", then followed by "UPDT"
GuardLogix 5580 SIL 3 controller during primary controller firmware update	Flashing Green	Solid Green	"Updating Firmware...Do Not Remove SD Card"
GuardLogix 5580 SIL 3 controller during Safety Partner firmware update	Flashing Green	Solid Green	"Updating Firmware...Do Not Remove SD Card"
GuardLogix 5580 SIL 3 controller during when loading project	Flashing Green	Solid Green	"Loading...Do Not Remove SD Card"

IMPORTANT Let the load complete without interruption. If you interrupt the load, data corruption or loss can occur.

5. When the load is complete, the controller reboots.

Other Secure Digital Card Tasks

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

You can perform these tasks with the SD card:

- Change the image that is loaded from the card
- Check for a load that was completed
- Clear an image from the SD card
- Store an empty image
- Change load parameters
- Read/write application data to the card
- (GuardLogix 5580 controllers only). View safety-lock status and safety signatures on the Nonvolatile Memory tab

For more information to complete any of these tasks, see the Logix 5000 Controllers Memory Card Programming Manual, publication [1756-PM017](#).

Manage Controller Communication

Connection Overview

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controller provides connection resources whenever communications are established between two devices.

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

- I/O modules, communication modules, and adapter modules 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.

Nodes on an EtherNet/IP Network

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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. [Table 14](#) shows the maximum number of EtherNet/IP nodes supported for each controller.

With firmware revision 29 or later, the Ethernet Nodes field on the Controllers Properties Capacity tab keeps a running count as you add EtherNet/IP nodes to the I/O configuration tree. See [Figure 23 on page 86](#).

Table 14 - Maximum Number of Ethernet/IP Nodes Supported

System	Cat. No. ⁽¹⁾	Version 28	Version 29	Version 30	Version 31 or later	Version 36 or later
ControlLogix®	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
GuardLogix®	1756-L81ES, 1756-L81ESK, 1756-L81EXTS	—	—	—	100	100
	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

(1) ControlLogix NSE controllers, ControlLogix-XT controllers, and ControlLogix Process controllers are available with version 32 or later.

IMPORTANT

EtherNet/IP communication modules in the local chassis with the controller do not count as nodes, but EtherNet/IP devices connected to the communication modules do count as nodes. See [Figure 23 on page 86](#).

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, such as I/O modules, drives, and linking devices
- EtherNet/IP devices connected to a communication module in the local chassis, even though the communication module in the local chassis does not count as a node
See [Figure 23 on page 86](#).
- HMI devices that are included in the I/O configuration section, for example, PanelView™ Plus terminals
- 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 example in [Figure 23](#) shows four nodes in the I/O tree.

Figure 23 – EtherNet/IP Nodes Example

Not a node. Module is in local chassis. →

Node →

Not a node. Module is in local chassis. →

Node →

Node →

Node →

Node →

Controller Organizer Logical Organizer

Controller Properties

General	Major Faults	Minor Faults	Date/Time	Advanced	SFC Execution
Safety	Nonvolatile Memory	Capacity	Internet Protocol	Port Configuration	

Standard Capacity

Total: 20,971,520 blocks
Available: 13,478,213 blocks
Used: 7,493,307 blocks

Safety Capacity

Total:
Available:
Used:

Ethernet Nodes

Recommended Maximum: 250 nodes
Used: 81 nodes

OK Cancel

CIP Security Considerations

If you use I/O data security (CIP Security) for safety I/O, the maximum amount of nodes supported is reduced as follows:

$$\text{Number of non-secure nodes} + 2 * (\text{number of secure nodes, integrity only}) + 4 * (\text{number of secure nodes, integrity and confidentiality}) \leq 150$$

or

Maximum nodes supported by the controller, **whichever is less**.

If you do not use secure connections, the maximum number of nodes are dictated by the controller catalog number. See [Table 14 on page 85](#).

Controller Communication Interaction with Control Data

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controller runs the communications task separately from the application code. The controller runs communications asynchronously to the application. Therefore, it is important to make sure communications that are delivered to the controller are 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.

Traditionally, programmers have used the following to control the effects of asynchronous communications:

- UID/UIE pairs
- Periodic tasks
- Moving data with CPS instructions

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 communications on an independent CPU core, these methods are no longer effective in all cases.

[Table 15](#) highlights the controllers behavior.

Table 15 - ControlLogix 5580 and GuardLogix 5580 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	Blocks	Blocks
Periodic Tasks	Allows	Allows	Allows	Allows	Allows	Allows

Blocks—Helps to prevent source data values from change by communications during application execution.

Allows—Communications can change source data values during application execution.

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.

[Table 16](#) shows 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 communications is in the process of filling the structure. The same applies to higher-level systems that are receiving data from the controller.

Table 16 - 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



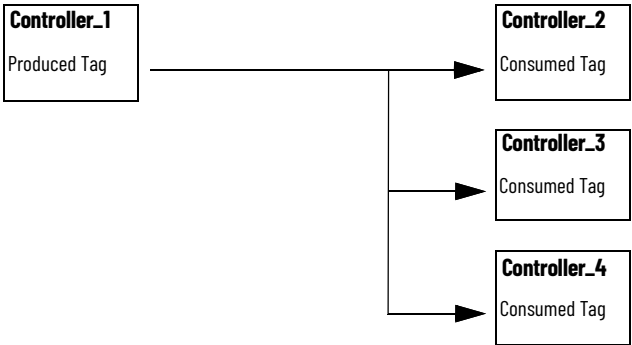
We recommend that you perform this test on a buffered copy of the data and not the actual data element being written to by the communications core. If you use buffered data, you help prevent the risk of the communication core changing data after you have passed the data valid test.

Produce and Consume
(Interlock) Data

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

The controllers let you produce (transmit) and consume (receive) controller-scoped tags. ControlLogix 5580 controllers and GuardLogix 5580 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 24 - Illustration of Produced and Consumed Tags



[Table 17](#) describes the system-shared tags.

Table 17 - 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 connections of the controller and the communication modules being used.

For information about produced/consumed safety tags, 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.

Table 18 - ControlNet Connections

Connection	Definition
Scheduled (unique to a ControlNet network)	<p>A scheduled connection is unique to ControlNet communication. A scheduled connection lets you send and receive data repeatedly at a predetermined interval, which is the requested packet interval (RPI). For example, a connection to an I/O module is a scheduled connection because you repeatedly receive data from the module at a specified interval.</p> <p>Other scheduled connections include connections to the following:</p> <ul style="list-style-type: none"> • Communication devices • Produced/consumed tags <p>On a ControlNet network, you must use RSNetWorx™ for ControlNet software to enable all scheduled connections and establish a network update time (NUT). A scheduled connection reserves network bandwidth specifically to handle the connection.</p>
Unscheduled	<p>An unscheduled connection is a message transfer between devices that the requested packet interval (RPI) or the program, such as a MSG instruction, triggers. Unscheduled messaging lets you send and receive data as you need.</p> <p>Unscheduled connections use the remainder of network bandwidth after scheduled connections are allocated.</p>

Requested Packet Interval (RPI) of Multicast Tags

The first consumer of a multicast produced tag on any given communications 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 will fail to connect. Controllers with backplane and EtherNet/IP 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

Applies to these controllers:

ControlLogix 5580
GuardLogix 5580

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 of the 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.

Table 19 - Message Types

Message Type	Communication Method	Connected Message	Message Can Be Cached
CIP™ data table read or write	N/A	Configurable	Yes ⁽²⁾
PLC-2®, PLC-3®, PLC-5®, or SLC™ (all types)	CIP	No	No
	CIP with Source ID	No	No
	DH+™	Yes	Yes ⁽²⁾
CIP generic	N/A	Optional ⁽¹⁾	Yes ⁽²⁾
Block-transfer read or write	N/A	Yes	Yes ⁽²⁾

(1) You can connect CIP generic messages. However, for most applications we recommend that you leave CIP generic messages unconnected.

(2) Connected messages that occur more frequently than once every 60 seconds should be cached if possible.

For more information about using messages, see the Logix 5000 Controllers Messages Programming Manual, publication [1756-PM012](#).

Determine Whether to Cache Message Connections

When you configure a MSG instruction, you can choose whether to cache the connection. Use [Table 20](#) to determine options for caching connections.

Table 20 - Options for Caching Connections

If the message executes	Then
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.



Cached connections transfer data faster than uncached connections. The controllers can cache 256 messages and trigger 256 messages simultaneously.

Socket Interface

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controller can use socket interfaces to communicate with Ethernet devices that do not support the EtherNet/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.

The controllers support up to 32 socket instances on a per-module basis: 32 sockets for the embedded Ethernet port, plus 32 more for each Ethernet bridge module in the local chassis.

These products support a secure socket object:

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

For more information on the socket interface, see 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

Simple Network Management Protocol (SNMP)

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.

For more information about SNMP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

Use a CIP Generic MSG to Enable SNMP on the Controller

1. Add a MSG instruction to your program.

IMPORTANT You cannot add a 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 tab on the Message Configuration dialog box as described in [Table 21 on page 93](#).

The screenshot shows the 'Message Configuration' dialog box with the 'Configuration' tab selected. The 'Message Type' is set to 'CIP Generic'. The 'Service Type' is 'Custom'. The 'Source' is 'onArray' with a 'Source Length' of 5 bytes. The 'Service Code' is '4c' (Hex), 'Class' is 'f5' (Hex), 'Instance' is '1', and 'Attribute' is '0' (Hex). The 'Destination Element' is empty, with a 'New Tag...' button next to it. At the bottom, there are radio buttons for 'Enable', 'Enable Waiting', 'Start', and 'Done'. The 'Done Length' is 0. There are also fields for 'Error Code', 'Extended Error Code', 'Error Path' (R010), 'Error Text', and a 'Timed Out' checkbox.

Configuration*	Communication	Tag
<p>Message Type: CIP Generic</p> <p>Service Type: Custom</p> <p>Source: onArray</p> <p>Source Length: 5 (Bytes)</p> <p>Service Code: 4c (Hex) Class: f5 (Hex)</p> <p>Instance: 1 Attribute: 0 (Hex)</p> <p>Destination Element: [Empty] New Tag...</p>		
<p> <input type="radio"/> Enable <input type="radio"/> Enable Waiting <input type="radio"/> Start <input type="radio"/> Done Done Length: 0 </p> <p> <input type="radio"/> Error Code: Extended Error Code: <input type="checkbox"/> Timed Out </p> <p>Error Path: R010</p> <p>Error Text:</p>		
<p>OK Cancel Apply Help</p>		

Table 21 - Enable SNMP

Field	Description																												
Message Type	CIP Generic																												
Service Type	Custom																												
Service Code	4c																												
Instance	1																												
Class	f5																												
Attribute	0																												
Source Element	<p>Controller tag of USINT[5] data type. In this example, the controller tag is named onArray and must match the following graphic.</p> <table><thead><tr><th>Name</th><th>Value</th><th>Style</th><th>Data Type</th></tr></thead><tbody><tr><td>onArray</td><td>{...}</td><td>Decimal</td><td>USINT[5]</td></tr><tr><td>onArray[0]</td><td>1</td><td>Decimal</td><td>USINT</td></tr><tr><td>onArray[1]</td><td>161</td><td>Decimal</td><td>USINT</td></tr><tr><td>onArray[2]</td><td>0</td><td>Decimal</td><td>USINT</td></tr><tr><td>onArray[3]</td><td>17</td><td>Decimal</td><td>USINT</td></tr><tr><td>onArray[4]</td><td>1</td><td>Decimal</td><td>USINT</td></tr></tbody></table> <p>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.</p>	Name	Value	Style	Data Type	onArray	{...}	Decimal	USINT[5]	onArray[0]	1	Decimal	USINT	onArray[1]	161	Decimal	USINT	onArray[2]	0	Decimal	USINT	onArray[3]	17	Decimal	USINT	onArray[4]	1	Decimal	USINT
Name	Value	Style	Data Type																										
onArray	{...}	Decimal	USINT[5]																										
onArray[0]	1	Decimal	USINT																										
onArray[1]	161	Decimal	USINT																										
onArray[2]	0	Decimal	USINT																										
onArray[3]	17	Decimal	USINT																										
onArray[4]	1	Decimal	USINT																										
Source Length	5																												

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

IMPORTANT Messages to THIS must be unconnected messages.

The screenshot shows the 'Message Configuration' dialog box with the 'Communication' tab selected. The 'Path' is set to 'THIS'. The 'Communication Method' is set to 'CIP'. The 'Channel' is set to 'A'. The 'Destination Link' is set to '0'. The 'Source Link' is set to '0'. The 'Destination Node' is set to '0' (Octal). The 'Connected' checkbox is unchecked. The 'Cache Connections' checkbox is unchecked. The 'Large Connection' checkbox is unchecked. The 'Enable' radio button is selected. The 'Done Length' is set to '0'. The 'Error Code' is set to 'R010'. The 'Error Text' is empty. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Use a CIP Generic MSG to Disable SNMP on the Controller

1. Add a MSG instruction to your program.

IMPORTANT

You cannot add a 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 tab on the Message Configuration dialog box as described in [Table 22](#).

Table 22 - Disable SNMP

Field	Description																		
Message Type	CIP Generic																		
Service Type	Custom																		
Service Code	4c																		
Instance	1																		
Class	f5																		
Attribute	0																		
Source Element	<div>Controller tag of USINT[5] data type. In this example, the controller tag is named offArray and must match the following graphic:</div> <table><tr><th>▾ offArray</th><th>{...} Decimal</th><th>USINT[5]</th></tr><tr><td>▸ offArray[0]</td><td>1 Decimal</td><td>USINT</td></tr><tr><td>▸ offArray[1]</td><td>161 Decimal</td><td>USINT</td></tr><tr><td>▸ offArray[2]</td><td>0 Decimal</td><td>USINT</td></tr><tr><td>▸ offArray[3]</td><td>17 Decimal</td><td>USINT</td></tr><tr><td>▸ offArray[4]</td><td>0 Decimal</td><td>USINT</td></tr></table> <div>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 disabled.</div>	▾ offArray	{...} Decimal	USINT[5]	▸ offArray[0]	1 Decimal	USINT	▸ offArray[1]	161 Decimal	USINT	▸ offArray[2]	0 Decimal	USINT	▸ offArray[3]	17 Decimal	USINT	▸ offArray[4]	0 Decimal	USINT
▾ offArray	{...} Decimal	USINT[5]																	
▸ offArray[0]	1 Decimal	USINT																	
▸ offArray[1]	161 Decimal	USINT																	
▸ offArray[2]	0 Decimal	USINT																	
▸ offArray[3]	17 Decimal	USINT																	
▸ offArray[4]	0 Decimal	USINT																	
Source Length	5																		

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

IMPORTANT Messages to THIS must be unconnected messages.

The screenshot shows the 'Message Configuration' dialog box with the 'Communication' tab selected. The 'Path' is set to 'THIS' with a 'Browse...' button. Below it, 'Broadcast' is set to a dropdown menu. The 'Communication Method' section has 'CIP' selected, with 'Channel' set to 'A' and 'Destination Link' set to '0'. 'CIP With Source ID' is also an option. 'Source Link' is set to '0' and 'Destination Node' is set to '0' (Octal). There are checkboxes for 'Connected', 'Cache Connections', and 'Large Connection'. At the bottom, there are radio buttons for 'Enable', 'Enable Waiting', 'Start', and 'Done', along with 'Done Length' set to '0'. There are also fields for 'Error Code', 'Extended Error Code', and a 'Timed Out' checkbox. The 'Error Path' is 'R010' and 'Error Text' is empty. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom right.

Message Configuration

Configuration* Communication* Tag

☒ Path: THIS Browse...

THIS

☐ Broadcast: ▼

Communication Method

☒ CIP ☐ DH+ Channel: 'A' ▼ Destination Link: 0 ▲▼

☐ CIP With Source ID Source Link: 0 ▲▼ Destination Node: 0 ▲▼ (Octal)

☐ Connected ☐ Cache Connections ☐ Large Connection

☐ Enable ☐ Enable Waiting ☐ Start ☐ Done Done Length: 0

☐ Error Code: Extended Error Code: ☐ Timed Out ▲

Error Path: R010

Error Text:

OK Cancel Apply Help

Notes:

Standard I/O Modules

Selecting ControlLogix I/O Modules

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Rockwell Automation offers many I/O modules for use in ControlLogix® controller systems. For a list of all I/O product lines that are compatible with the ControlLogix controllers, see the 1756 ControlLogix Controllers Technical Data, publication [1756-TD001](#).

When you select I/O modules, remember the following:

- A wide variety of digital, analog, and specialty I/O modules are available from Rockwell Automation. A number of these 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 use with I/O modules, and you may have to order these separately.
- 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 that 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: <ul style="list-style-type: none">• Same catalog number• Same or higher Major Revision• Minor Revision as follows:<ul style="list-style-type: none">- 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. 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.
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

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 23 - 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.

Add Local I/O to the I/O Configuration

If you are adding local I/O, add the I/O module to the backplane with the controller. To add an I/O module to the local chassis, complete these steps.

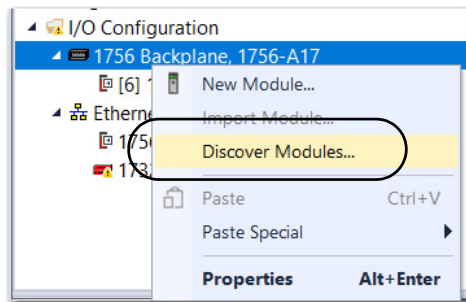
There are two methods to add local I/O modules to the project:

- [Discover Modules on page 99](#)
- [New Module on page 101](#)

Discover Modules

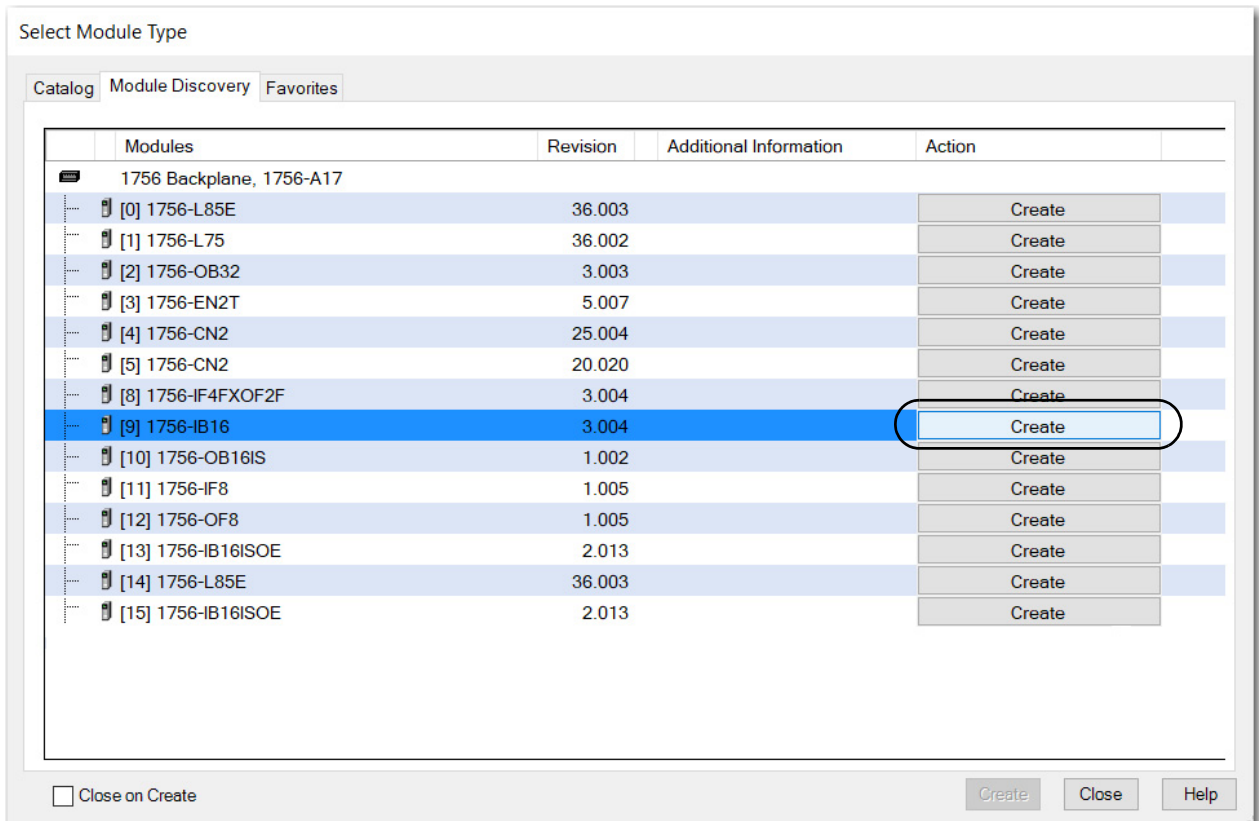
To use Discover Modules to add a local I/O module, complete these steps.

1. Go online with your controller.
2. In the I/O configuration, right-click the 1756 backplane and select Discover Modules.

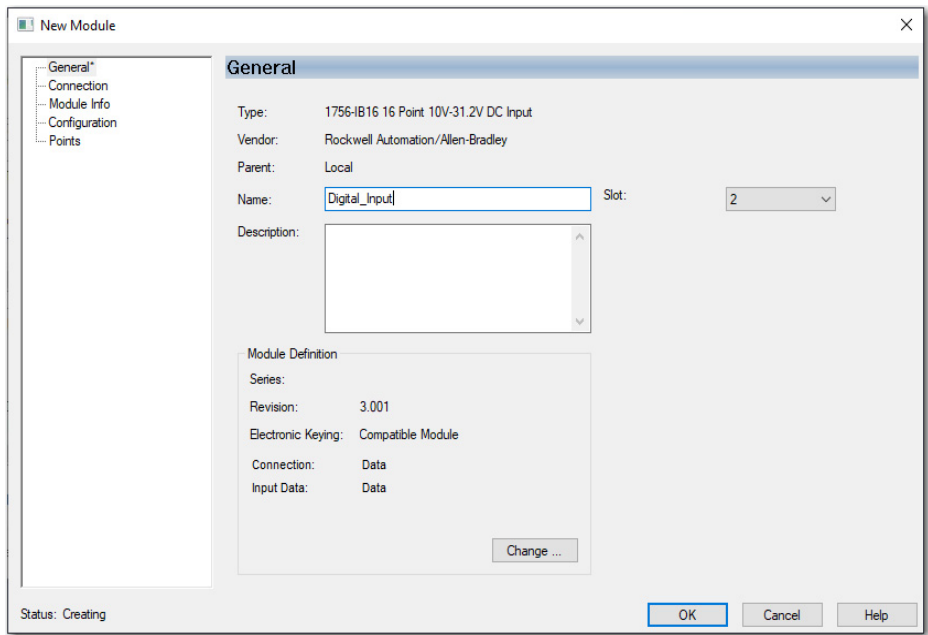


The Logix Designer application automatically detects available modules that are installed in the system.

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



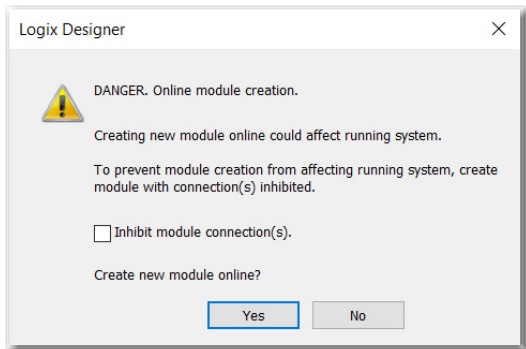
4. Configure the properties for the new module and click OK.



5. At the warning dialog box, click Yes.



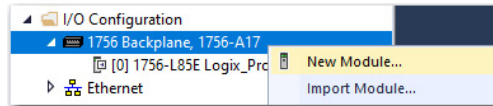
If you inhibit the module connection, you must remember to uninhibit the connection later.



6. Close the Select Module Type dialog box.

New Module

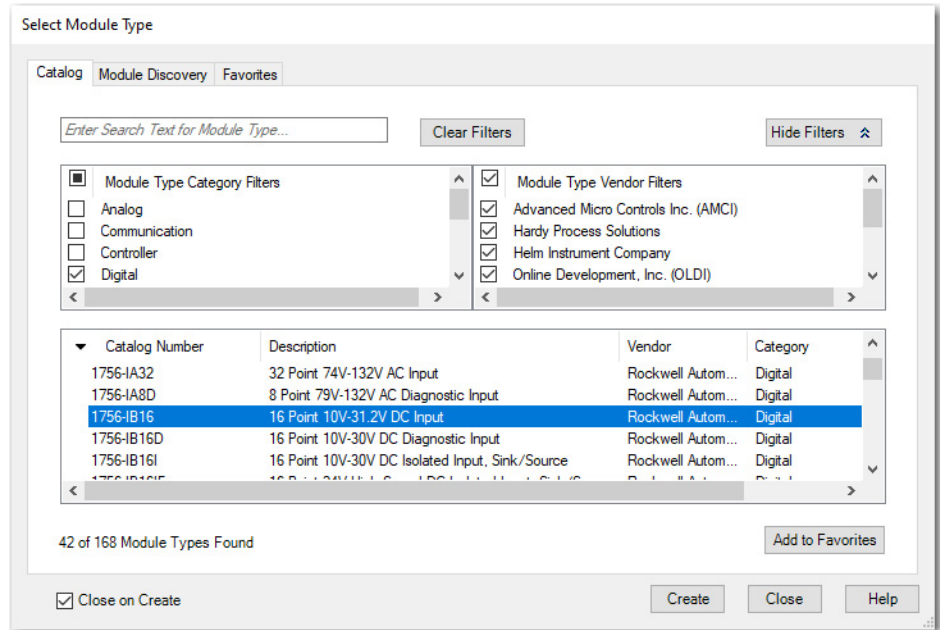
1. In the I/O configuration, right-click the backplane and select New Module.



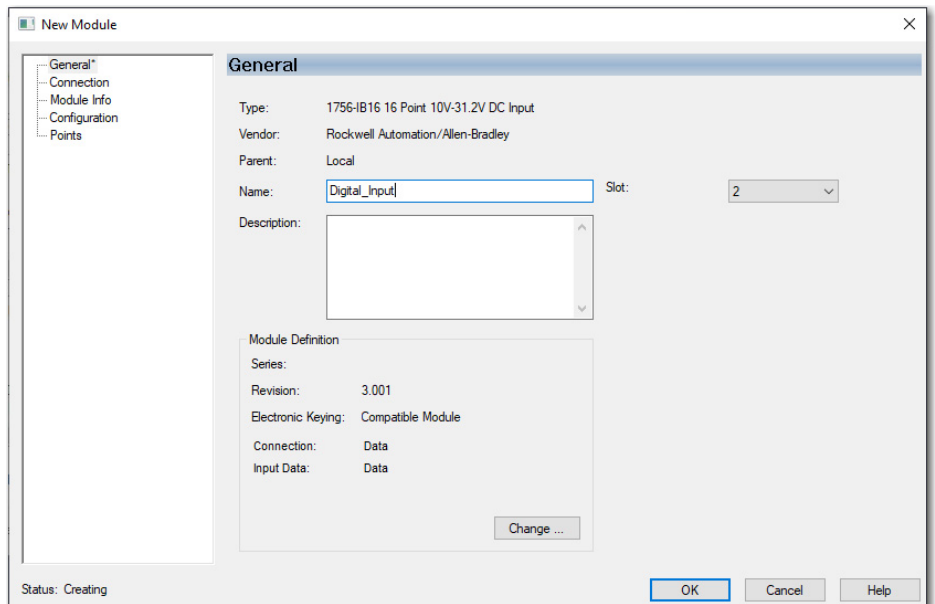
2. On the Select Module Type dialog box, select the I/O module and click Create.



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

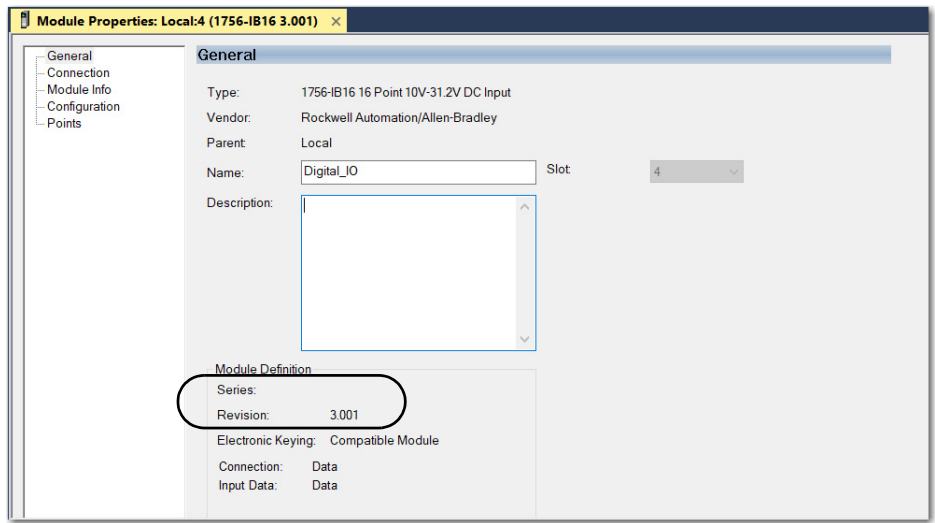


3. On the New Module dialog box, configure the module and click OK.





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

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

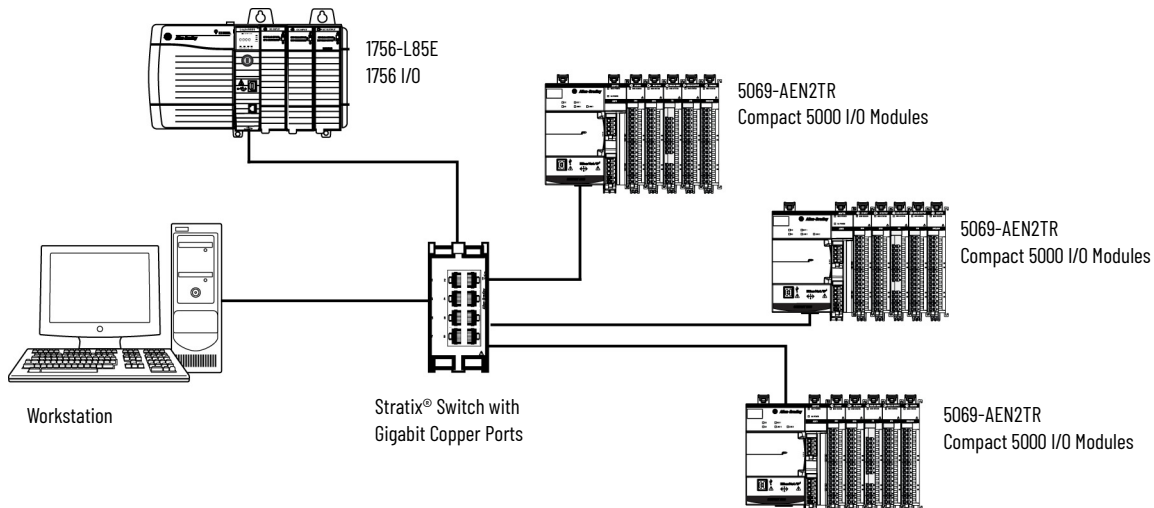
- Compact 5000™ I/O modules in a remote bank using a 5069-AEN2TR or similar adapter
- 1756 I/O in a remote chassis via a Network Bridge Module
- Distributed I/O families such as POINT I/O™ or Block I/O™
- On-Machine™ I/O families such as ArmorPOINT® or ArmorBlock® I/O

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

- EtherNet/IP™
- ControlNet®
- 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 35](#).

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

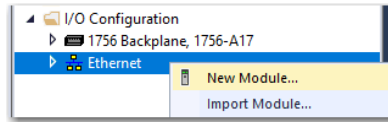


Add Remote I/O to the Ethernet Port on the Controller

If you are adding remote I/O, you can add the I/O modules to the Ethernet port of the controller. To add remote I/O to the I/O configuration of the controller 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.

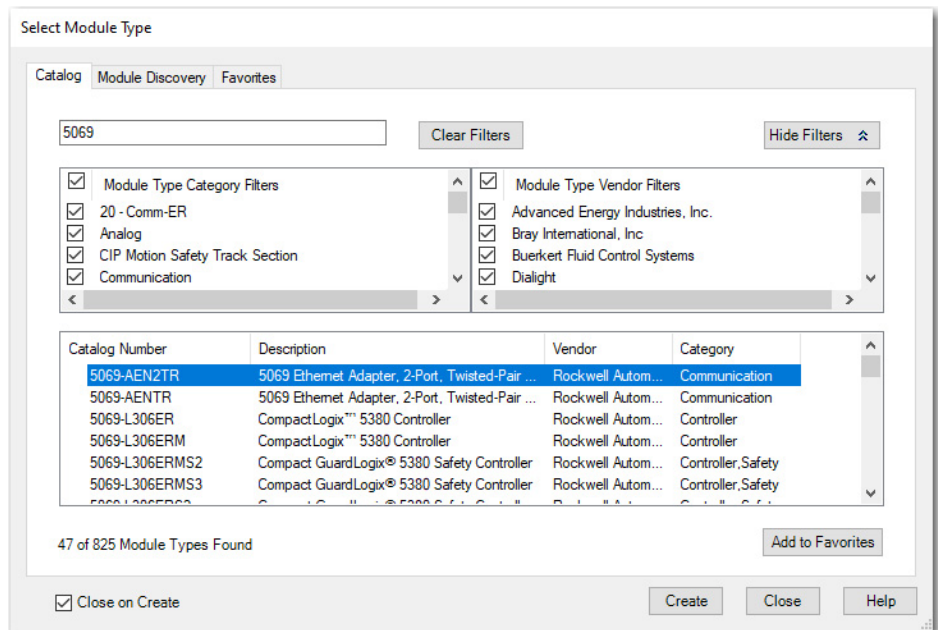


2. On the Select Module Type dialog box, select the remote communication module or EtherNet/IP device and click Create.



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

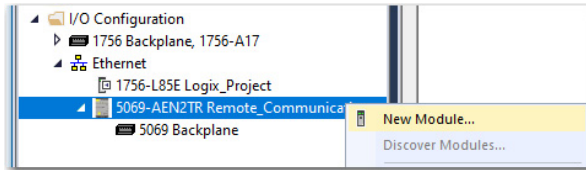
For some modules, the Select Major Revision dialog box can appear. If the dialog box appears, choose the major revision of the module and click OK.



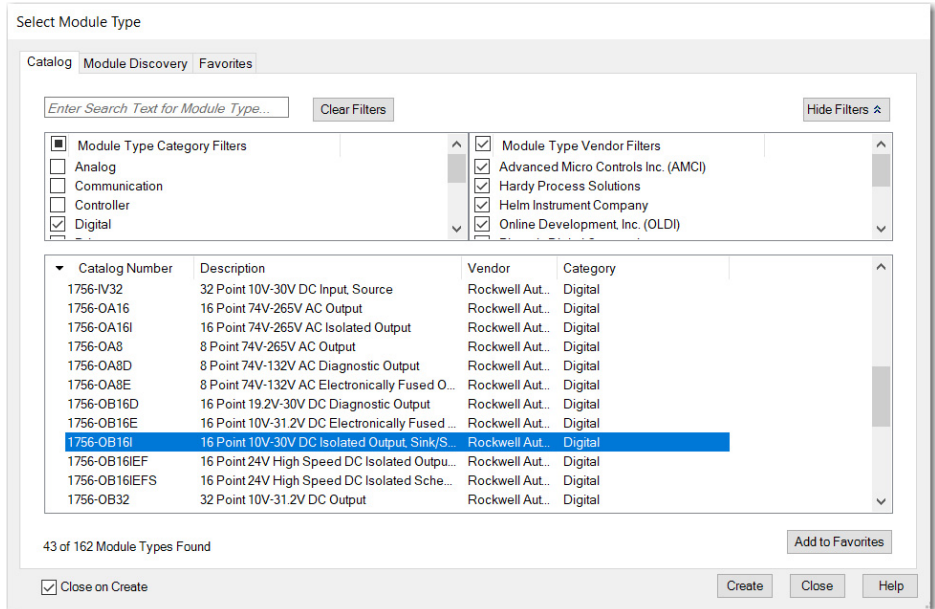
- Specify the communication module properties according to your network configuration and click OK.

For more information about the communication module and network properties, see [Additional Resources on page 9](#).

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



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

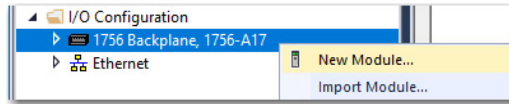


- Specify the Module Properties according to your module and application and click OK.

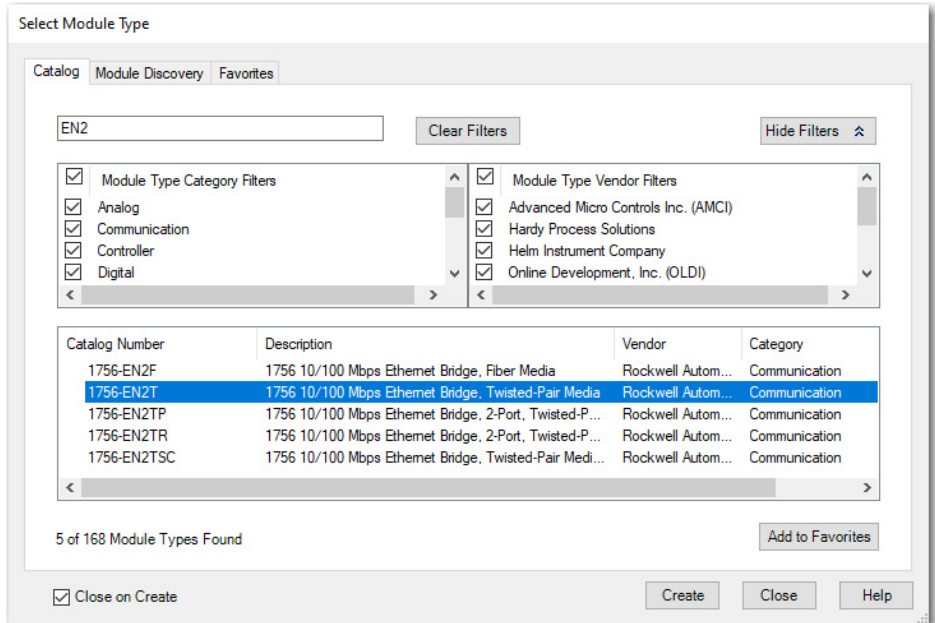
Add Remote I/O to a Local Communication Module

If you are using local communication modules that are connected to the controller, then 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.

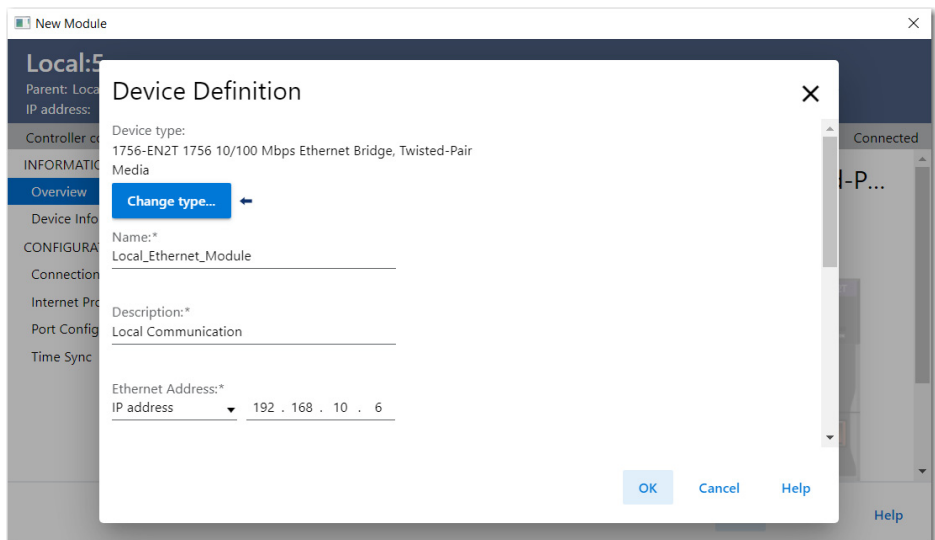
1. Right-click the backplane of the local chassis and select New Module.



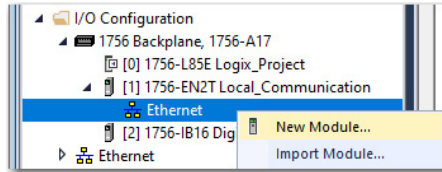
2. On the Select Module Type dialog box, select a communication module and click Create.



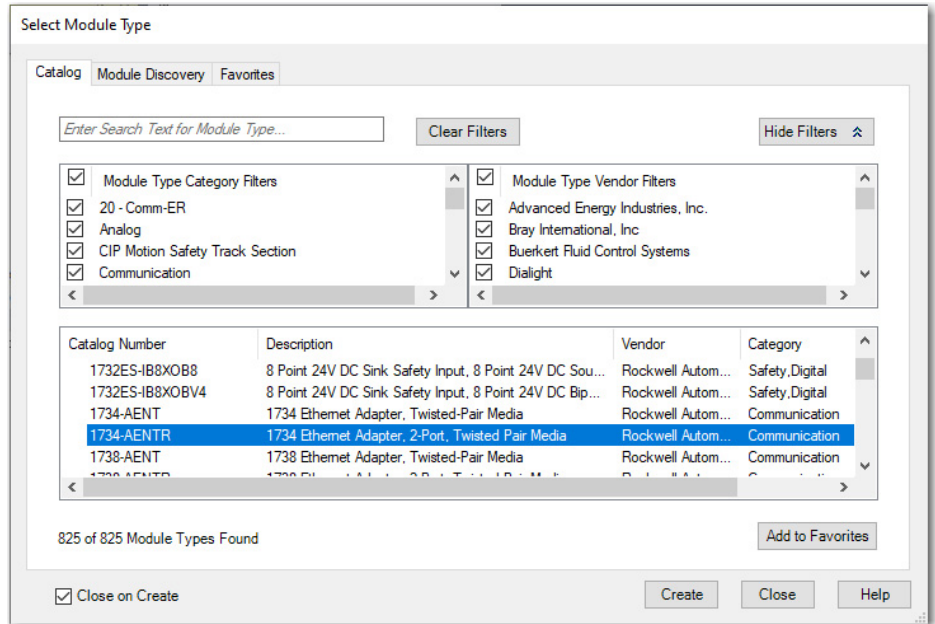
3. Specify the communication module properties according to your network configuration and click OK.



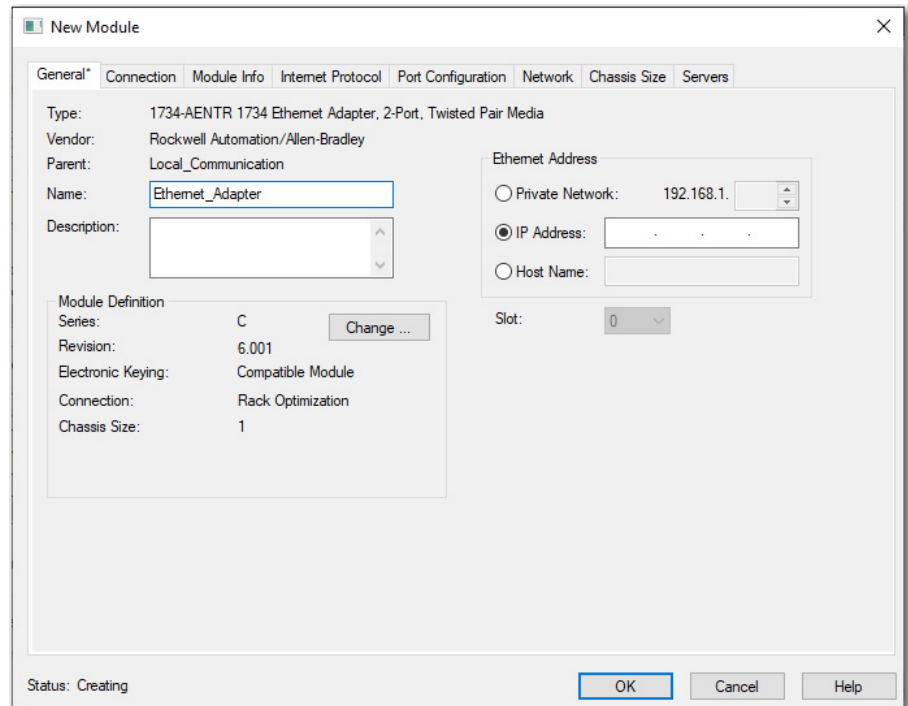
- Right-click the communication network under the communication module and select New Module.



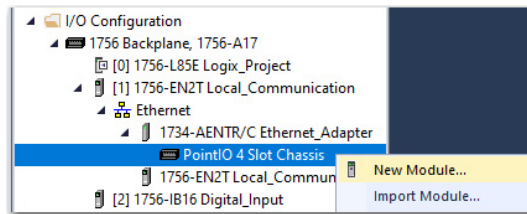
- Select the communication adapter for the I/O platform that you are using and click Create.



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



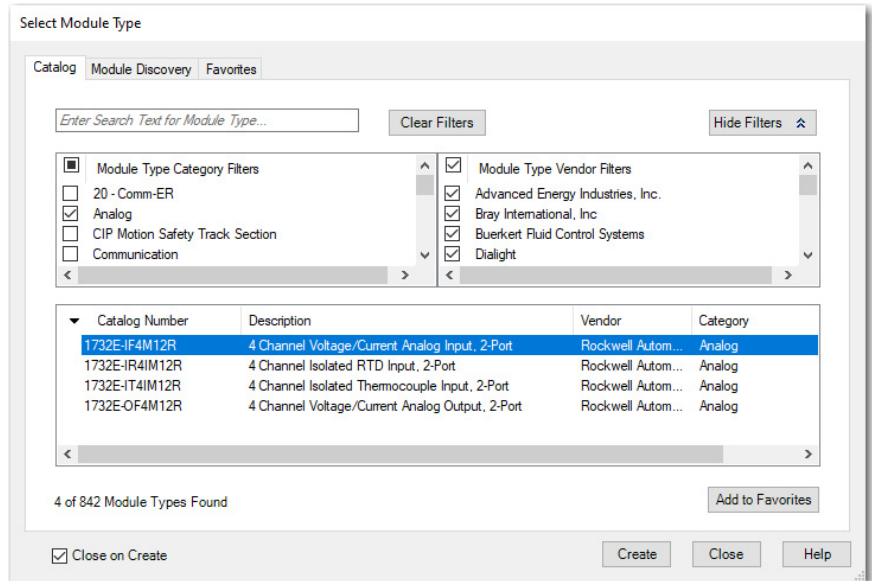
7. Right-click the backplane of the newly added communication adapter and select New Module.



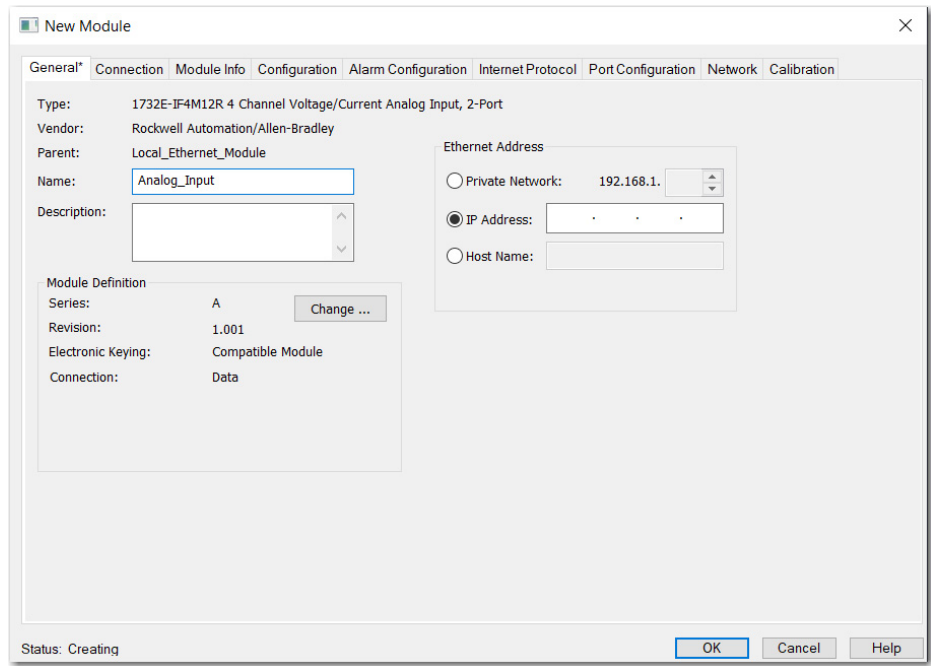
8. On the Select Module Type dialog box, select the I/O module to add and click Create.



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

Applies to these controllers:

ControlLogix 5580
GuardLogix 5580

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 [Nodes on an EtherNet/IP Network on page 85](#).

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 Logix Designer, version 28.00.00 or later.

- 1756 controllers
- 1756 ControlNet modules
- 1756 DeviceNet bridges
- 1756 EtherNet/IP modules
- Compact 5000 EtherNet/IP adapters and I/O modules
- FLEX 5000™ EtherNet/IP adapters and I/O modules
- 1756 I/O and specialty modules
- 1756-DHRIO
- 1756-DHRIOXT

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
-

Determine When Data is Updated

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

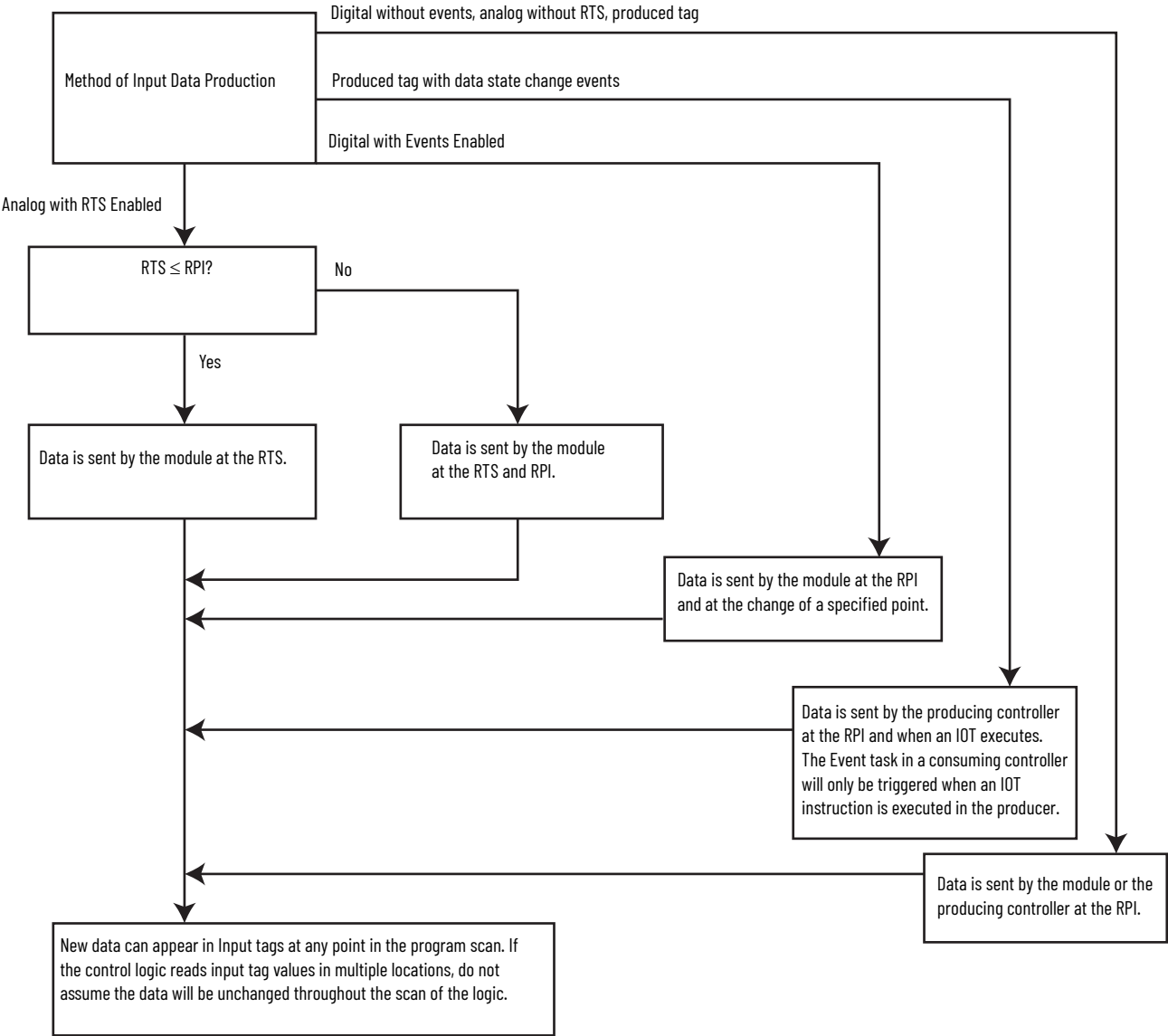
ControlLogix controllers update data asynchronously with the execution of logic. See these flowcharts to determine when a controller, input module, or bridge sends data:

- [Input Data Update Flowchart](#) on this page
- [Output Data Update Flowchart on page 111](#)

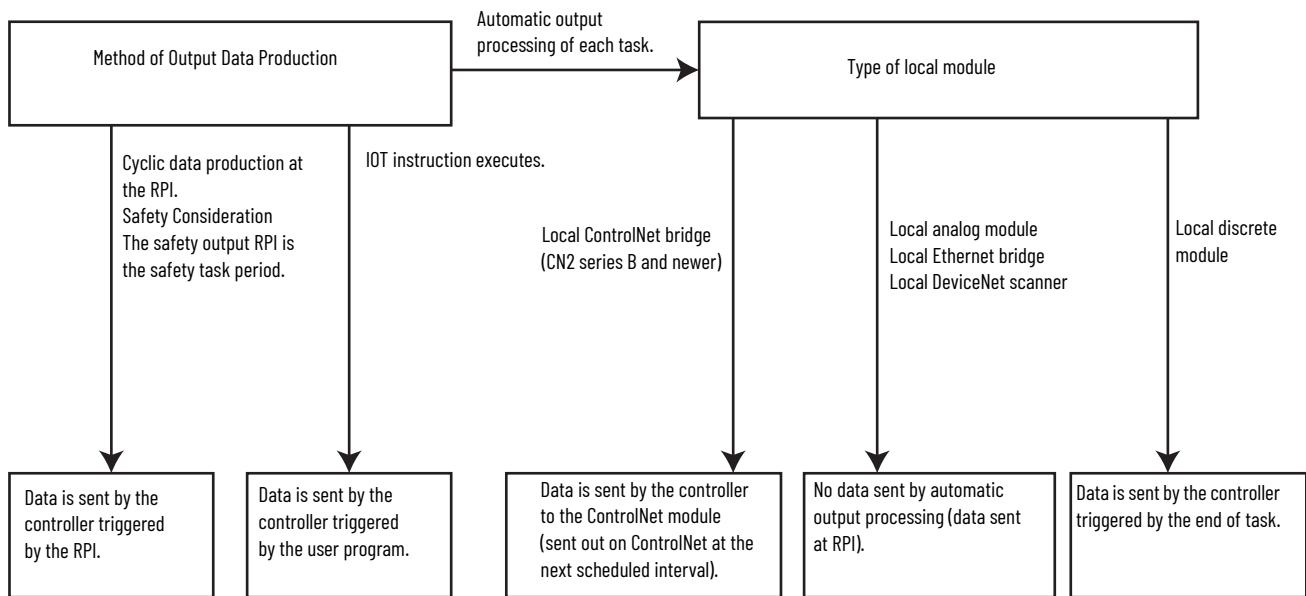
Input Data Update Flowchart

IMPORTANT Safety Consideration

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.



Output Data Update Flowchart



Notes:

Safety I/O Devices

Add Safety I/O Devices

Applies to these controllers:

GuardLogix 5580

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

- IP address for EtherNet/IP™ networks.
- Safety network number (SNN). To set the SNN, see page [page 116](#).
- Configuration signature. For information on when the configuration signature is set automatically and when you need to set it, see page [page 120](#).
- Reaction time limit. For information on setting the reaction time limit, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems 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.

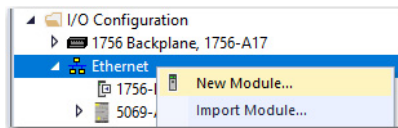
Configure Safety I/O Devices

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.



- 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.

Select Module Type

Catalog Module Discovery Favorites

Enter Search Text for Module Type... Clear Filters Hide Filters

☒ Module Type Category Filters

- ☒ Safety
- ☐ SCANport to EtherNet/IP
- ☐ Specialty
- ☐ UPS (Uninterruptible Power Supply)

☒ Module Type Vendor Filters

- ☒ Advanced Energy Industries, Inc.
- ☒ Bray International, Inc.
- ☒ Buerkert Fluid Control Systems
- ☒ Dialight

Catalog Number	Description	Vendor	Category
1732ES-IB12XOB4	12 Point 24V DC Sink Safety Input, 4 Point 24...	Rockwell Aut...	Safety.Digital
1732ES-IB12XOBV2	12 Point 24V DC Sink Safety Input, 4 Point 24...	Rockwell Aut...	Safety.Digital
1732ES-IB16	16 Point 24V DC Sink Safety Input	Rockwell Aut...	Safety.Digital
1732ES-IB8XOB8	8 Point 24V DC Sink Safety Input, 8 Point 24...	Rockwell Aut...	Safety.Digital
1732ES-IB8XOBV4	8 Point 24V DC Sink Safety Input, 8 Point 24...	Rockwell Aut...	Safety.Digital
1756-L81ES	GuardLogix® 5580 Safety Controller	Rockwell Aut...	Controller,Safety
1756-L82ES	GuardLogix® 5580 Safety Controller	Rockwell Aut...	Controller,Safety
1756-L83ES	GuardLogix® 5580 Safety Controller	Rockwell Aut...	Controller,Safety
1756-L84ES	GuardLogix® 5580 Safety Controller	Rockwell Aut...	Controller,Safety
1769-L30ERMS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety
1769-L33ERMS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety
1769-L36ERMS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety

167 of 861 Module Types Found Add to Favorites

☒ Close on Create Create Close Help

- 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 115](#).

New Module

General* Connection Safety Module Info Input Configuration Test Output Internet Protocol Port Configuration Network

Type: 1732ES-IB16 16 Point 24V DC Sink Safety Input

Vendor: Rockwell Automation/Allen-Bradley

Parent: DistribIO_2

Name: Safety_Input

Description:

Ethernet Address

☒ Private Network: 192.168.1. 15

☐ IP Address:

Advanced...

Module Definition

Series: A Change ...

Revision: 1.001

Electronic Keying: Compatible Module

Controlled By: This Controller

Input Data: Safety

Output Data: Test

Input Status: None


Safety Network Number: 49E5_032A_8488

10/17/2023 9:45:18.88 AM

Status: Creating OK Cancel Help

- To modify the module definition settings, click Change.

IMPORTANT For safety I/O devices, do not use Disable Keying.
See [Electronic Keying on page 97](#).

5. To modify the safety network number, click the  button.
See [Set the SNN of a Safety I/O Device on page 116](#).
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 Controller Systems 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

Applies to these controllers:

GuardLogix 5580

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.

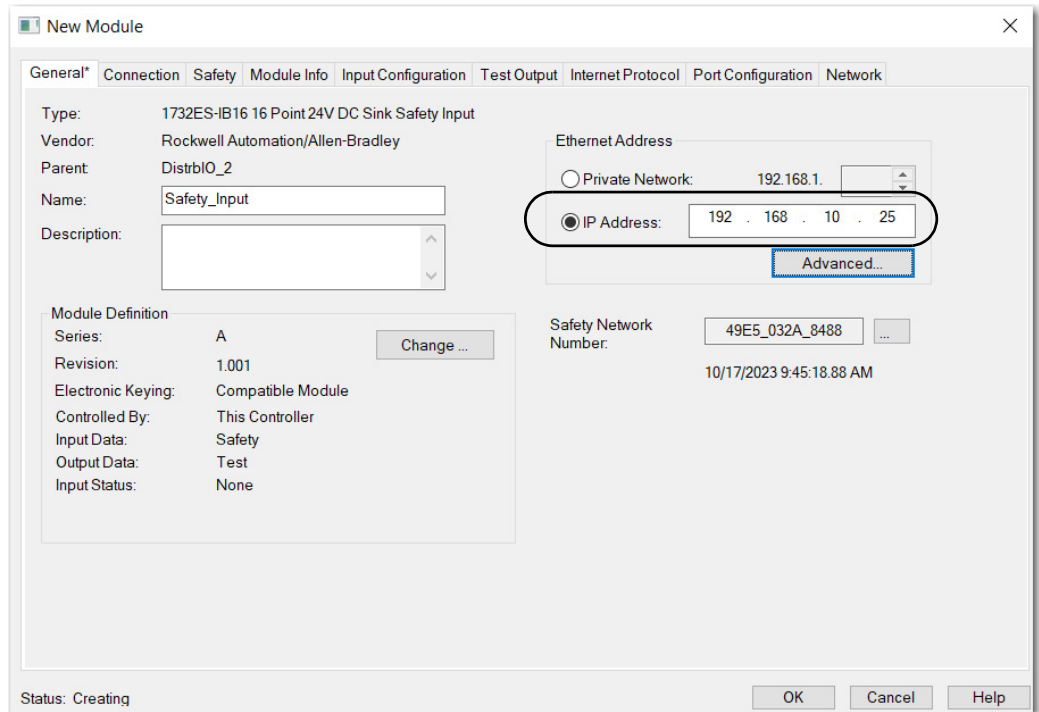
This service is useful if you need to reuse IP addresses throughout a network. For example, NAT makes it possible for devices to be segmented into multiple identical private subnets while maintaining unique identities on the public subnet, such as for multiple identical machines or lines.

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'd IP address. The controller uses the translated address, but the CIP Safety protocol requires the actual address of the device.

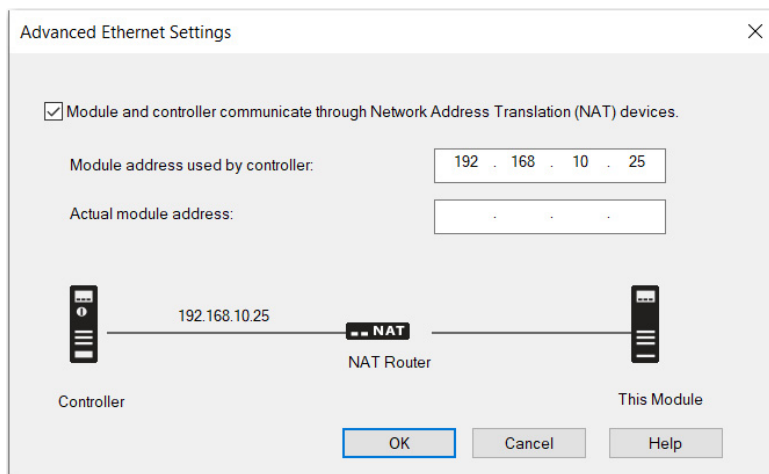
If you use NAT to communicate with a CIP Safety device, follow these steps to set the IP address.

1. In the IP Address field, type the IP address that the controller will use.
This is usually the IP address on the public network when using NAT.



The screenshot shows the 'New Module' dialog box with the 'Network' tab selected. The 'Ethernet Address' section has the 'IP Address' radio button selected, and the IP address '192.168.10.25' is entered in the field. The 'Advanced...' button is visible below the IP address field. The 'Safety Network Number' is set to '49E5_032A_8488'.

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



- Select the checkbox to indicate that this device and the controller communicate through NAT devices.
- 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 shown on the Internet Protocol tab.

- 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 in the case of ports attached to the controller. For most applications, the automatic, time-based SNN is sufficient.

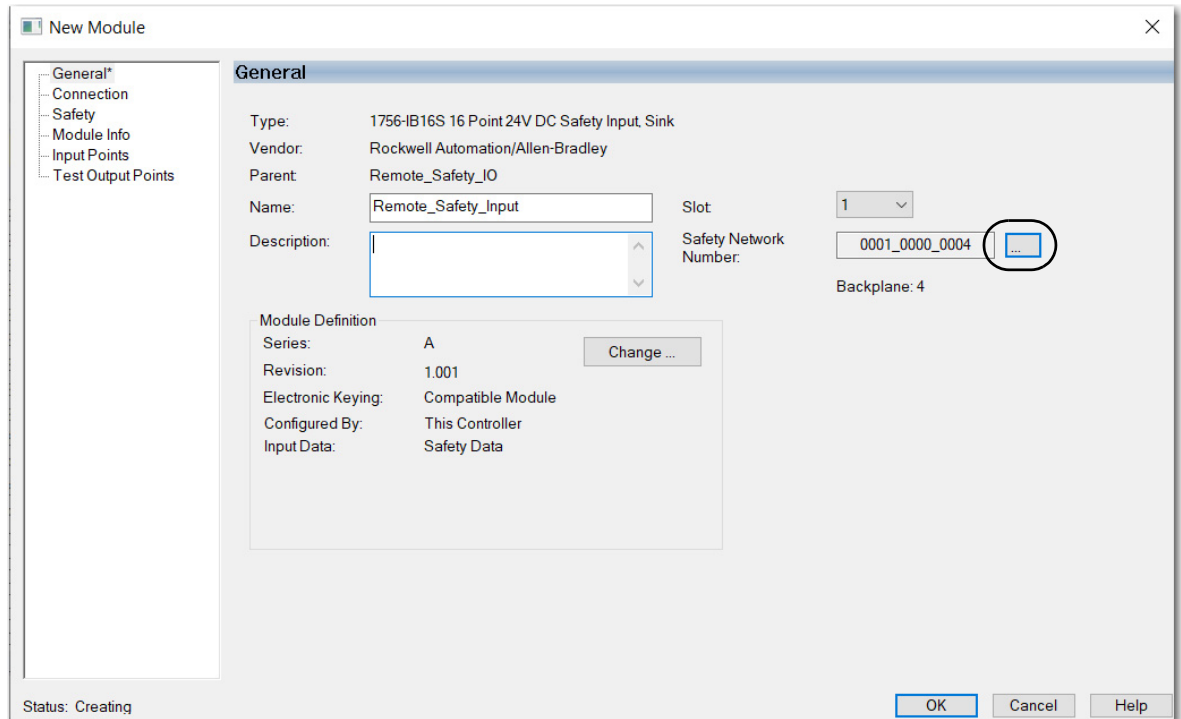
If your application requires you to manually assign the SNN of safety I/O devices, you only have to assign the SNN of the first safety I/O device you add in a remote network or backplane. Logix Designer then assigns the SNN of the first device to any additional devices that you add to that same remote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

For an explanation on SNN, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

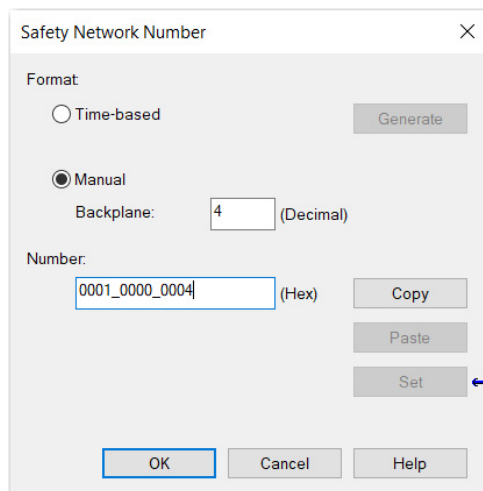
Change a Safety I/O Device SNN

Follow these steps to change the safety I/O device SNN to a manual assignment.

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 click Create.
3. On the New Module dialog box, click  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 click OK.



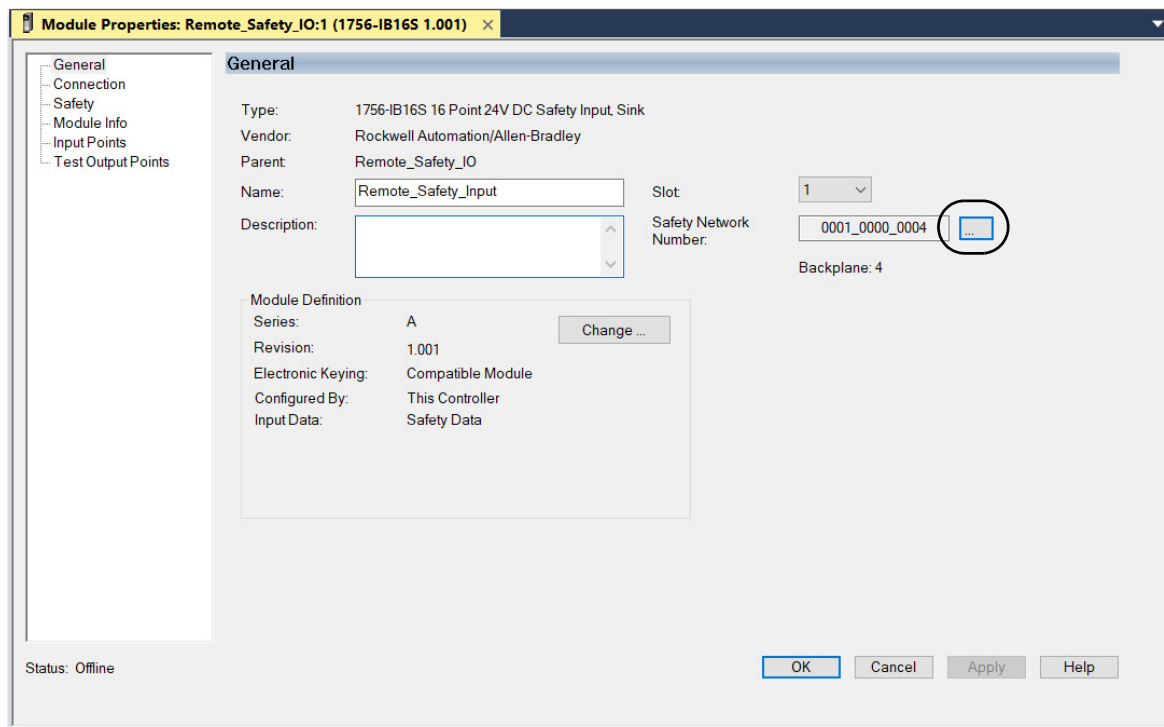
6. On the New Module dialog box, click OK.

Copy and Paste a Safety I/O Device SNN

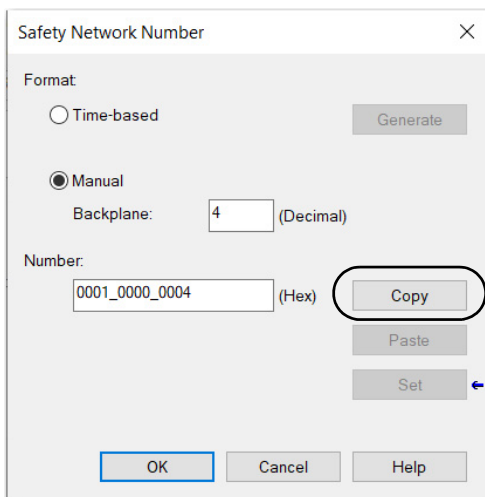
If you must apply an SNN to other safety I/O devices, you can copy and paste the SNN.

Copy an SNN


1. On the General view of the Module Properties dialog box, click  to the right of the SNN.

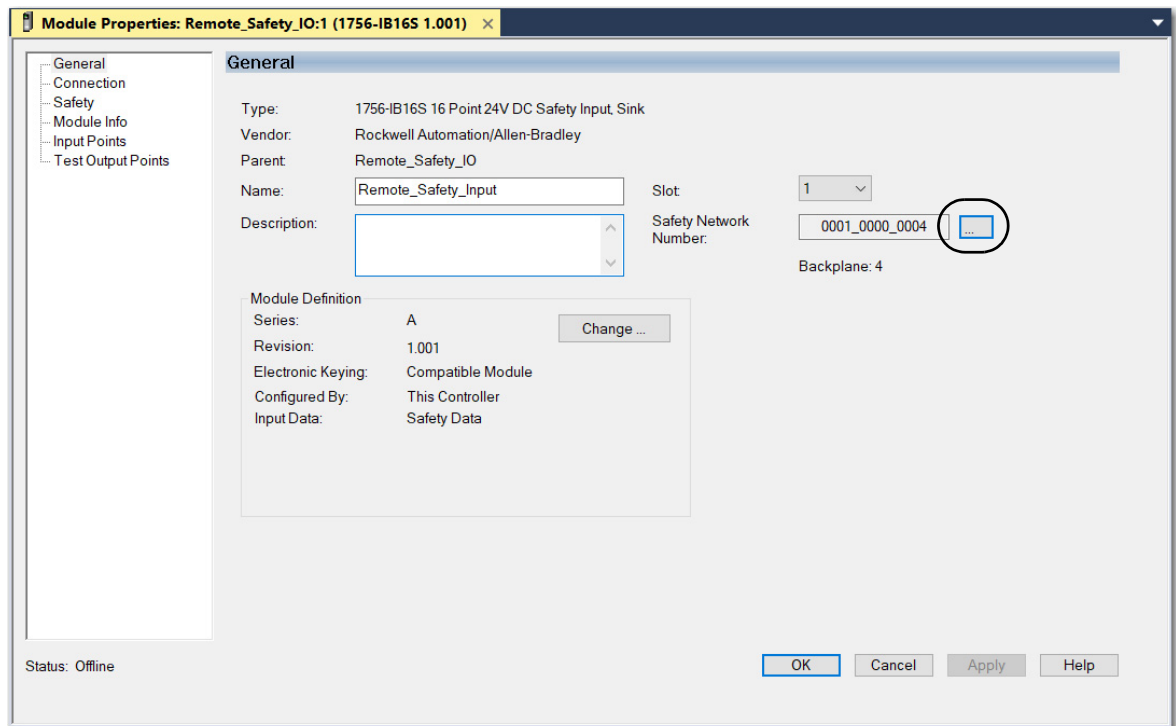


2. On the Safety Network Number dialog box, click Copy.

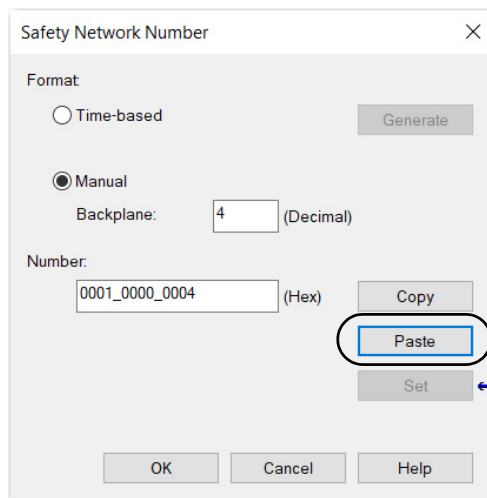


Paste an SNN

1. On the General view of the Module Properties dialog box, click  to the right of the SNN.



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



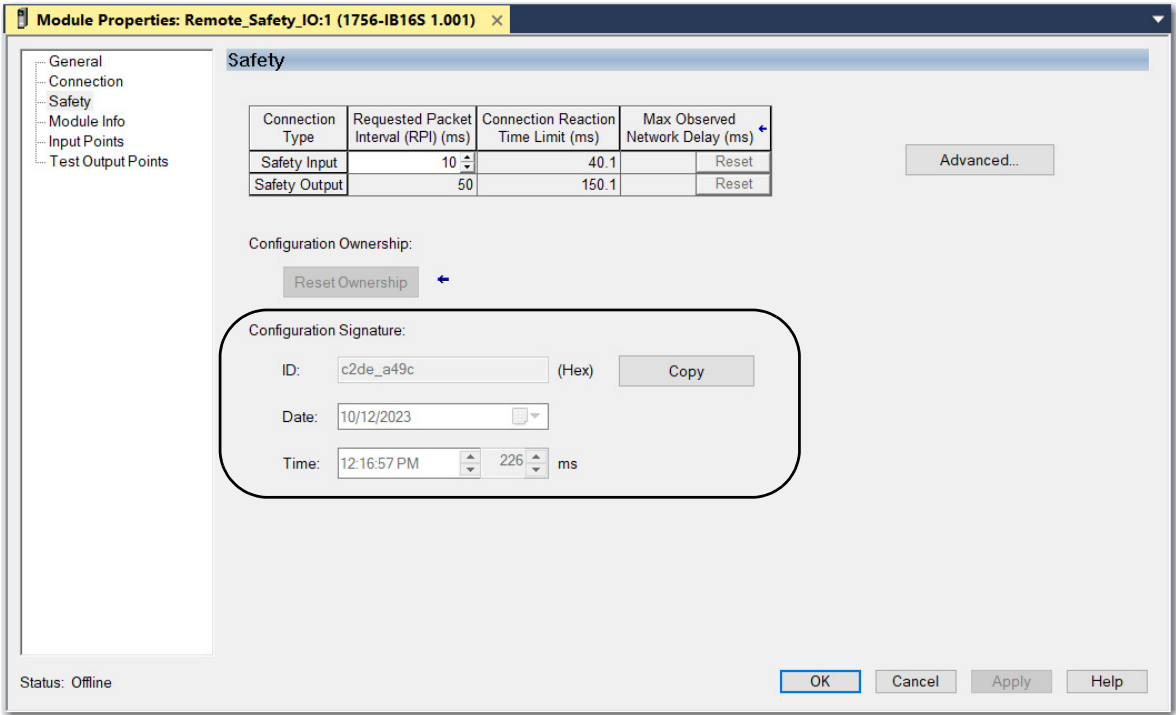
Safety I/O Device Signature

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.

Configuration via the Logix Designer Application

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 26 - View and Copy the Configuration Signature



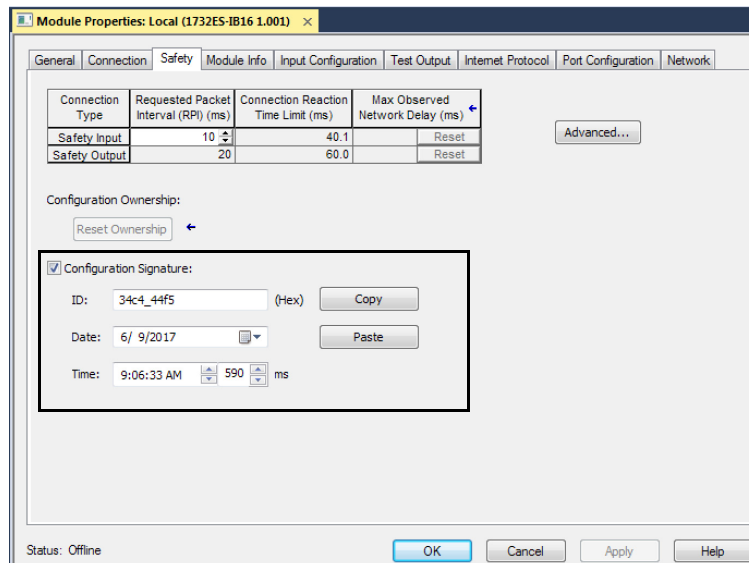
Different Configuration Owner (Data-only Connection)

When the I/O device configuration is owned by another controller, you need to 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 27 - View and Copy the Configuration Signature from Different Owner



Reset Safety I/O Device to 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.

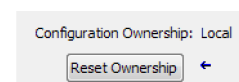
When the controller project is online, the Safety tab of the device properties displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the SNN and node address or slot number of the configuration owner. Communication error is displayed 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 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 24 - 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
Member	Specific data from the I/O device	
	Input-only device	devicename:I.RunMode ⁽¹⁾ devicename:I.ConnectionFaulted ⁽¹⁾ devicename:I.Input Members
	Output-only device	devicename:I.RunMode ⁽¹⁾ devicename:I.ConnectionFaulted ⁽¹⁾ devicename:O.Output Members
	Combination I/O	devicename:I.RunMode ⁽¹⁾ devicename:I.ConnectionFaulted ⁽¹⁾ devicename:I.Input Members devicename:O.Output Members

(1) This member is required.

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

Monitor Safety I/O Device Status

You can monitor safety I/O device status via Explicit Messaging or via the status indicators on the device. For more information, see the product documentation for the device.

Replace a Safety I/O Device

You can replace safety I/O devices while they are connected to GuardLogix® controllers.

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.

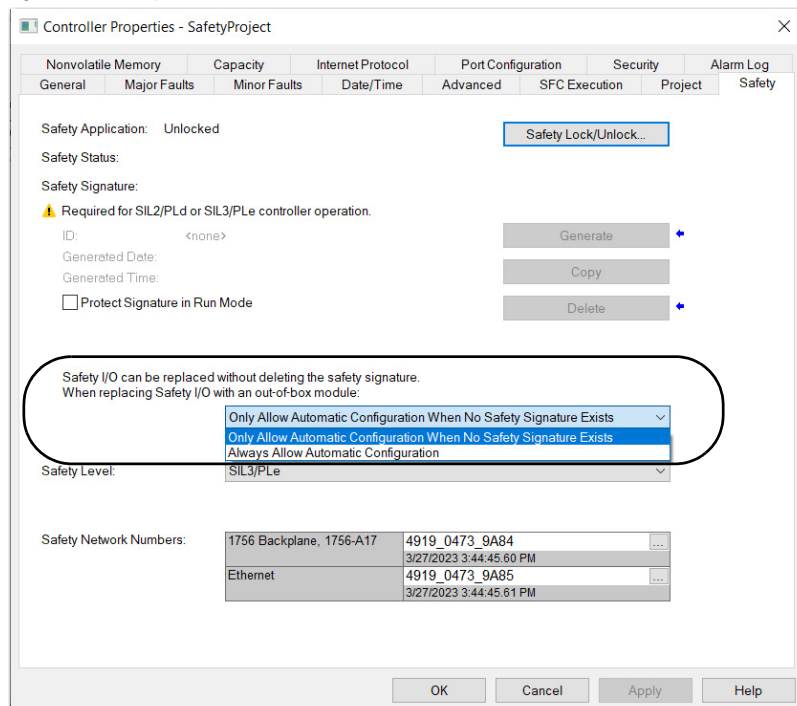
1. Right-click the device and choose Properties.
2. Click the Connection tab.
3. Check Inhibit Connection.
4. Click Apply and then OK.

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.
See [Only Allow Automatic Configuration When No Safety Signature Exists on page 123](#).
- 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.
See [Always Allow Automatic Configuration on page 127](#)

Figure 19 - 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.

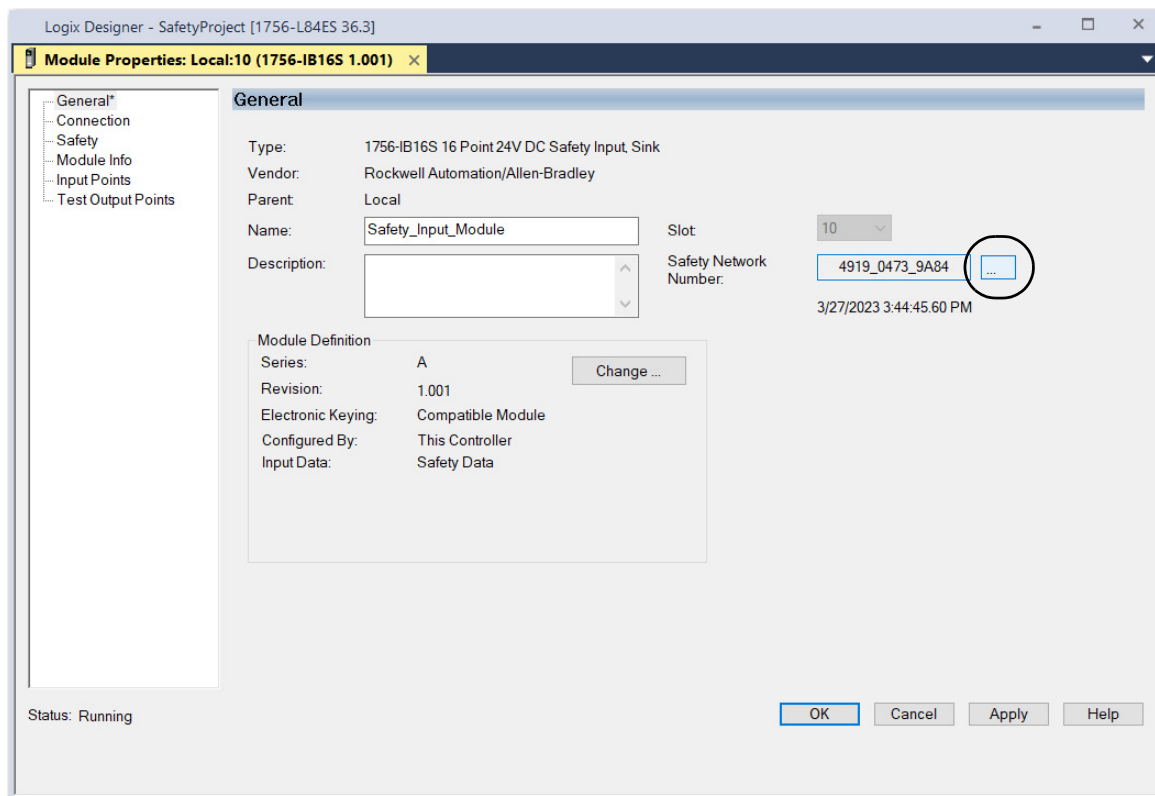
If you select the Only Allow Automatic Configuration When No Safety Signature Exists option, follow the guidance in [Table 25](#) to replace a safety I/O device based on your scenario. After you complete the steps, the DeviceID matches the original and enables the safety controller to download the proper device configuration and re-establish the safety connection.

Table 25 - Replace a Device

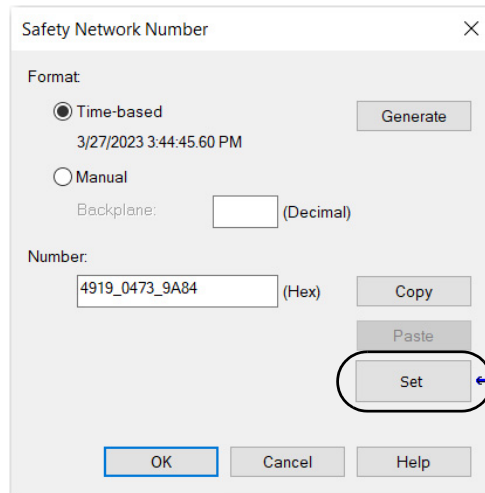
Safety Signature Exists	Replacement Device Condition	Action Required
No	No SNN (out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (out-of-box)	See Scenario 1 - Replacement Device is Out-of-box and Safety Signature Exists on page 124.
Yes	Different SNN from original safety task configuration	See Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists on page 125.
No	Different SNN from original safety task configuration	See Scenario 3 - Replacement Device SNN is Different from Original and No Safety Signature Exists on page 127.

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  to the right of the safety network number to open the Safety Network Number dialog box.



4. Click Set.

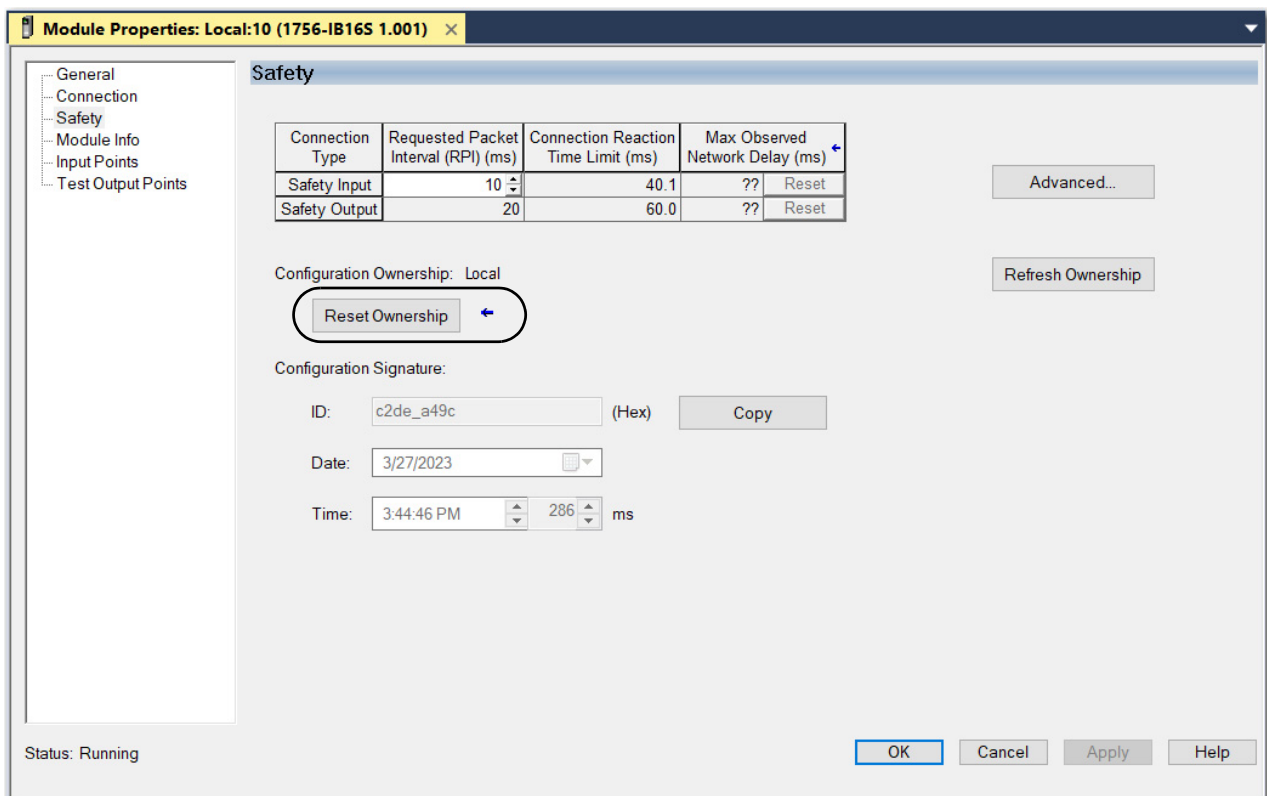


The dialog box is titled "Safety Network Number". It has a "Format" section with two radio buttons: "Time-based" (selected) and "Manual". Below "Time-based" is a timestamp "3/27/2023 3:44:45.60 PM" and a "Generate" button. Below "Manual" is a "Backplane:" label followed by an empty text box and the label "(Decimal)". Below this is a "Number:" label followed by a text box containing "4919_0473_9A84" and the label "(Hex)". To the right of the "Number:" text box are "Copy" and "Paste" buttons. Below these is a "Set" button, which is circled with a blue arrow pointing to it. At the bottom are "OK", "Cancel", and "Help" buttons.

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.



The screenshot shows the "Module Properties" window for "Local:10 (1756-IB16S 1.001)". The "Safety" tab is selected in the left navigation pane. The main area displays a table of connection parameters, configuration ownership, and configuration signature.

Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)
Safety Input	10	40.1	?? Reset
Safety Output	20	60.0	?? Reset


Below the table, the "Configuration Ownership" is set to "Local". A "Reset Ownership" button is circled with a blue arrow pointing to it. To the right of the table are "Advanced..." and "Refresh Ownership" buttons.

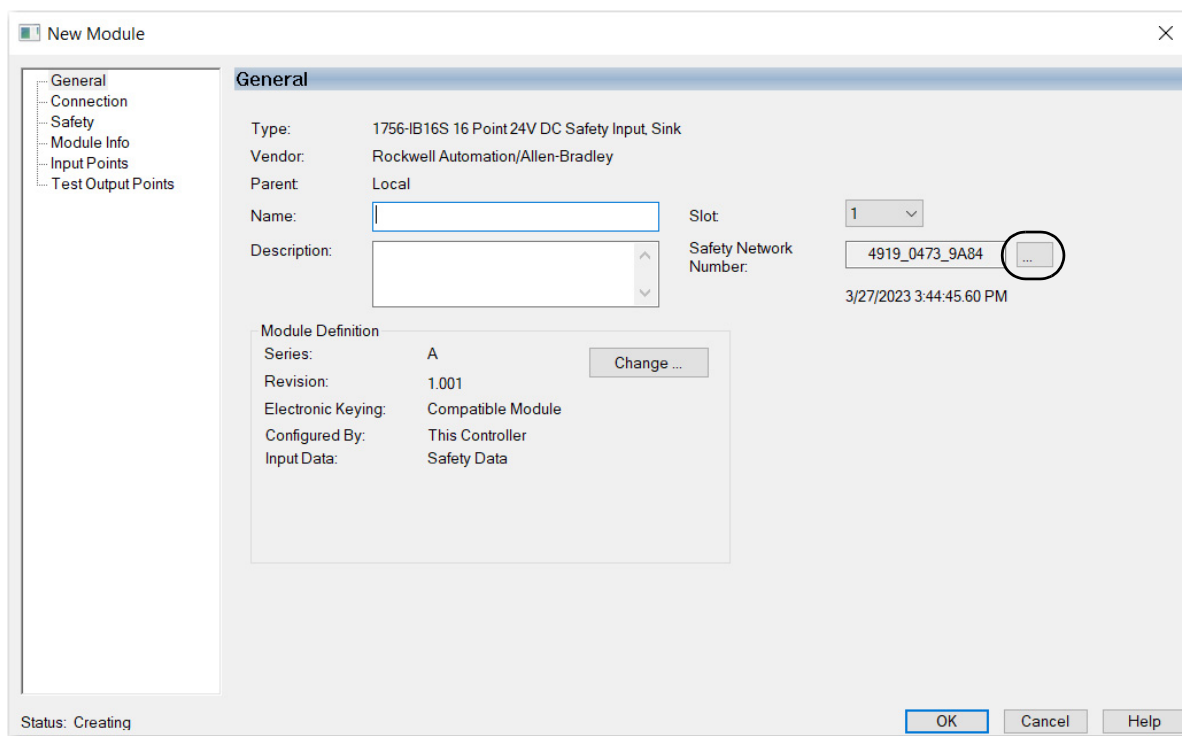
The "Configuration Signature" section includes:

- ID: c2de_a49c (Hex) with a "Copy" button.
- Date: 3/27/2023
- Time: 3:44:46 PM, 286 ms

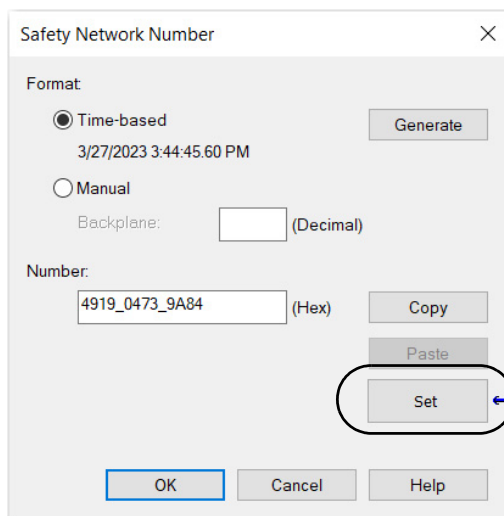
At the bottom left, the status is "Running". At the bottom right are "OK", "Cancel", "Apply", and "Help" buttons.

5. Click OK.
6. Right-click the device and select Properties.

7. Click  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, select Safety.
4. Click Reset Ownership.

Module Properties: Local:10 (1756-IB16S 1.001)

Safety

Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)
Safety Input	10	40.1	?? Reset
Safety Output	20	60.0	?? Reset

Configuration Ownership: Local

Reset Ownership (circled in red)

Configuration Signature:

ID: c2de_a49c (Hex) **Copy**

Date: 3/27/2023

Time: 3:44:46 PM 286 ms

Status: Running

OK **Cancel** **Apply** **Help**

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



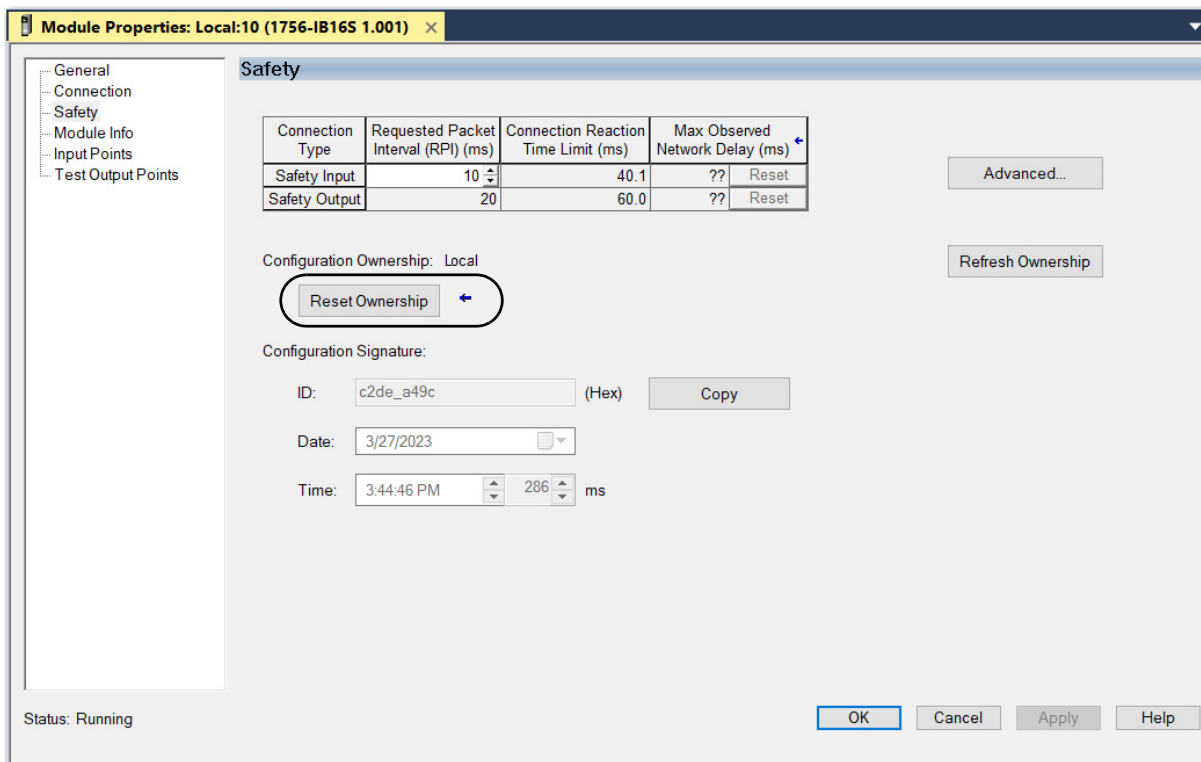
ATTENTION: Select the Always Allow Automatic Configuration option only if the entire CIP Safety Control System is not being relied on to maintain SIL 2 or SIL 3 behavior during the replacement and functional testing of a device. Do not place devices that are in the out-of-box condition on a CIP Safety 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 of 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 step 5.
 - 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 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

Elements of a Control Application

Applies to these controllers:

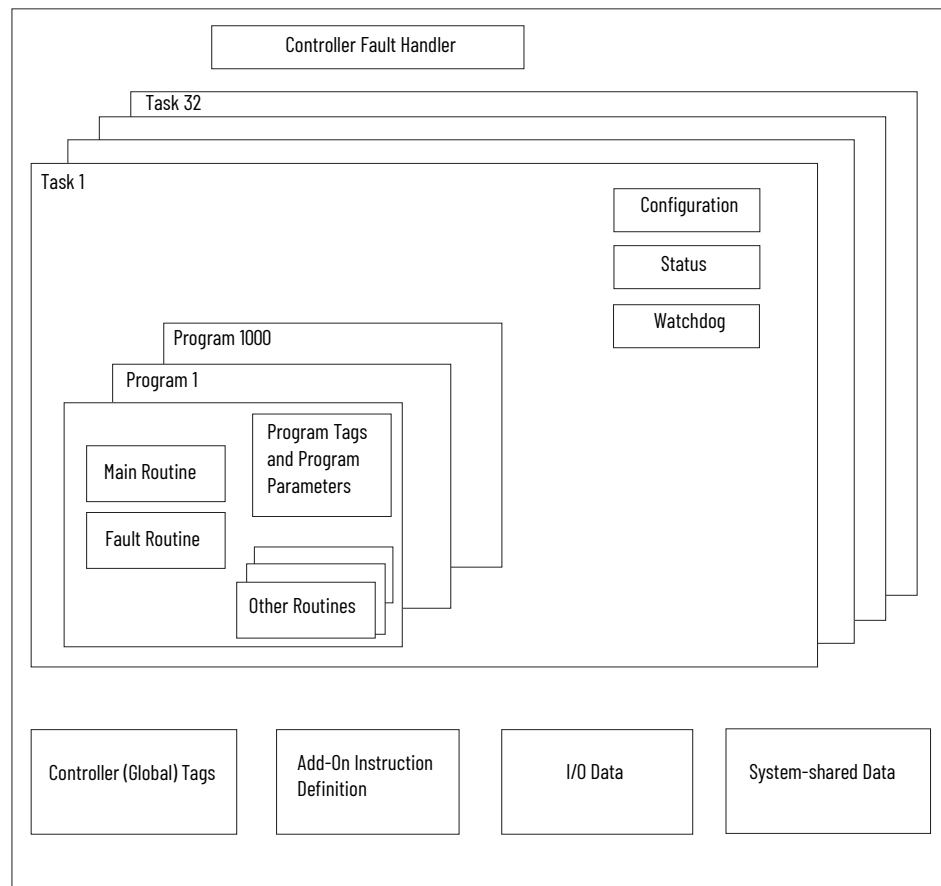
ControlLogix 5580

GuardLogix 5580

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 28 - 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 29 - Task Within a Control Application

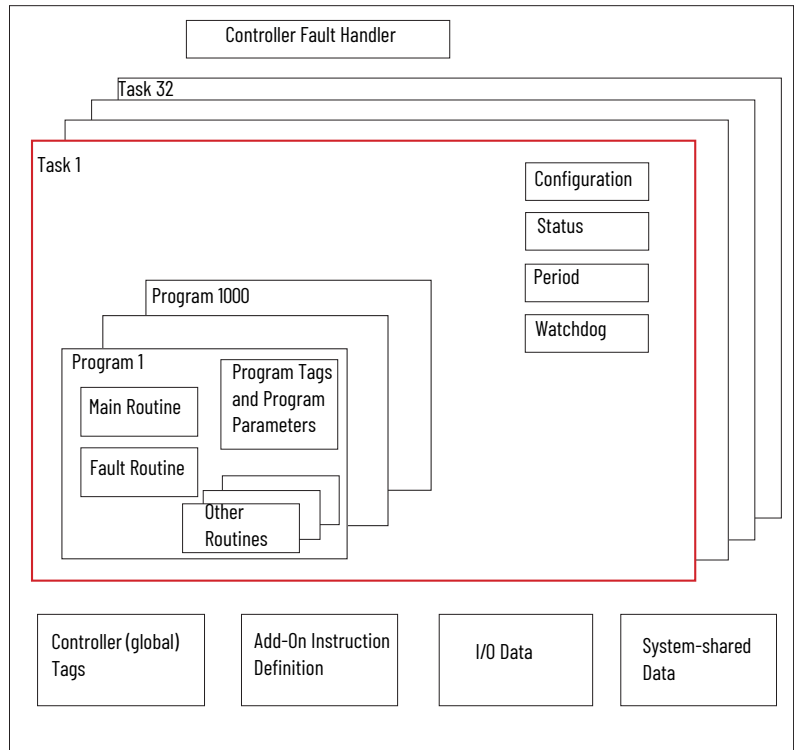
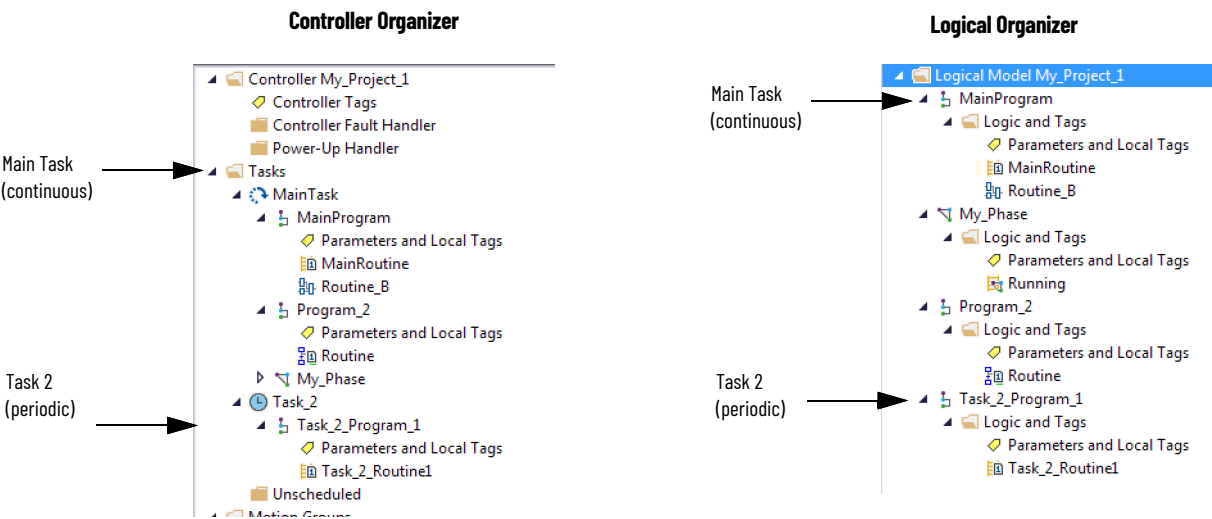
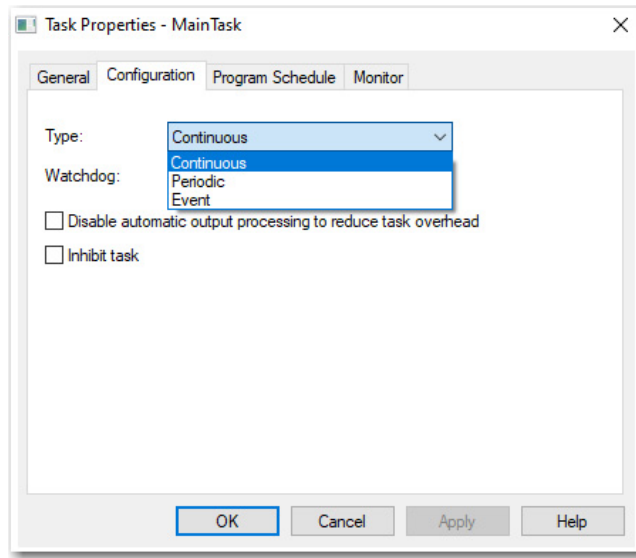


Figure 30 - Tasks



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 31 - Configure the Task Type



[Table 26](#) explains the types of tasks you can configure.

Table 26 - Task Types and Execution Frequency

Task Type	Task Execution	Description
Continuous	Constant	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>A periodic task performs a function at an interval.</p> <ul style="list-style-type: none"> • 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	<p>An event task performs a function when an event (trigger) occurs. The trigger for the event task can be the following:</p> <ul style="list-style-type: none"> • Module input data change of state • A consumed tag trigger • An EVENT instruction • An axis trigger • A motion event trigger <p>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 Execute Task If No Event Occurs Within <timeout period> check box for task.</p>

The ControlLogix™ 5580 and GuardLogix® 5580 controllers support up to 32 tasks. Only one of the tasks can be continuous.

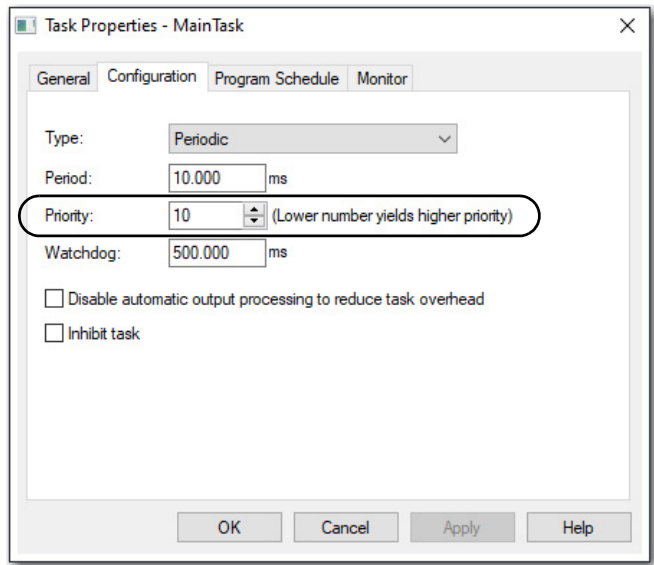
A task can have up to 1000 programs, each with its own executable routines and program-scoped tags. Once a task is triggered (activated), the programs that are assigned to the task execute in the order in which they are grouped. Programs can appear only once in the Controller Organizer and multiple tasks 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 32 - Configure the Task Priority



Programs

The controller operating system is a pre-emptive 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 33 - Program Within a Control Application

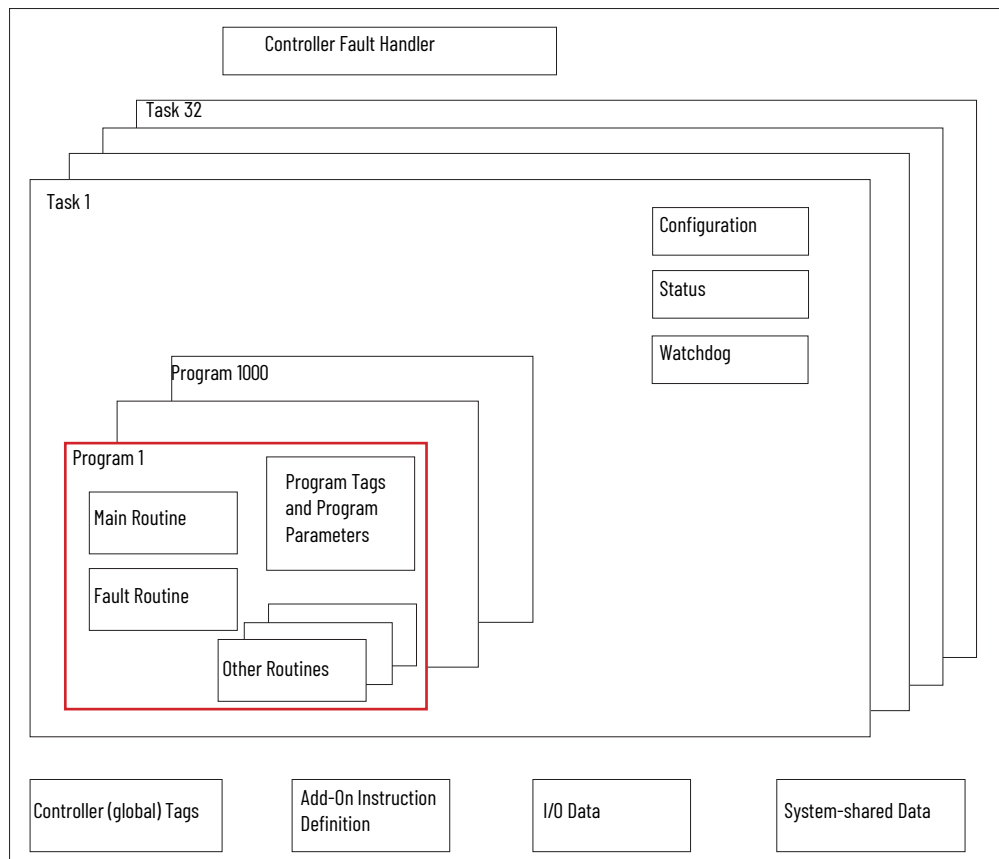
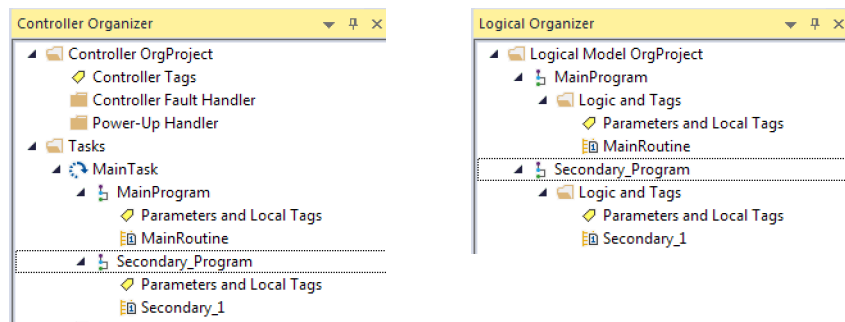


Figure 34 - Programs



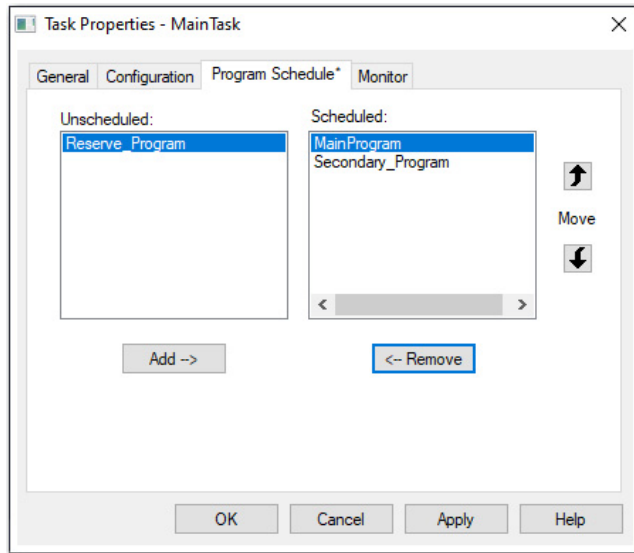
Scheduled and Unscheduled Programs

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 35 - Scheduling 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 36 - Routines in a Control Application

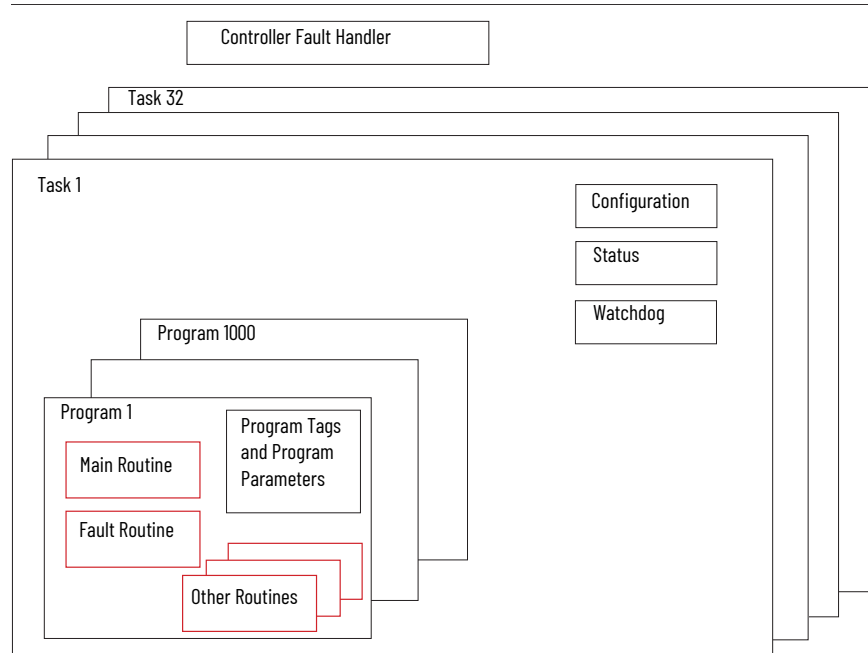
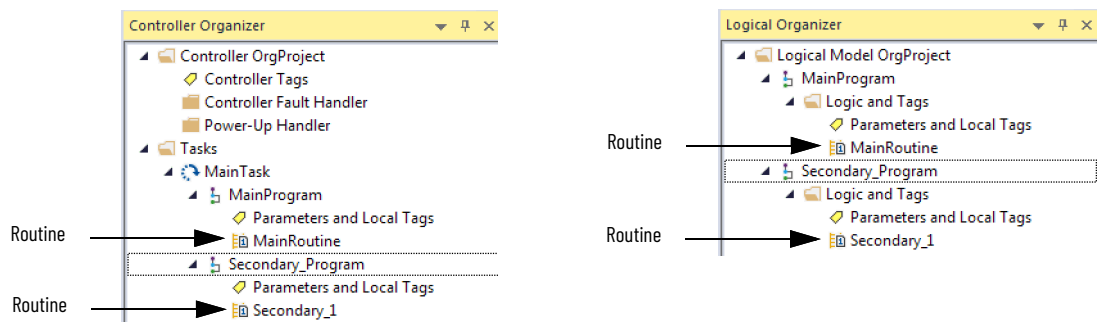


Figure 37 - Routines



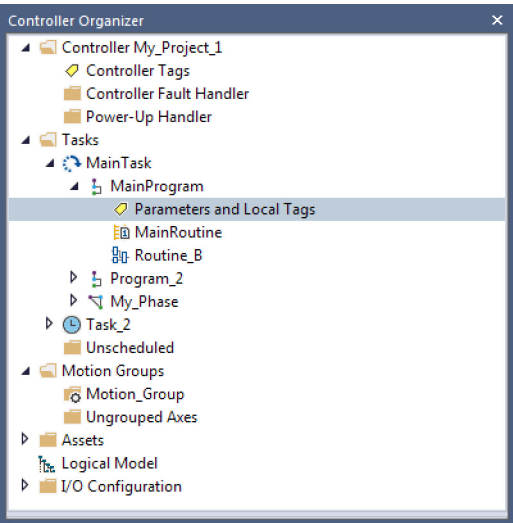
Parameters and Local Tags

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:

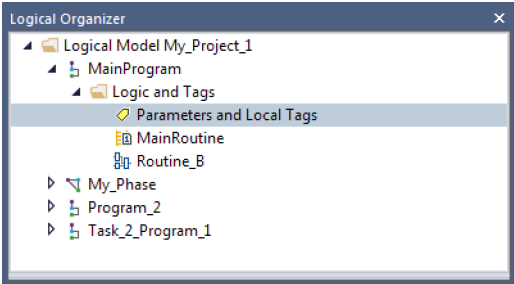
- Organize your data to mirror your machinery.
- Document your application as you develop it.

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

Controller Organizer —Main Program Parameters and Local Tags



Logical Organizer —Main Program Parameters and Local Tags



Program Parameters and Local Tags Window

Program Parameters and Local Tags - MainProgram								
Scope: [MainProgram]		Show: All Tags		Enter Name Filter...				
Name	Usage	Value	Style	Data Type	Description	Constant	Alias For	
ADD_01	Local	{...}		FBD_MATH		<input type="checkbox"/>		
ADD_02	Local	{...}		FBD_MATH		<input type="checkbox"/>		
Disabled	Local	0	Decimal	BOOL		<input type="checkbox"/>		
Motor_Starter_01	Local	{...}		Motor_Starter	Starts the motor.	<input type="checkbox"/>		

There are several guidelines for how to create and configure parameters and local tags for optimal task and program execution. For more information, see the Logix 5000 Controllers and I/O Tag Data Programming Manual, publication [1756-PM004](#).

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 individual basis for each parameter.

There are several guidelines for creating and configuring 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.

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
	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.
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 the Logix Designer application, 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. [Table 27](#) explains some of the capabilities and advantages of use Add-On Instructions.

Table 27 - Add-On Instruction Capabilities

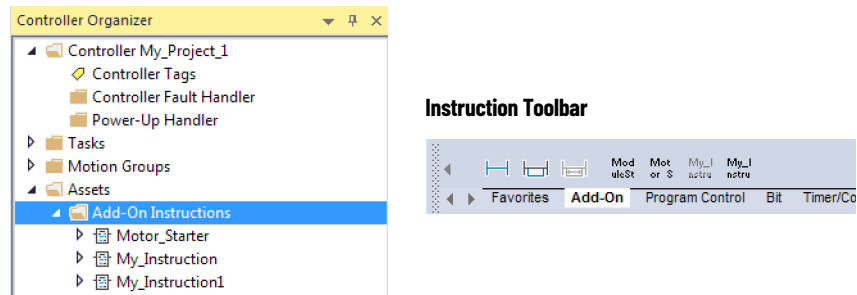
Capability	Description
Save Time	With Add-On Instructions, you can combine your most commonly used logic into sets of reusable instructions. You save time when you create instructions for your projects and share them with others. Add-On Instructions increase project consistency because commonly used 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: <ul style="list-style-type: none"> • 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.

Table 27 - Add-On Instruction Capabilities

Capability	Description
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 AOI, and include the AOI 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 AOI for better Intellectual property protection. Using this feature has less of a performance impact than the Logix-designer 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 tool bar for easy access along with internal instructions.

Figure 38 - Add-On Instructions (Studio 5000 Logix Designer Application Version 31 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.

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:

- 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.

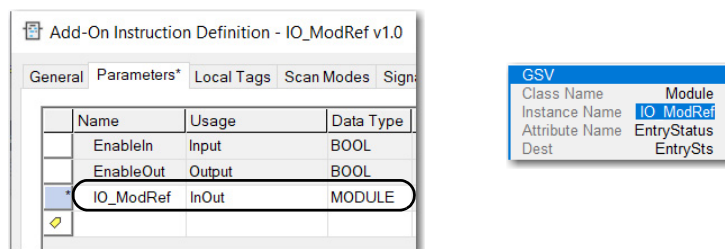
For more information on Extended Properties, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication [1756-PM004](#).

Access the Module Object from an Add-On Instruction

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.



For more information on the Module Reference parameter, see the 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:

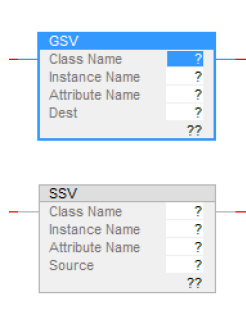
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Monitor Controller Status

The ControlLogix 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 39 - 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 online help for the GSV and SSV instructions.


Monitor 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.

For more information on how to determine the time for your application, see Knowledgebase Technote [EtherNet/IP Reduced Heartbeats as of RSLogix5000 version 16](#).

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.
- A  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

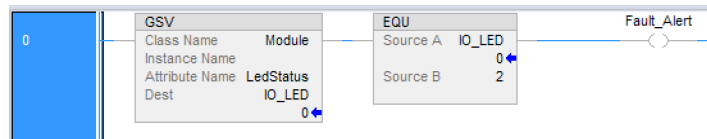
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#).

Determine If I/O Communication Has Timed Out

This example can be used with the ControlLogix 5580 or GuardLogix 5580 controllers, and 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 40 - 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.

Determine if I/O Communication to a Specific I/O Module has Timed 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.

For more information about monitoring safety I/O faults, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

Automatic Handling of I/O Module Connection Faults

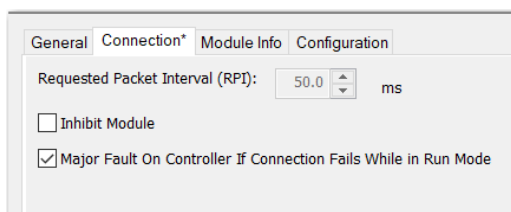
Depending on your application, you may want an I/O connection error to cause the Controller Fault Handler to execute. To do so, set the module property that causes a major fault to result from an I/O connection error. The major fault causes the execution of the Controller Fault Handler.



ATTENTION: You cannot program Safety I/O module connections or safety produce/consume connections to automatically cause a major fault on the controller. See [Develop Safety Applications on page 143](#).

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 41 - 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 141 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.



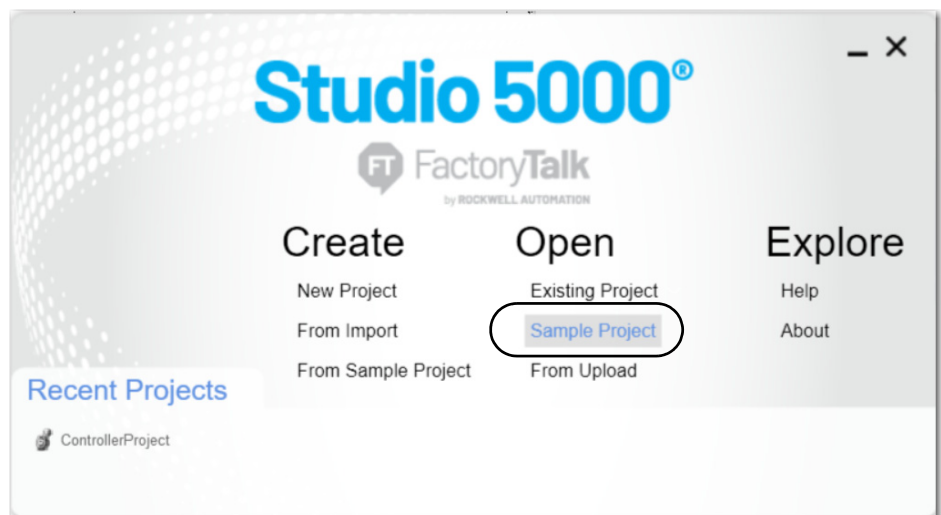
It takes at least 100 milliseconds to detect an I/O connection loss, even if the Controller Fault Handler is used.

For more information about programming the Controller Fault Handler, see the Logix 5000 Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#).

Sample Controller Projects

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

Figure 42 - Opening Sample Projects



Develop Safety Applications

You can use both standard (non-safety-related) and safety-related components in the GuardLogix® control system. Within a GuardLogix project, you can perform standard automation control from standard tasks. GuardLogix 5580 controllers and Compact GuardLogix 5380 controllers provide the same functionality as other controllers. What differentiates the controllers from standard controllers is that the controllers also provide a SIL 2 or SIL 3 capable safety task.

However, 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.

Safety Overview

Applies to these controllers:

GuardLogix 5580

This chapter explains the components that make up a safety project and the features that help protect safety application integrity, such as the safety signature and safety-locking.

The GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#) addresses the following topics:

- Guidelines and requirements for developing and commissioning SIL 2/PLD and SIL 3/PLE safety applications, including Add-on Profiles
- Creating a detailed project specification
- Writing, documenting, and testing the application
- Generating the safety signature to identify and protect the project
- Confirming the project by printing or displaying the uploaded project and manually comparing the configurations, safety data, and safety program logic
- Verifying the project through test cases, simulations, functional verification tests, and an independent safety review, if required
- Locking the safety application
- Calculating system reaction time

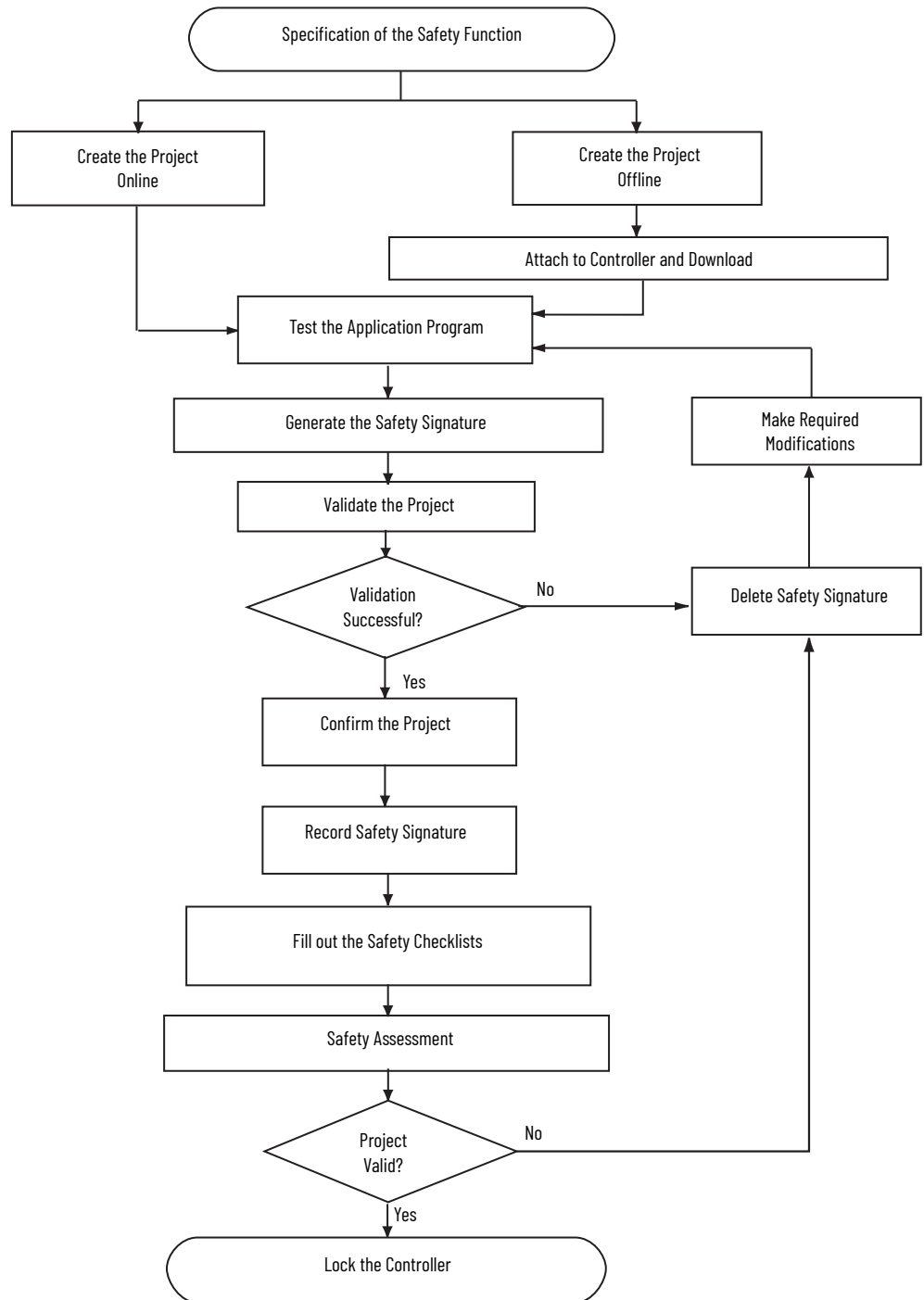


ATTENTION: Performing an on-line modification (to logic, data, or configuration) can affect the Safety Functions of the system if the modification is performed while the application is running. A modification should only be attempted if absolutely necessary. Also, if the modification is not performed correctly, it can stop the application. Therefore, when the safety signature is deleted to make an online edit to the safety task, before performing an online modification alternative safety measures must be implemented and be present for the duration of the update.

Program Safety Applications

Figure 43 shows the steps that are required for commissioning a GuardLogix system. For an explanation of those steps, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

Figure 43 – Commission the System



Develop Secure Applications

Applies to these controllers:

ControlLogix 5580

These ControlLogix® 5580 controllers support IEC-62443-4-2 SL 1 security requirements:

- ControlLogix 5580 standard controllers, firmware revision 32 or later
- ControlLogix 5580 NSE, XT, K, and Process controllers, firmware revision 33 or later

These controllers **do not** support IEC-62443-4-2 SL 1 security requirements:

- ControlLogix 5580 redundancy-enabled controllers
- GuardLogix® 5580® safety controllers

To help meet these requirements, you must use this publication and the Security Configuration User Manual, publication [SECURE-UM001](#). The Security Configuration User Manual describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.

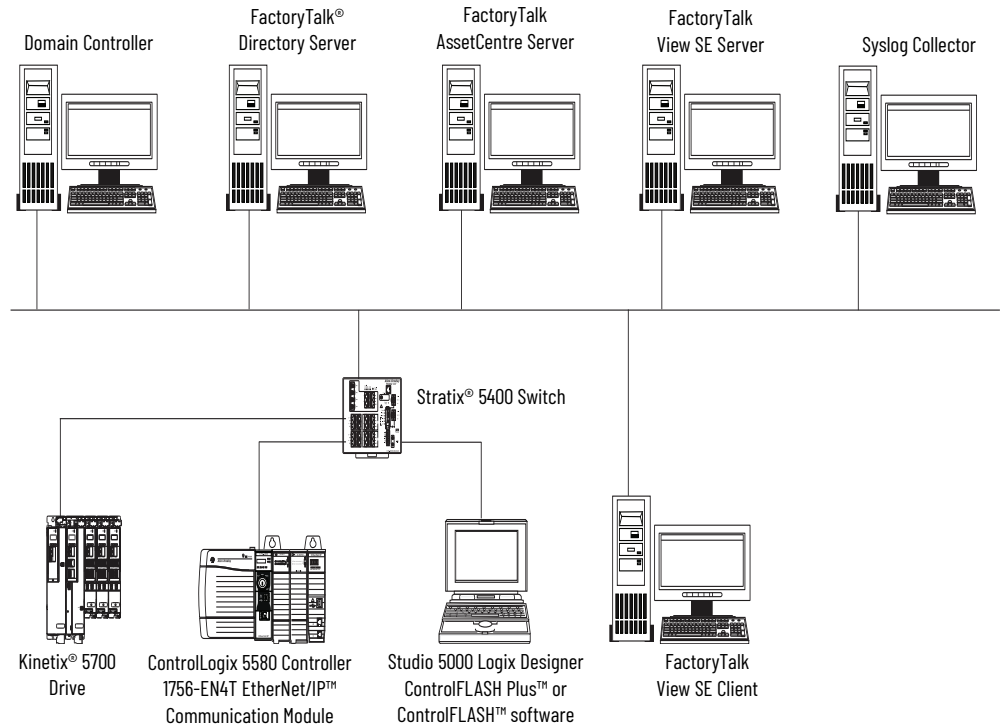
The controller accepts all values appropriate for a tag data type, and it is the responsibility of the user program to specify valid ranges and perform validity to check for those ranges. The controller verifies incoming messages for syntax, length, and format.

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

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

Controller Security Features

For the ControlLogix controller to comply with the certification requirements, implement the control system with these other security-focused products.



Security Checklists

Follow the security checklists in this chapter 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.

Table 28 - Requirements for Identification and Authorization

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk® Security software Studio 5000 Logix Designer application	Yes	<p>Configure FactoryTalk Security to define policies, user groups, and other permission sets.</p> <ul style="list-style-type: none"> 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. <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>

Table 29 - Requirements for Use Control

✓	Product	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.	<p>Configure the controller project in the Logix Designer application to use these user access methods:</p> <ul style="list-style-type: none"> 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. <p>For more information, see Logix 5000 Controllers Security Programming Manual, 1756-PM016.</p>
	FactoryTalk Security software Studio 5000 Logix Designer application	Yes	<p>Configure FactoryTalk Security to define policies, user groups, and other permission sets.</p> <ul style="list-style-type: none"> 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™ 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. 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. <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>
	Controller keyswitch position	May be required based on system design, threat model, and risk assessment.	<p>Place the keyswitch in RUN position to help prevent unauthorized remote configuration changes to the controller, and restrict some communication services.</p> <p>Remove the keyswitch from a running controller to help prevent modifications to the configuration or program.</p> <p>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.</p>
	Disable the controller Ethernet port	May be required based on system design, threat model, and risk assessment.	<p>The Ethernet port is enabled by default. Disable the Ethernet port if required by the system design, threat model, or risk assessment.</p> <p>For more information, see page 159.</p>
	Disable Simple Network Management Protocol (SNMP) on the controller	May be required based on system design, threat model, and risk assessment.	<p>SNMP is disabled by default. If SNMP has been enabled, disable SNMP if required by the system design, threat model, or risk assessment.</p> <p>For more information, see page 91.</p>

Table 29 - Requirements for Use Control (Continued)

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	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 ports if required by the system design, threat model, or risk assessment. For more information, see page 162 .
	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 page 165 .
	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 page 166 .
	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 page 172 .

Table 30 - Requirements for System Integrity

✓	Product	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. Configure the Device Monitor - Change Detect operation for the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
	FactoryTalk Security software		
	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 download 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: <ul style="list-style-type: none"> 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 page 30 .
	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 page 151 .
	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 page 159 .

Table 31 - Requirements for Data Confidentiality

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk Security software	Yes	<p>Configure FactoryTalk Security to define policies, user groups, and other permission sets.</p> <ul style="list-style-type: none"> 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. <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>
	FactoryTalk Policy Manager software	Yes	<p>Use the FactoryTalk Policy Manager software to define a secure data transport over an EtherNet/IP™ network to the controller.</p> <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>
	SD card encryption	May be required based on system design, threat model, and risk assessment.	<p>If your system allows SD card use, the load process to the SD card encrypts and digitally signs the project by using the controller key. The SD card itself is not encrypted.</p> <p>When you save (load) firmware to the SD card, the process stores encrypted firmware and certificates on the SD card.</p> <p>Do not use a Message to Self (MSG with a Path of THIS) to auto-write controller logs or manually force a write of controller logs to the SD card. This can help prevent against potential loss of controller logs before FactoryTalk AssetCentre can read them.</p> <p>For more information, see page 77.</p>
	License-based source and execution protection	May be required based on system design, threat model, and risk assessment.	<p>Configure licenses to manage access to controller source logic and execution of that logic. These licenses are not enabled by default.</p> <ul style="list-style-type: none"> 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. <p>For more information, see page 153.</p>

Table 32 - Requirements for Restricted Data Flow

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	CIP Security	Yes	<p>Use FactoryTalk Policy Manager software to define conduits.</p> <p>For more information, see CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001.</p>

Table 33 - Requirements for Timely Response to Events

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	Configure and use the following: <ul style="list-style-type: none"> • Audit log accessibility • Continuous monitoring For more information, see the following: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • RFC-5424 syslog protocol • Ability to receive messages from the controller IMPORTANT: The controller sends events to a syslog collector through its 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 page 156 .
	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 page 158 .
	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: <ul style="list-style-type: none"> • 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 page 158 .

Table 34 - Requirements for Resource Availability

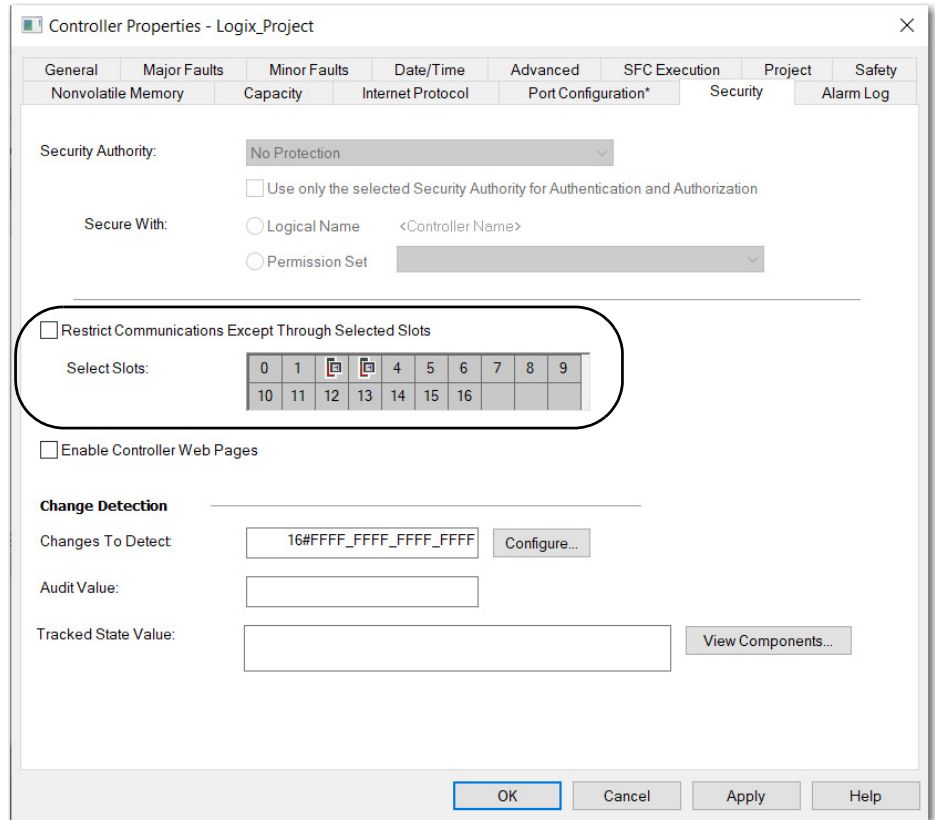
✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	Configure and use the following: <ul style="list-style-type: none"> • Asset inventory • Control system backup • Disaster recovery For more information, see Configure System Security Features User Manual, SECURE-UM001 .
	UPS	Yes	Provide your own UPS with separate battery unit and redundant power supplies. Size the UPS so that it correctly supports the system and provides enough power to properly shut down servers and workstations.

Configure Trusted Slots on the Controller

To maintain network segmentation, configure Trusted slots on the controller. On the Security tab of the Controller Properties dialog box, configure Trusted slots to restrict the communication paths through which certain operations are performed on Logix controllers.

IMPORTANT

- 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 97](#).
- 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.



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 USB or serial ports and firmware updates are restricted to Trusted slots when using AutoFlash, or ControlFLASH Plus and ControlFLASH™ 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 are displayed in the dialog box. Otherwise, 17 slots (0...16) are displayed in the dialog box.

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 the 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.

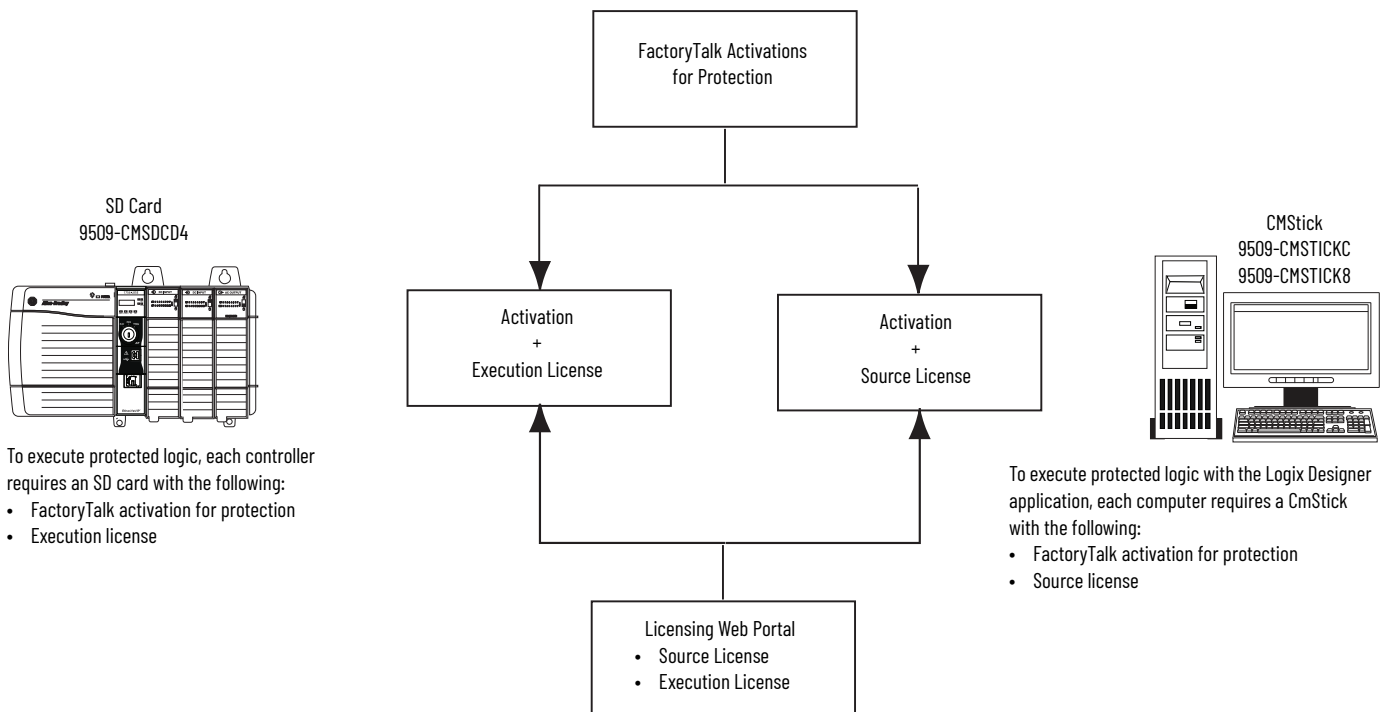


License-based Source and Execution Protection

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.

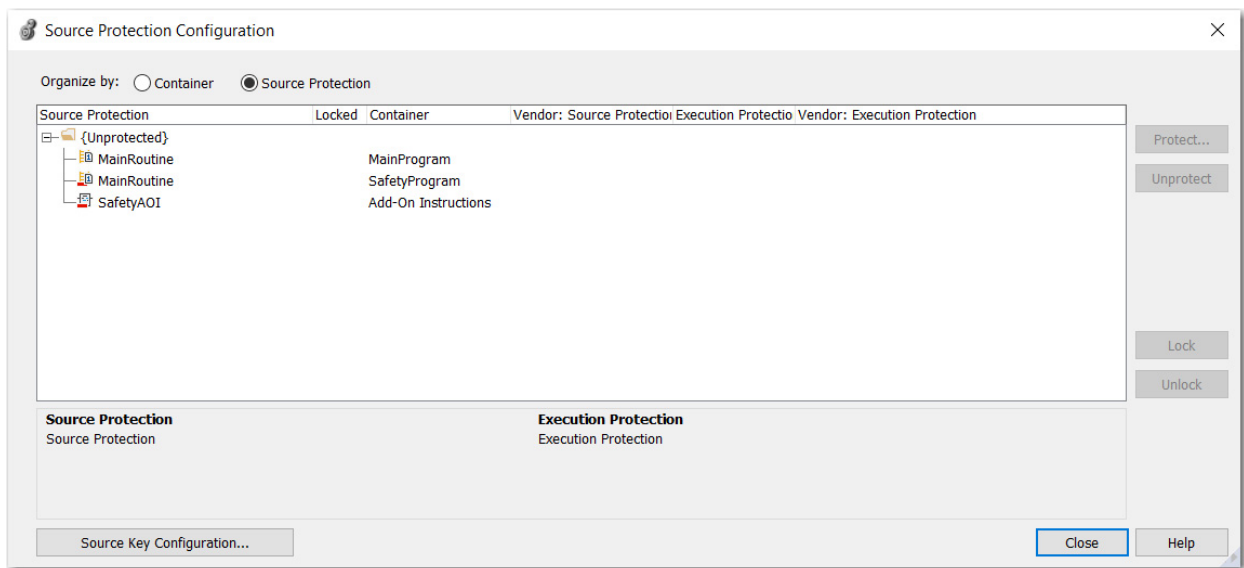


To apply license-based protection, you need the following:

- 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.

Enable License-based Protection

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.

Protect

Protection Type: License

Apply Source Protection:

Name	Vendor
Content Protector A (Protect License)	OEM A
Content Protector B (Protect License)	OEM B
Content Protector C (Protect License)	OEM C

Select Execution Protection:

☒ Protect with controller key only

☐ Protect with controller key and specific license

Name	Vendor
Execution Protector A1	OEM A
Execution Protector A2	OEM A
Execution Protector A5	OEM A
Execution Protector A6	OEM A
Execution Protector A7	OEM A
Execution Protector A8	OEM A
Execution Protector A9	OEM A
Execution Protector A10	OEM A

OK Cancel Help

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.

Configure 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](#).

Controller Properties - Logix_Project

General Major Faults Minor Faults Date/Time Advanced SFC Execution Project Safety
Nonvolatile Memory Capacity Internet Protocol Port Configuration* **Security** Alarm Log

Security Authority: No Protection
☐ Use only the selected Security Authority for Authentication and Authorization

Secure With:
☐ Logical Name <Controller Name>
☐ Permission Set

☐ Restrict Communications Except Through Selected Slots

Select Slots:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16			

☐ Enable Controller Web Pages

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF Configure...

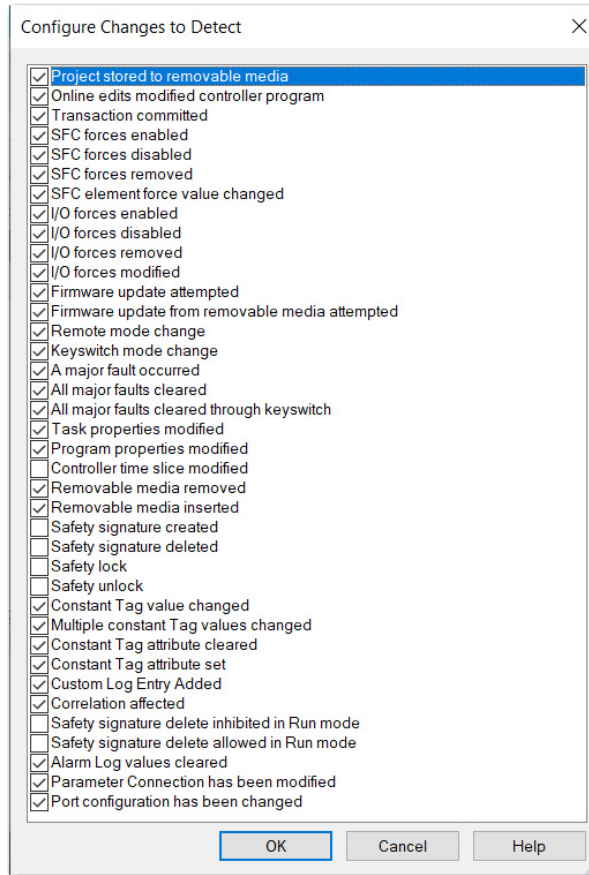
Audit Value:

Tracked State Value: View Components...

OK Cancel Apply Help

Changes to Detect

Click Configure to open the Configure Changes to Detect dialog box. We recommend tracking the changes that are shown in the following image for a standard ControlLogix 5580 controller. 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.

Configure 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 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](#).

Controller Properties - Logix_Project

General Major Faults Minor Faults Date/Time Advanced SFC Execution Project Safety
Nonvolatile Memory Capacity Internet Protocol Port Configuration* Security Alarm Log

Security Authority: No Protection
☐ Use only the selected Security Authority for Authentication and Authorization

Secure With:
☐ Logical Name <Controller Name>
☐ Permission Set

☐ Restrict Communications Except Through Selected Slots

Select Slots:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16			

☐ Enable Controller Web Pages

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF [Configure...](#)

Audit Value:

Tracked State Value: [View Components...](#)

OK Cancel Apply Help

Configure Controller Logging

The controller log stores various security-related events that can be written to an SD card or accessed via FactoryTalk Asset Center 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.

Disable the Controller Ethernet Port

You can disable the controller Ethernet port with the Studio 5000 Logix Designer application, version 28 or later.

IMPORTANT

Remember the following:

- 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 keyswitch 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.

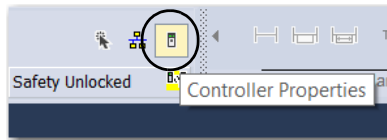
There are two ways to disable the Ethernet port:

- [Disable the Ethernet Port on the Port Configuration Tab on page 159](#)
- [Disable the Ethernet Port with an MSG Instruction on page 160](#)

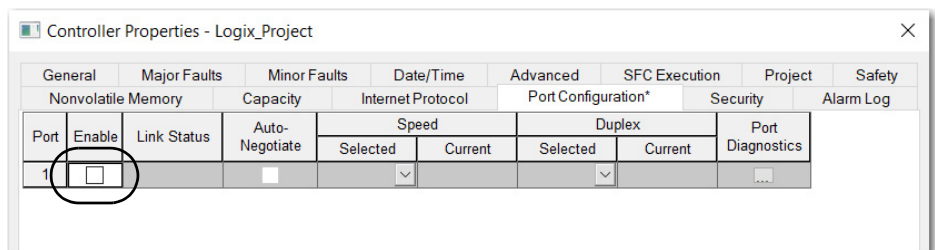
Disable the Ethernet Port on the Port Configuration Tab

You can disable the 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.

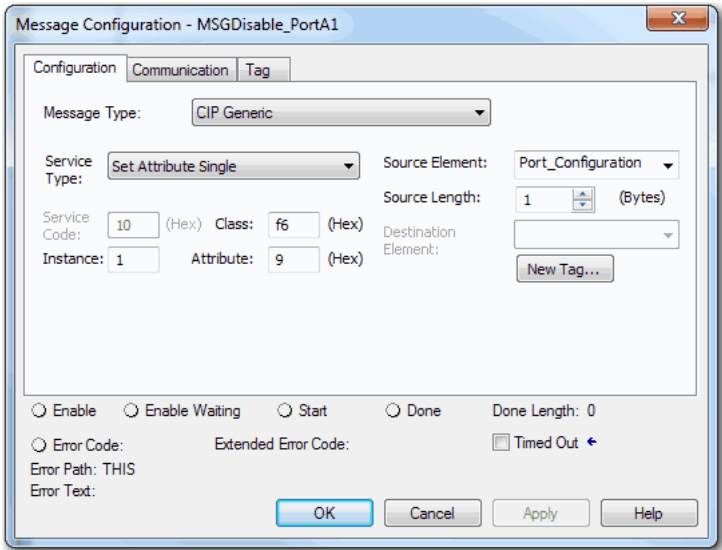
Disable the Ethernet Port with an MSG Instruction

You use a CIP™ Generic MSG with a Path of THIS to execute this option. You cannot use this MSG instruction to disable the 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 keyswitch 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 [Table 35 on page 160](#).



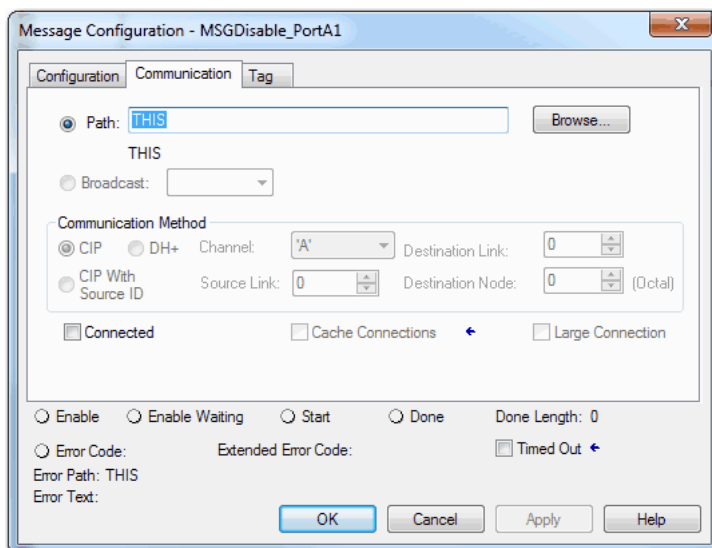
IMPORTANT These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

Table 35 - Disable the Ethernet Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	f6
Attribute	9
Source Element	Controller tag of SINT data type. In this example, the controller tag 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.



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.

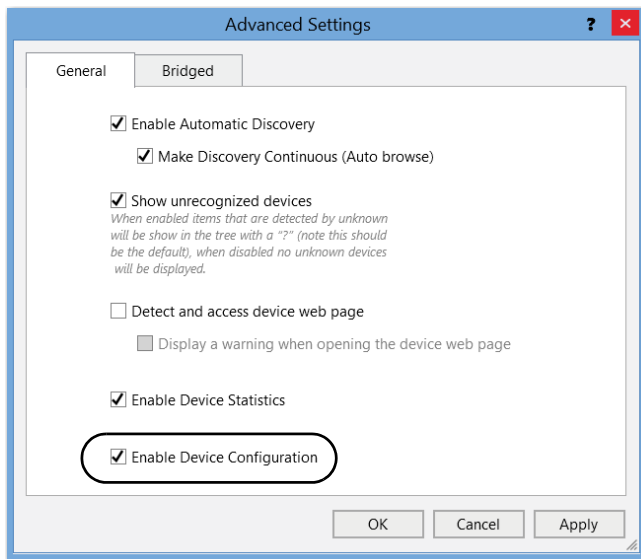
Disable the Controller CIP Security Ports

There are two ways to disable the CIP Security ports on the controller:

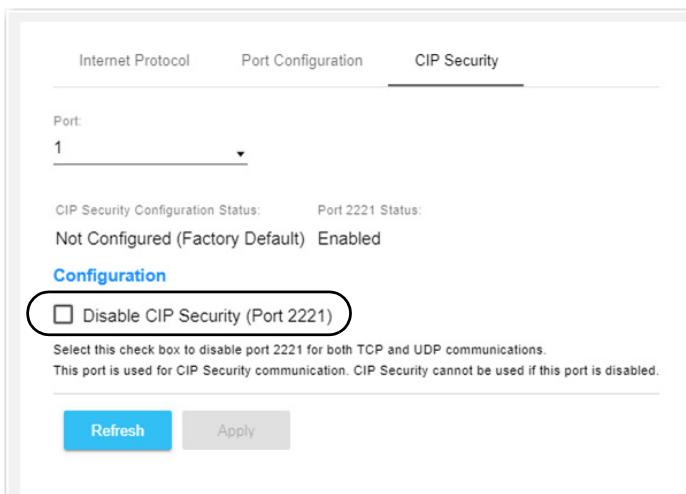
- Use the Disable CIP Security checkbox in FactoryTalk Linx software, version 6.30.00 or later
- Use a CIP Generic MSG in Studio 5000 Logix Designer application, version 32 or later

Use the Disable CIP Security Checkbox in FactoryTalk Linx

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.



Use a CIP Generic MSG Instruction in the Logix Designer Application

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.
See [Stage 2 Reset on page 76](#).

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 keyswitch 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 [Table 36 on page 164](#).

Message Configuration - MSGDisable_CIP_Security

Configuration Communication Tag

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex) Instance: 1 Attribute: 0 (Hex)

Source Element: CIPSEC_DISABLE Source Length: 9 (Bytes)

Destination Element: [Empty]

Buttons: New Tag...

Enable Enable Waiting Start **Done** Done Length: 0

Error Code: Extended Error Code: Timed Out

Error Path: THIS Error Text:

OK Cancel Apply Help

Table 36 - Disable the CIP Security Ports

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 in step 1.
Source Length	9

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

IMPORTANT Messages to THIS must be unconnected messages.

Message Configuration - MSGDisable_CIP_Security

Configuration **Communication** Tag

Path: THIS Browse...

Broadcast: [Empty]

Communication Method

CIP DH+ Channel: A Destination Link: 0

CIP With Source ID Source Link: 0 Destination Node: 0 (Octal)

Connected Cache Connections Large Connection

Enable Enable Waiting Start **Done** Done Length: 0

Error Code: Extended Error Code: Timed Out

Error Path: THIS Error Text:

OK Cancel Apply Help

5. Cycle power on the controller for the configuration to take effect.

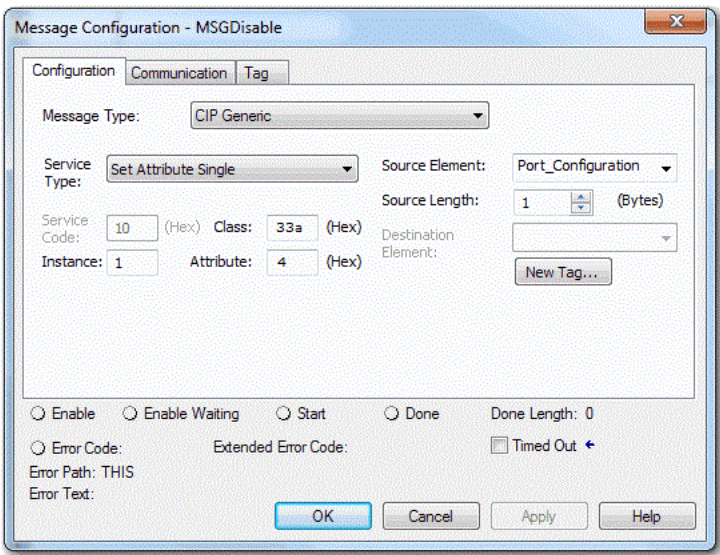
Disable the Controller USB Port

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 keyswitch 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 [Table 37](#).



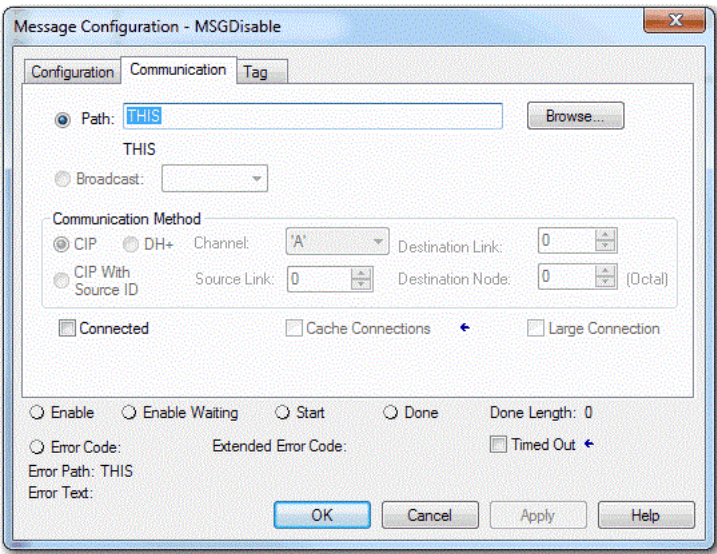
IMPORTANT These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute up each time the controller powers up.

Table 37 - 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 SD Card

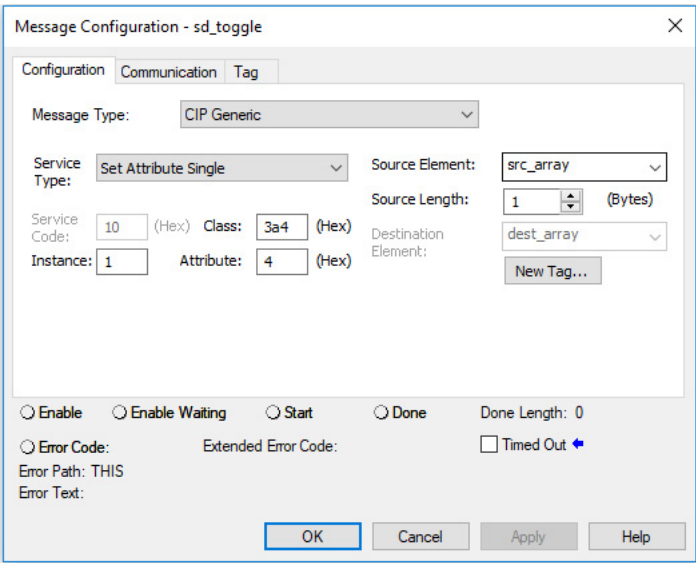
With the Studio 5000 Logix Designer application, version 32.00.00 or later, you can use a CIP Generic MSG with a Path of THIS to execute this option.

- IMPORTANT** Remember the following:
- An SD card can only be disabled with a Message to Self.
 - Once an SD slot is disabled, you lose all ability to communicate to an SD 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 keyswitch 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 [Table 38 on page 167](#).



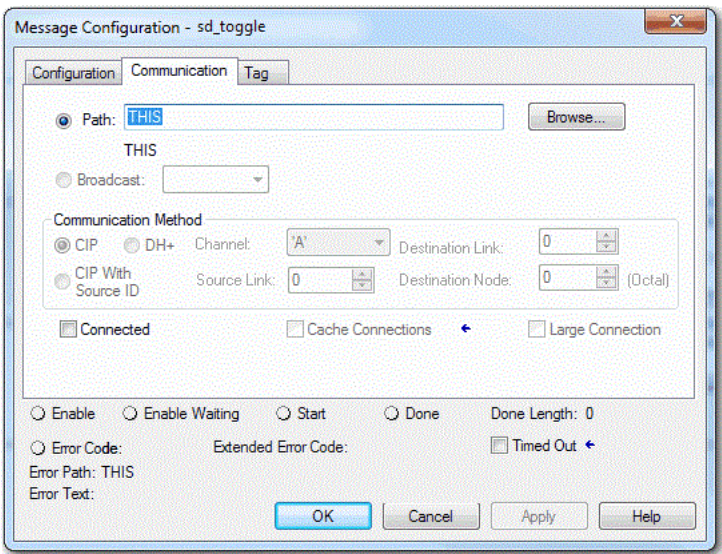
IMPORTANT These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

Table 38 - Disable the SD 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. 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 Messages to THIS must be unconnected messages.



Disable the 4-character
Status Display

With the Studio 5000 Logix Designer application, version 29 or later, you can disable certain categories of messages on the 4-character status display:

- [Disable All Categories of Messages on page 168](#)
- [Disable Individual Categories of Messages on page 170](#)

You use a CIP Generic MSG to execute each option.

IMPORTANT You cannot disable these system messages, and they will 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

When you disable all categories of messages, this information no longer shows:

- Project name
- Link status
- Port status
- IP address

Complete these steps.

1. Add an MSG instruction to your program.
2. Configure the Configuration tab on the Message Configuration dialog box as described in [Table 39](#).

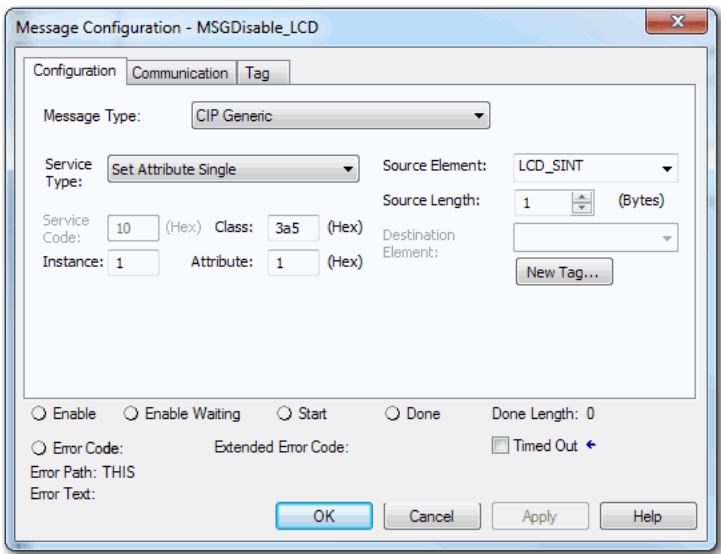
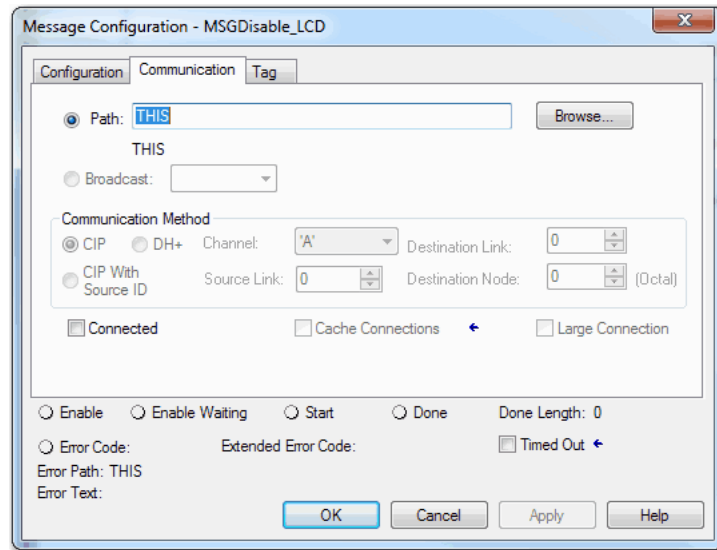


Table 39 - Disable All Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a5
Attribute	1
Source Element	Controller tag of SINT data type. In this example, the controller tag is named LCD_SINT.
Source Length	1

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

IMPORTANT Messages to THIS must be unconnected messages.



- Before you enable the MSG instruction, make sure that the Source Element tag value is 1.

IMPORTANT You can re-enable the 4-character display after it is disabled. To re-enable the 4-character display, 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 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 keyswitch 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 [Table 40](#).

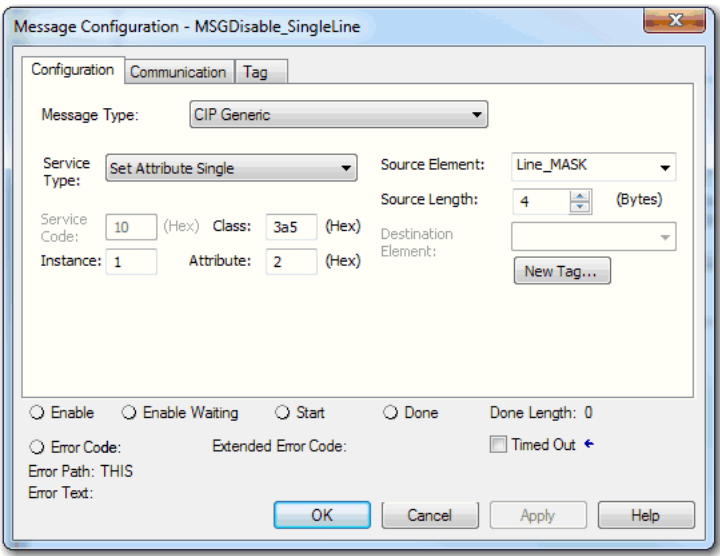
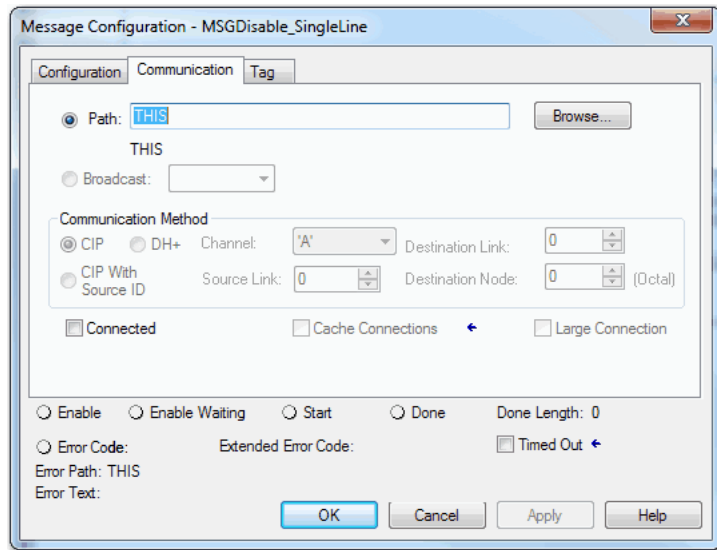


Table 40 - Disable Individual Categories of Messages

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. In this example, the controller tag is named Line_MASK.
Source Length	4

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

IMPORTANT Messages to THIS must be unconnected messages.



- 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.

Disable Controller Webpages

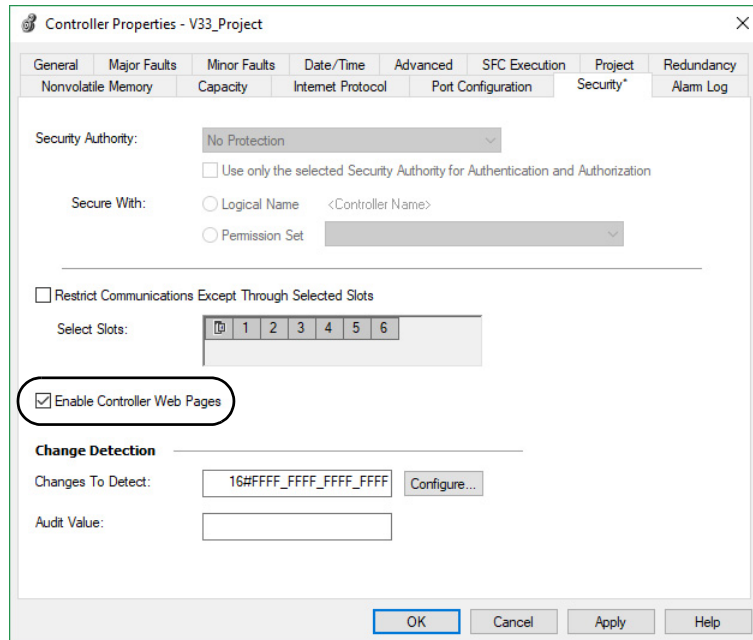
You can disable the controller webpages with the Studio 5000 Logix Designer application, version 28 or later.

Studio 5000 Logix Designer Application Version 33 or Later

With the Studio 5000 Logix Designer application version 33 or later, controller webpages are disabled by default.

While using a CIP Generic MSG to disable controller webpages is supported in version 33 or later, Rockwell Automation recommends these 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 SD 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 SD card.

- For CIP Security applications, you can also use FactoryTalk Policy Manager to disable the webpages (this overrides the Controller Properties checkbox).

Studio 5000 Logix Designer Application Version 32 or Earlier

For Studio 5000 Logix Designer application, version 32 or earlier, you use a CIP Generic MSG to execute this option.

See the following:

- [Use a CIP Generic MSG to Disable the Controller Webpages on page 173](#)
- [Use a CIP Generic MSG to Enable the Controller Webpages on page 175](#)

Controller Web Page Default Settings

These are the default settings for controller webpages:

- Webpages are enabled for controller firmware revision 32 or earlier
- Webpages are disabled for controller firmware revision 33 or later

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 web page configuration (webpages enabled) and does not automatically change to the default setting for version 33 (disable the webpages).

- You must reconfigure the settings to disable the controller webpages after it returns to its default settings.

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.

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 tab on the Message Configuration dialog box as described in the [Table 41 on page 174](#).

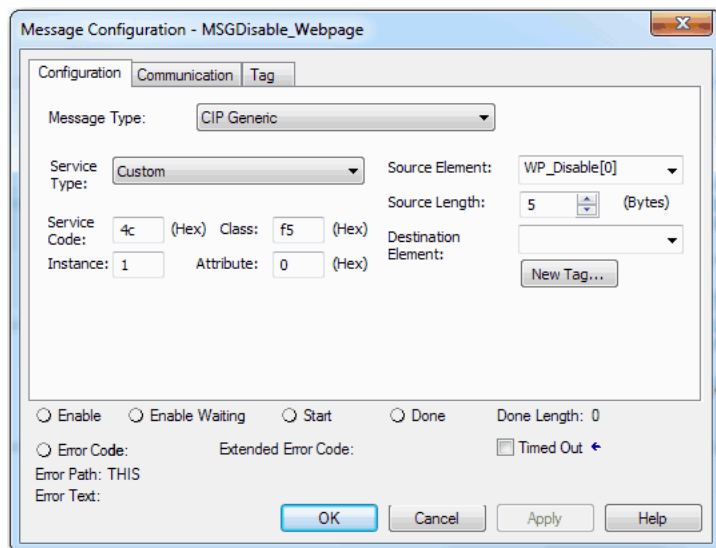
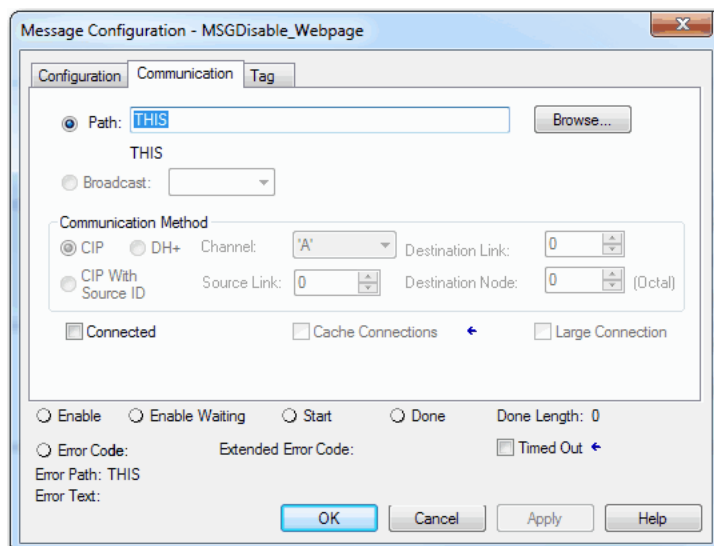


Table 41 - Disable the Webpages

Field	Description																								
Message Type	CIP Generic																								
Service Type	Custom																								
Service Code	4c																								
Instance	1																								
Class	f5																								
Attribute	0																								
Source Element	<p>Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Disable and must match the following graphic:</p> <table><tr><td>WP_Disable</td><td>{...}</td><td>Decimal</td><td>SINT[5]</td></tr><tr><td>WP_Disable[0]</td><td>1</td><td>Decimal</td><td>SINT</td></tr><tr><td>WP_Disable[1]</td><td>80</td><td>Decimal</td><td>SINT</td></tr><tr><td>WP_Disable[2]</td><td>0</td><td>Decimal</td><td>SINT</td></tr><tr><td>WP_Disable[3]</td><td>6</td><td>Decimal</td><td>SINT</td></tr><tr><td>WP_Disable[4]</td><td>0</td><td>Decimal</td><td>SINT</td></tr></table> <p>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.</p>	WP_Disable	{...}	Decimal	SINT[5]	WP_Disable[0]	1	Decimal	SINT	WP_Disable[1]	80	Decimal	SINT	WP_Disable[2]	0	Decimal	SINT	WP_Disable[3]	6	Decimal	SINT	WP_Disable[4]	0	Decimal	SINT
WP_Disable	{...}	Decimal	SINT[5]																						
WP_Disable[0]	1	Decimal	SINT																						
WP_Disable[1]	80	Decimal	SINT																						
WP_Disable[2]	0	Decimal	SINT																						
WP_Disable[3]	6	Decimal	SINT																						
WP_Disable[4]	0	Decimal	SINT																						
Source Length	5																								

- 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. On the Configuration tab of the Message Configuration dialog box, configure the message as described in [Table 42](#).

Message Configuration - MSGEnable_Webpage

Configuration* Communication Tag

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex) Instance: 1 Attribute: 0 (Hex)

Source Element: WP_Enable Source Length: 5 (Bytes) Destination Element:

Enable Enable Waiting Start Done Done Length: 0

Error Code: Extended Error Code: Timed Out

Error Path: THIS Error Text:

OK Cancel Apply Help

Table 42 - Enable 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. In this example, the controller tag is named WP_Enable and must match the following graphic:		
	WP_Enable	{...} Decimal	SINT[5]
	WP_Enable[0]	1 Decimal	SINT
	WP_Enable[1]	80 Decimal	SINT
	WP_Enable[2]	0 Decimal	SINT
	WP_Enable[3]	6 Decimal	SINT
	WP_Enable[4]	1 Decimal	SINT
	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		

- On the Communication tab, configure a Path to THIS.

IMPORTANT Messages to THIS must be unconnected messages.

The screenshot shows the 'Message Configuration - MSGEnable_Webpage' dialog box with the 'Communication' tab selected. The 'Path' is set to 'THIS'. The 'Communication Method' section shows 'CIP' selected, with 'Channel' set to 'A' and 'Destination Link' set to '0'. The 'CIP With Source ID' option is also visible. At the bottom, there are checkboxes for 'Connected', 'Cache Connections', and 'Large Connection', all of which are currently unchecked. The 'Error Path' is set to 'THIS'.

Message Configuration - MSGEnable_Webpage

Configuration* Communication Tag

☒ Path: THIS Browse...

THIS

☐ Broadcast: [v]

Communication Method

☒ CIP ☐ DH+ Channel: 'A' Destination Link: 0

☐ CIP With Source ID Source Link: 0 Destination Node: 0 (Octal)

☐ Connected ☐ Cache Connections ☐ Large Connection

☐ Enable ☐ Enable Waiting ☐ Start ☐ Done Done Length: 0

☐ Error Code: Extended Error Code: ☐ Timed Out

Error Path: THIS

Error Text:

OK Cancel Apply Help

Develop Motion Applications

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers support these motion interfaces:

- Integrated Motion on an EtherNet/IP™ network.
- Digital drive interfaces include EtherNet/IP connected drives and Sercos interface connected drives.
- Analog drives support $\pm 10V$ analog output and can interface with various feedback devices, such as quadrature encoder, SSI, and LVDT feedback.

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](#)

Motion Overview

The controllers support up to 256 axes of integrated motion. The 256 axes can be 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.



Rockwell Automation recommends using the built-in EtherNet/IP port for high-performance motion applications.

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.

Drive Type	Requirements
CIP Motion™	<ul style="list-style-type: none"> • EtherNet/IP communication module • Digital drive with an EtherNet/IP connection
Sercos interface	Select a Sercos interface module: <ul style="list-style-type: none"> • 1756-M03SE • 1756-M08SE • 1756-M16SE
Analog interface	Select an analog interface module: <ul style="list-style-type: none"> • 1756-HYD02 • 1756-M02AE • 1756-M02AS

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](#).



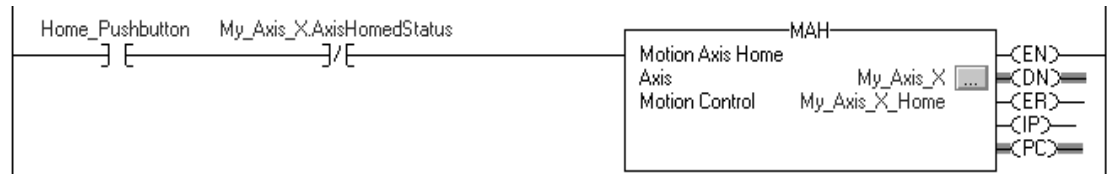
ATTENTION: Use each motion control tag in only one motion instruction. Unintended operation can result if you reuse the same motion control tag in other motion instructions, or if you write to any of the motion control tag elements.

In this example, a simple ladder diagram that homes, jogs, and moves an axis.

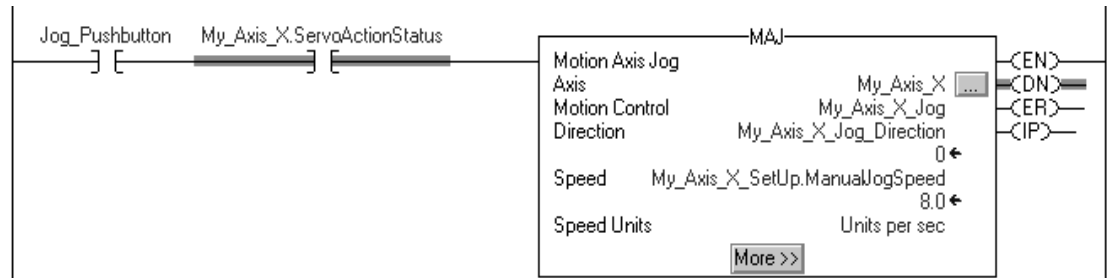
If Initialize_Pushbutton = on and the axis = off (My_Axis_X.ServoActionStatus = off) then the MSO instruction turns on the axis.



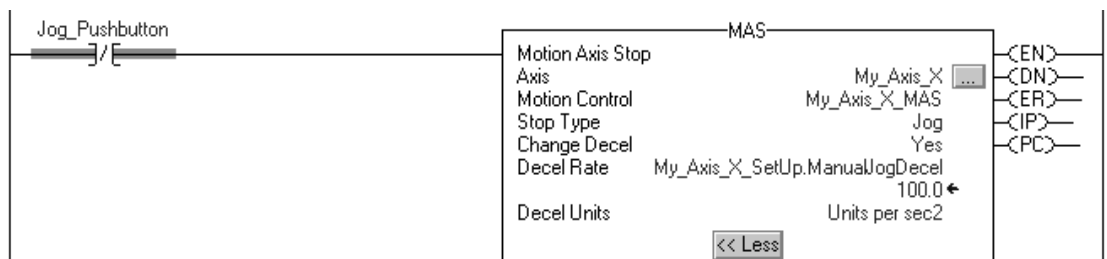
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off) then the MAH instruction homes the axis.



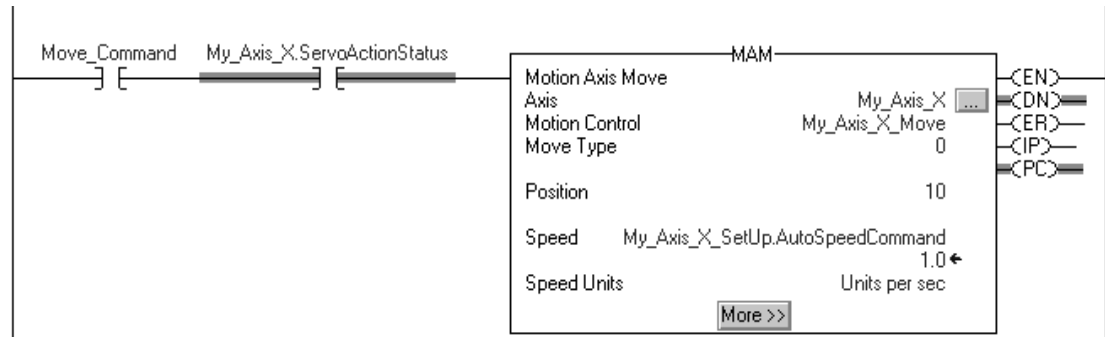
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAJ instruction jogs the axis forward at 8 units/second.



If Jog_Pushbutton = off then the MAS instruction stops the axis at 100 units/second². 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.

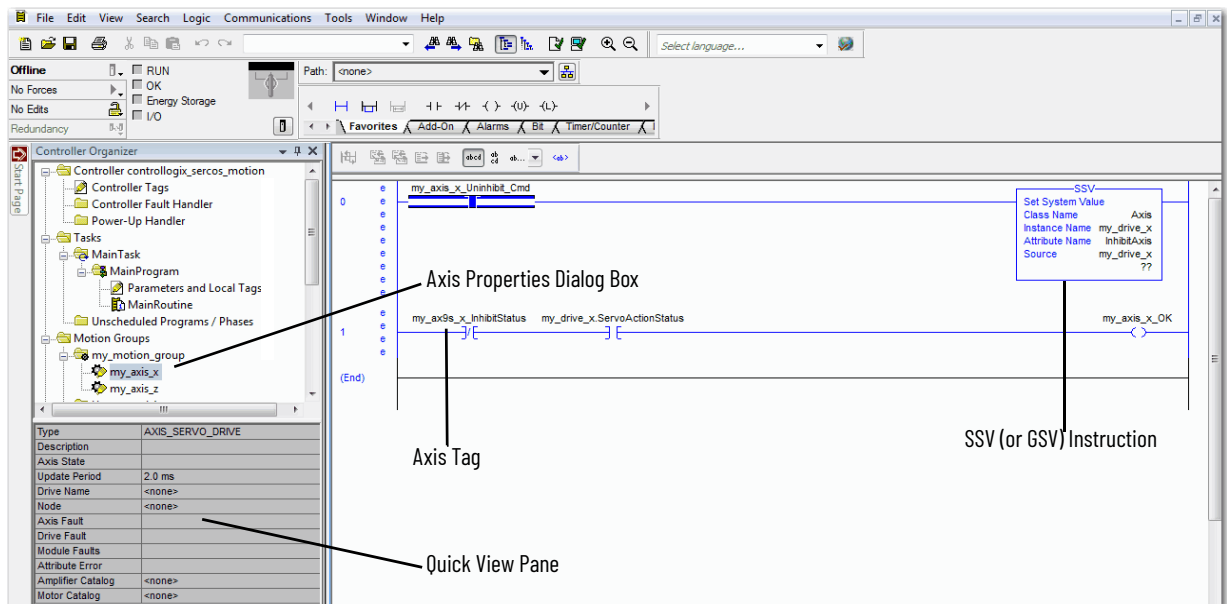


Obtain Axis Information

You can obtain axis information by using these methods:

- Double-click the axis to open the Axis Properties dialog box.
- Use a Get System Value (GSV) or Set System Value (SSV) instruction to read or change the configuration at runtime.
- View the QuickView™ pane to see the state and faults of an axis.
- Use an axis tag for status and faults.

Figure 44 - Obtain Axis Information



Notes:

Troubleshoot the Controller

This chapter describes how to troubleshoot the controller if issues occur during normal operation. In addition to the ways described in this chapter, you can use messages on the 4-character display to troubleshoot the controller. For more information, see [Status Indicators on page 199](#).

Automatic Diagnostics

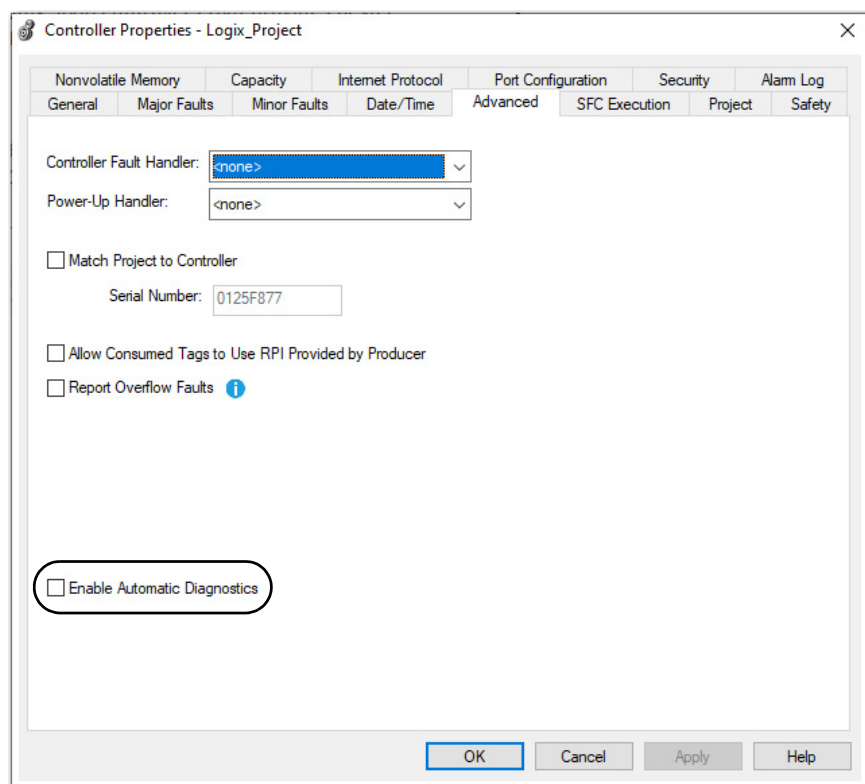
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Automatic Diagnostics is a system-level feature in Logix 5000 controllers that provides device diagnostics to HMI's and other clients, with zero programming. The diagnostics include device description conditions and state events.

Automatic Diagnostics is enabled by default in Logix 5000 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.



Considerations for Communication Loss Diagnostics

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

The response time and diagnostic information for a loss of communication depends on the device and configuration settings.

Type of Connection	Device Behavior
Direct connection to a Logix 5000 controller	Device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter.
No connection to a Logix 5000 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	Device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter
Rack-optimized connection	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:

- Communication loss diagnostics for all devices in the controller I/O configuration
- Device-level automatic diagnostics evaluations for all uninhibited and enabled devices.

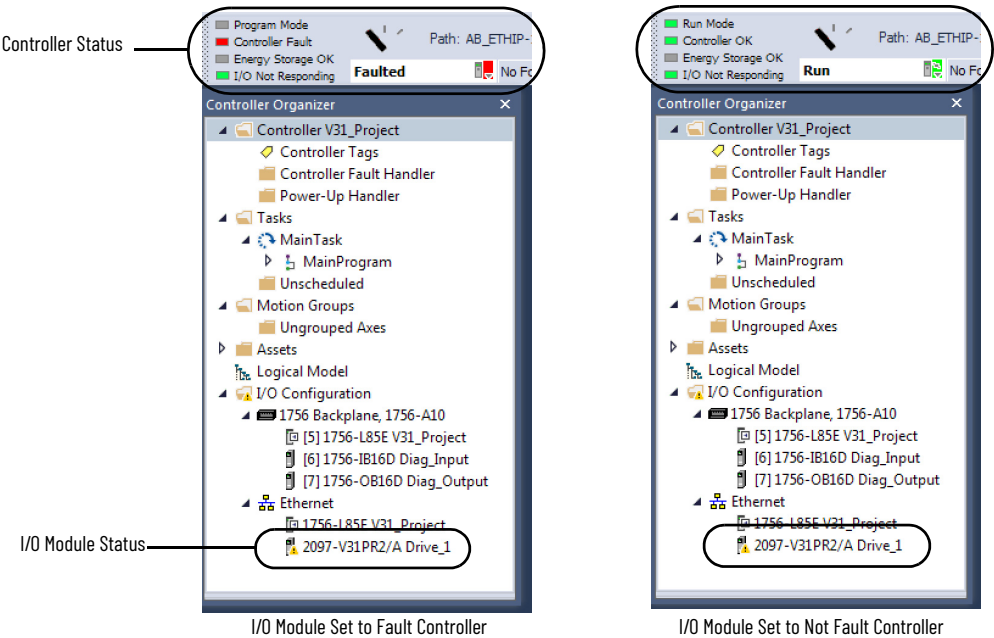
You can disable Automatic Diagnostics for a specific device in the device configuration. The communication loss diagnostic remains active even if the device disables Automatic Diagnostics. To disable communication loss diagnostic, inhibit the device or disable Automatic Diagnostics at the controller.

Controller Diagnostics with the Logix Designer Application

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

A warning symbol appears in the controller organizer next to the I/O module. This occurs when there are faults or other conditions in the I/O module, or if the connection to the I/O module fails while in run mode.

- If you have set a standard I/O module to fault the controller when the connection fails, then the controller state indicates Faulted and the controller status displays Controller Fault and is lit steady red. I/O Not Responding blinks green.
- If you have set a standard I/O module to not fault the controller when the connection fails, or there is a safety connection fault, then the controller status displays Controller OK and is lit steady green. I/O Not Responding blinks green.



IMPORTANT Safety Consideration

You cannot configure safety connections to automatically fault the controller.

I/O Module Properties

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The Module Properties dialog box for an I/O device shows fault information:

- The General view shows a Faulted status.
- The Connection view shows the module fault.
- The Module Info view lists the major and minor faults along with the internal state of the module.

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.

If communication is faulted and you try to view the Module Info view, a dialog box appears that shows the module reported general error status and the fault code.

Figure 45 - I/O Fault Status on General View

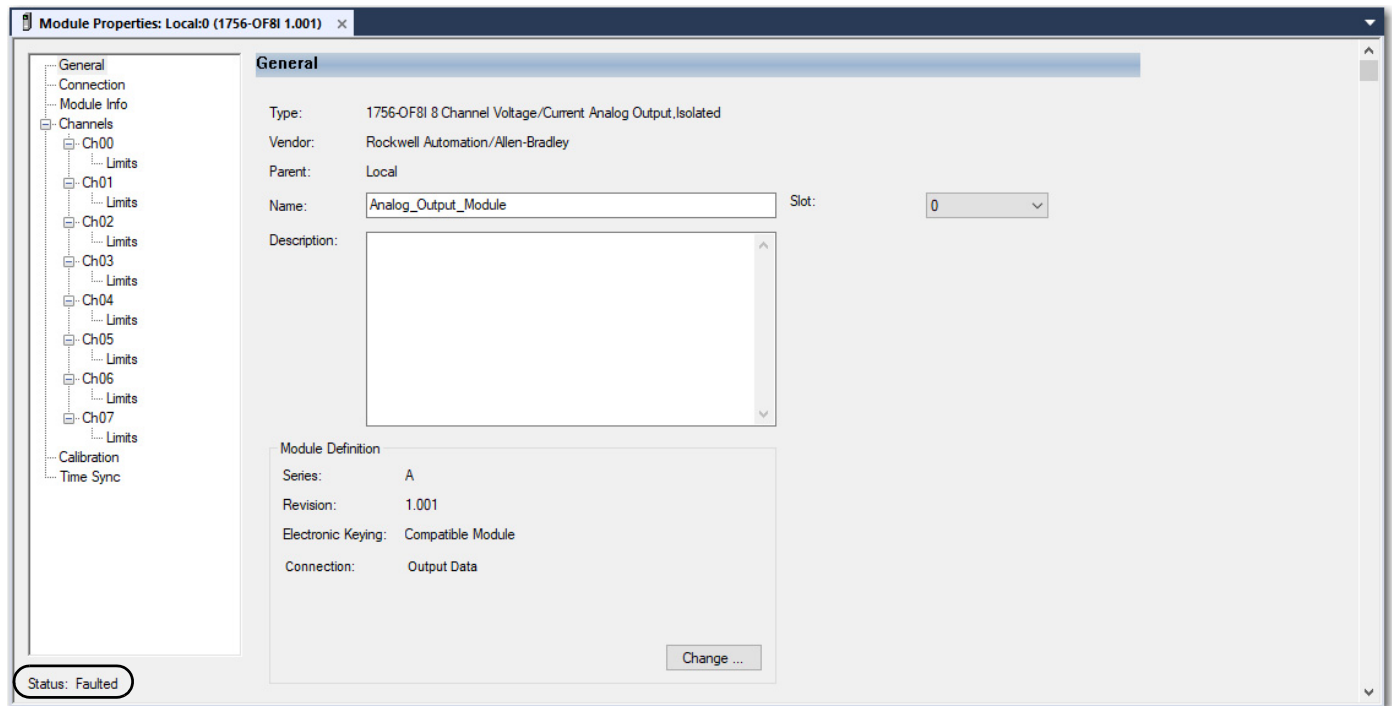
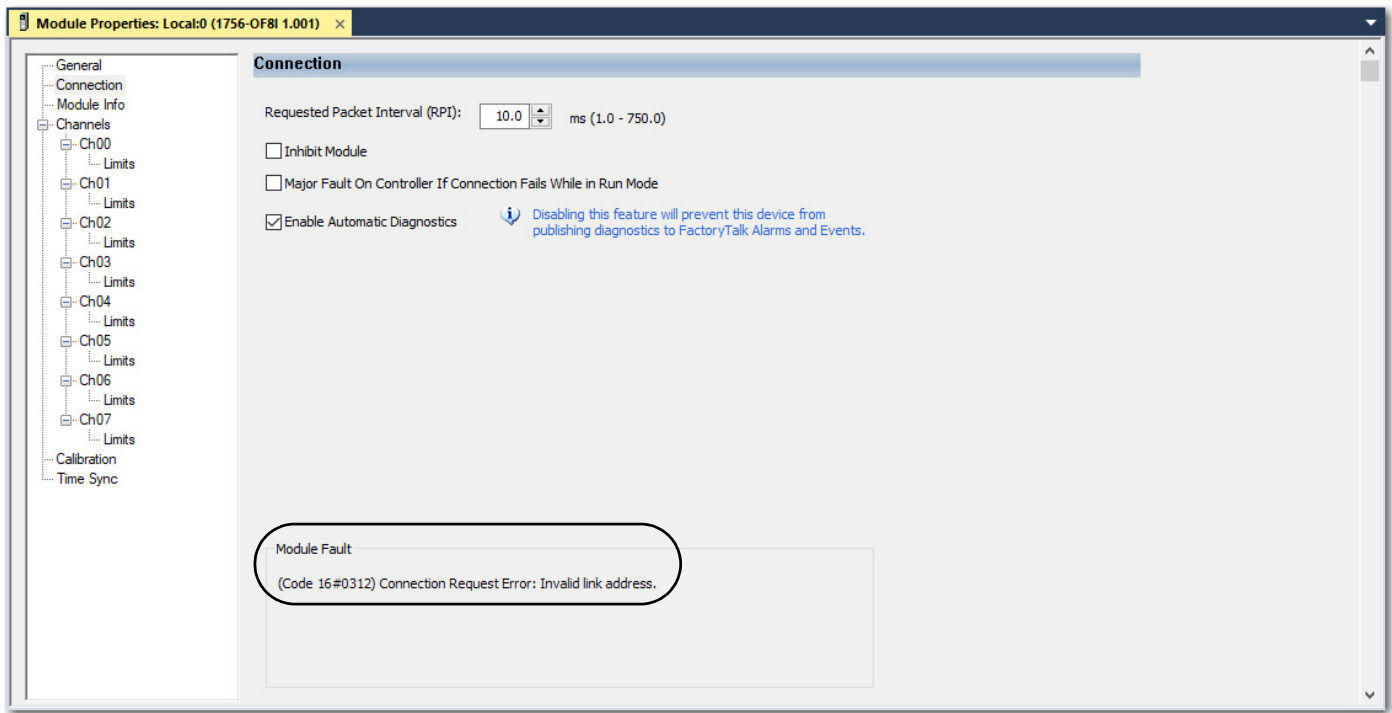


Figure 46 - I/O Fault on Connection View



Notification in the Tag Monitor

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 47 - I/O Module Fault










Scope:  Test_case_1		Show: All Tags			
Name	Value	Force Mask	Style	Data Type	
 Local:1:C	{...}	{...}		AB:1756_OF8I:C:0	
 Local:1:I	{...}	{...}		AB:1756_OF8I:I:0	
 Local:1:I.Fault	2#1111_11...		Binary	DINT	
 Local:1:I.Fault.0	1		Decimal	BOOL	
 Local:1:I.Fault.1	1		Decimal	BOOL	
 Local:1:I.Fault.2	1		Decimal	BOOL	
 Local:1:I.Fault.3	1		Decimal	BOOL	
 Local:1:I.Fault.4	1		Decimal	BOOL	

Figure 48 - Safety I/O Connection Fault

Controller Tags - SIL_3_Safety_Project(controller)					
Scope: SIL_3_Safety_Pr		Show: All Tags			
Name	Value	Force Mas	Style	Data Type	
Remote_Safety_Input_2:I	{...}	{...}		AB:1732ES_IB12XOB4_Safety1:I:0	
Remote_Safety_Input_2:I.ConnectionFaulted	1		Decimal	BOOL	
Remote_Safety_Input_2:I.Pt00Data	0		Decimal	BOOL	
Remote_Safety_Input_2:I.Pt01Data	0		Decimal	BOOL	
Remote_Safety_Input_2:I.Pt02Data	0		Decimal	BOOL	
Remote_Safety_Input_2:I.Pt03Data	0		Decimal	BOOL	
Monitor Tags / Edit Tags					

Enable Major Fault on Controller

Applies to these controllers:

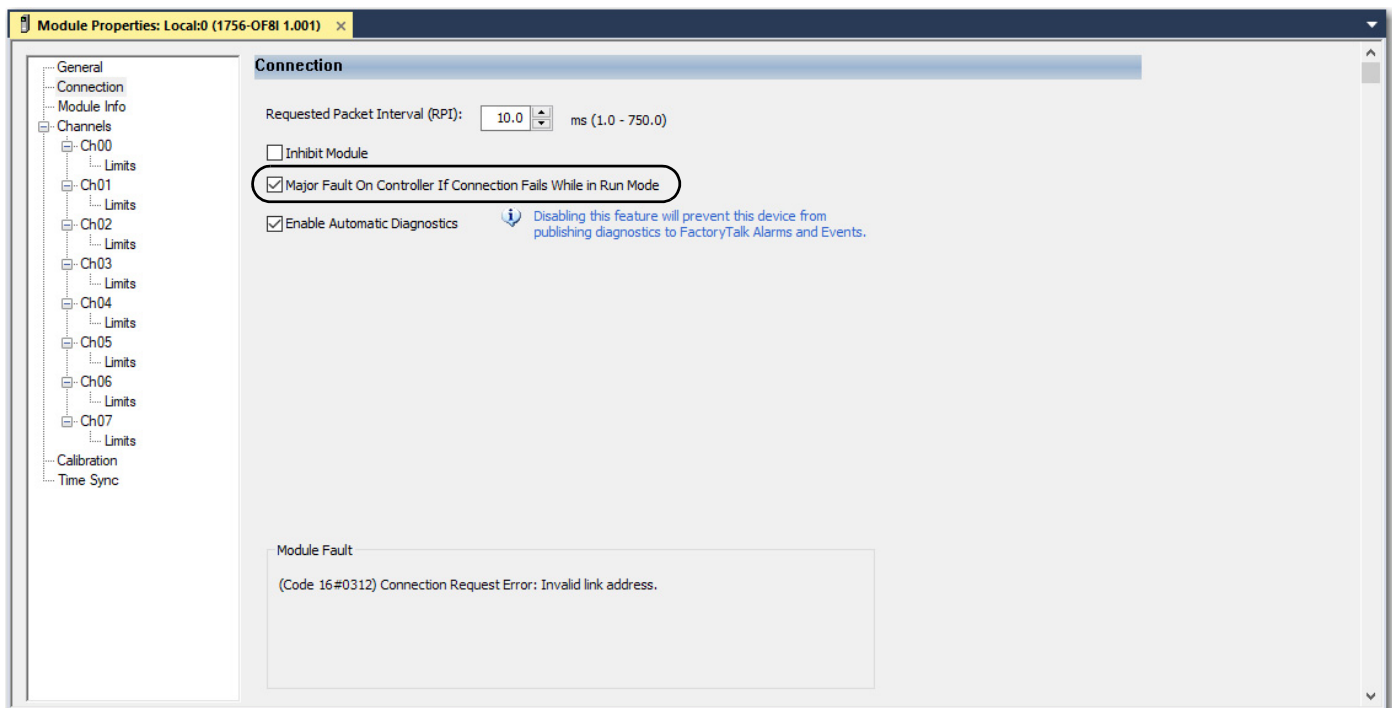
ControlLogix 5580

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.



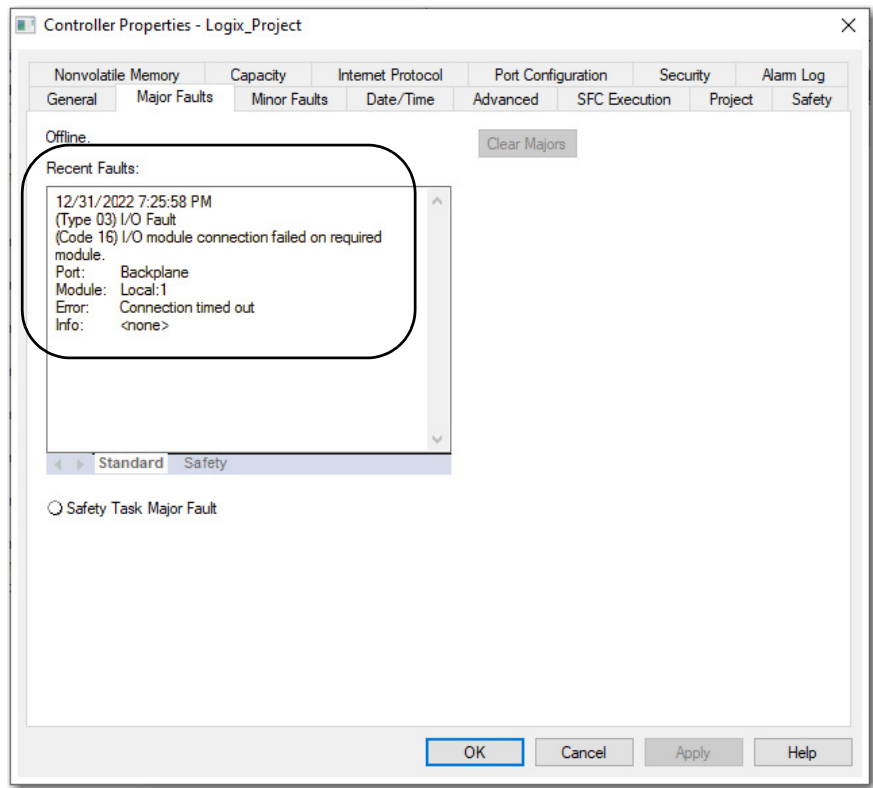
WARNING: If you select this option, a connection fault on the I/O module can cause a major fault on the controller. A major fault on the controller causes the outputs to go to their configured fault state.

Figure 49 - Major Fault on Controller Checkbox



When you are monitoring the configuration properties of a module in the 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 50 - Major Faults in Controller Properties



Port Diagnostics

Applies to these controllers:

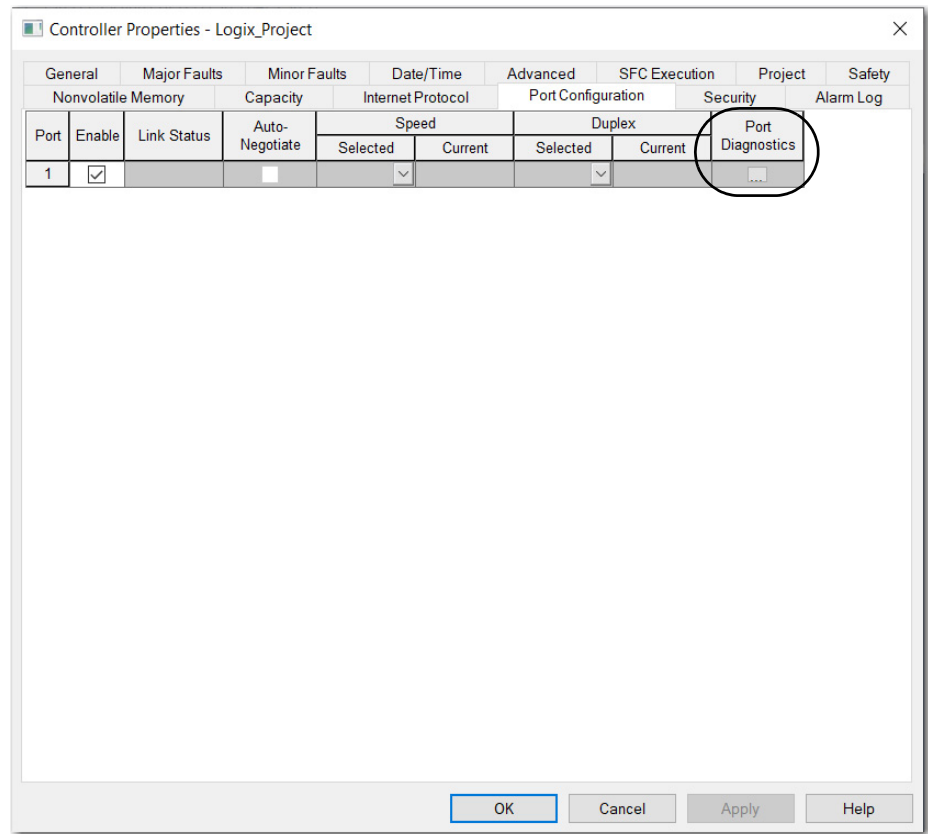
ControlLogix 5580

GuardLogix 5580

When your project is online, you can view the status of the embedded Ethernet port on the controller.

On the Controller Properties dialog box, click the Port Configuration tab and then click the Ellipse button in the Port Diagnostics column.

Figure 51 - Ethernet Port Diagnostics



The Port Diagnostics dialog box displays diagnostic details. For descriptions, see [Table 43 on page 188](#) for parameter descriptions.

Figure 52 - Port Diagnostic Details

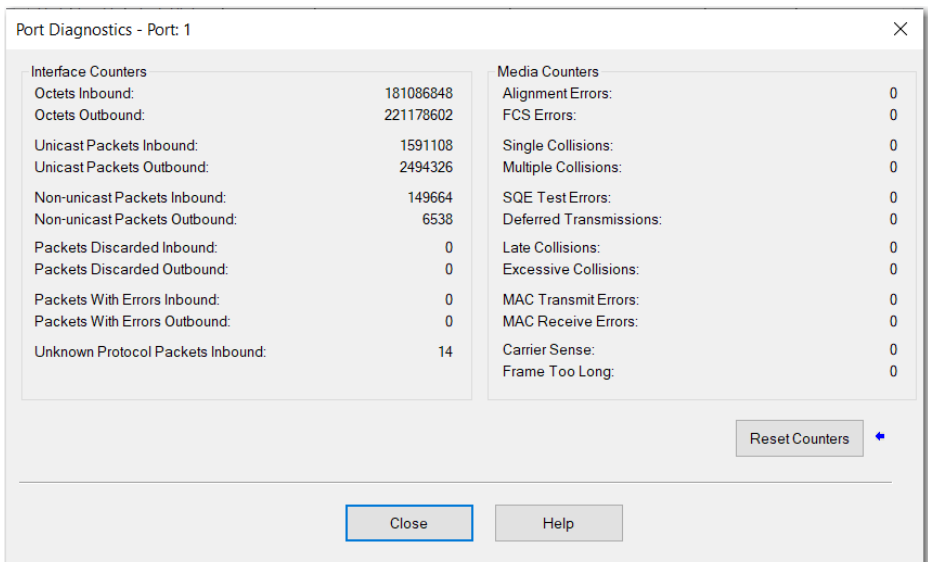


Table 43 - Port Diagnostics Parameters - Logix Designer Application

Parameter	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. Reset Counter appears dimmed when offline or when online and a communication error occurs.

Advanced Time Sync

Applies to these controllers:

ControlLogix 5580

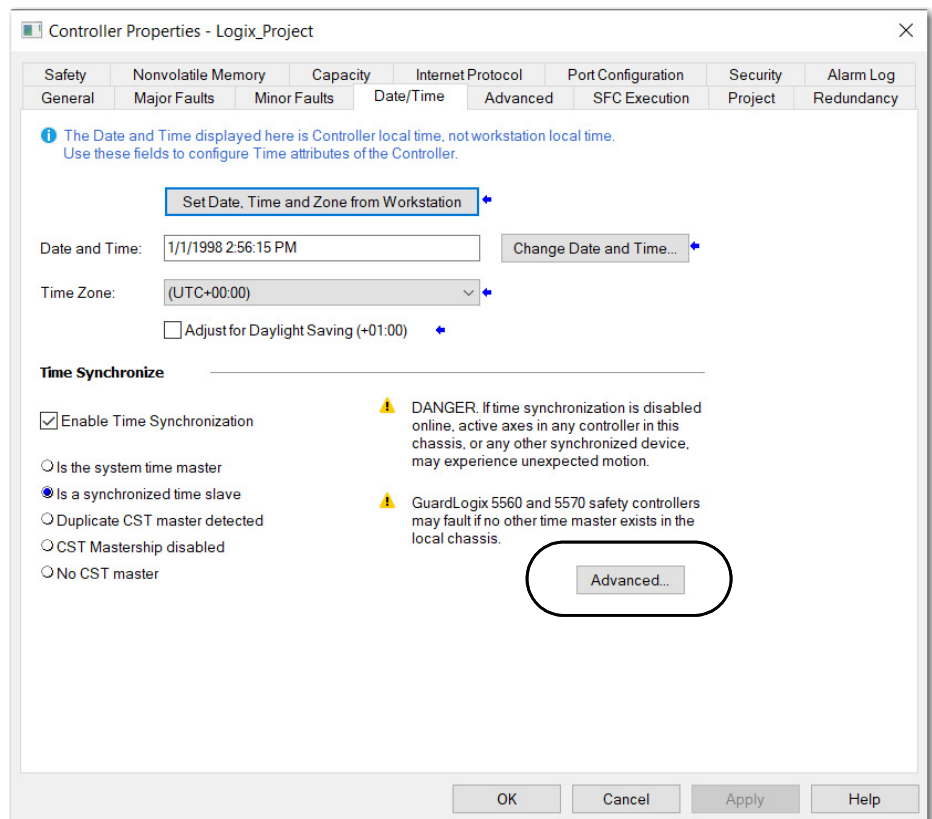
GuardLogix 5580

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/updates the Precision Time Protocol on a control system network should 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.

1. On the Date/Time tab, click the Advanced button.



The Advanced Time Sync dialog box opens. See [Table 44 on page 190](#) for parameter descriptions.

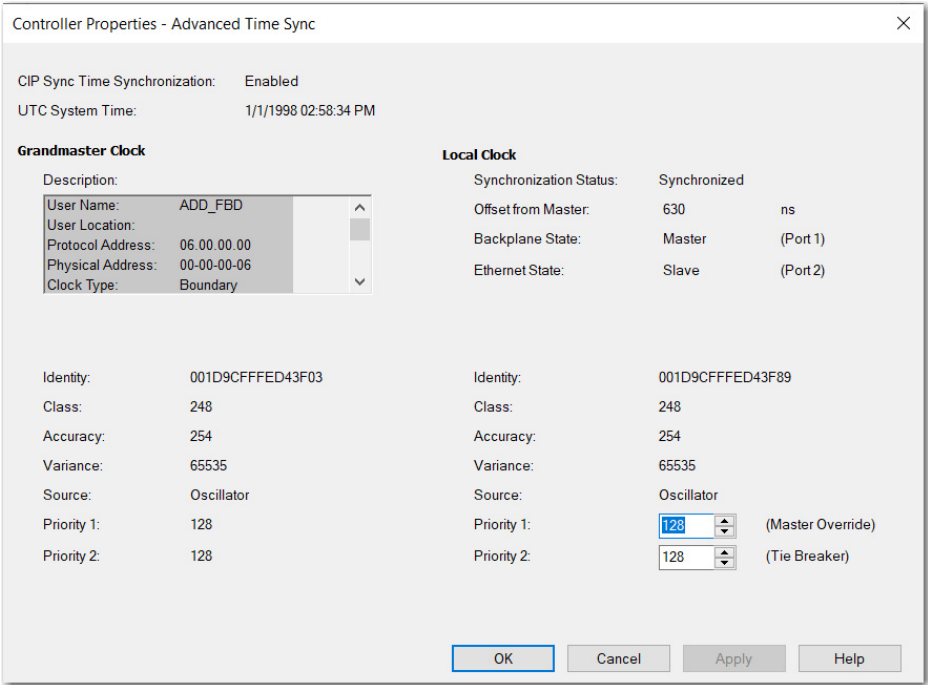


Table 44 - Advanced Time Sync Parameters

Grandmaster Clock	
Description	<p>Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified:</p> <ul style="list-style-type: none">• 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 <p>Use the vertical scroll bar to view the data.</p>
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.
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	<p>Displays the time source of the Grandmaster clock. The available values are:</p> <ul style="list-style-type: none">• 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	

Table 44 - Advanced Time Sync Parameters (Continued)

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 time 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 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: <ul style="list-style-type: none"> Atomic Clock GPS Terrestrial Radio PTP NTP HAND set Other Oscillator

Controller Diagnostics with Linux-based Software

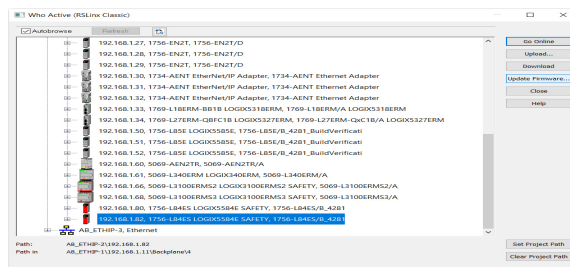
Applies to these controllers:

ControlLogix 5580

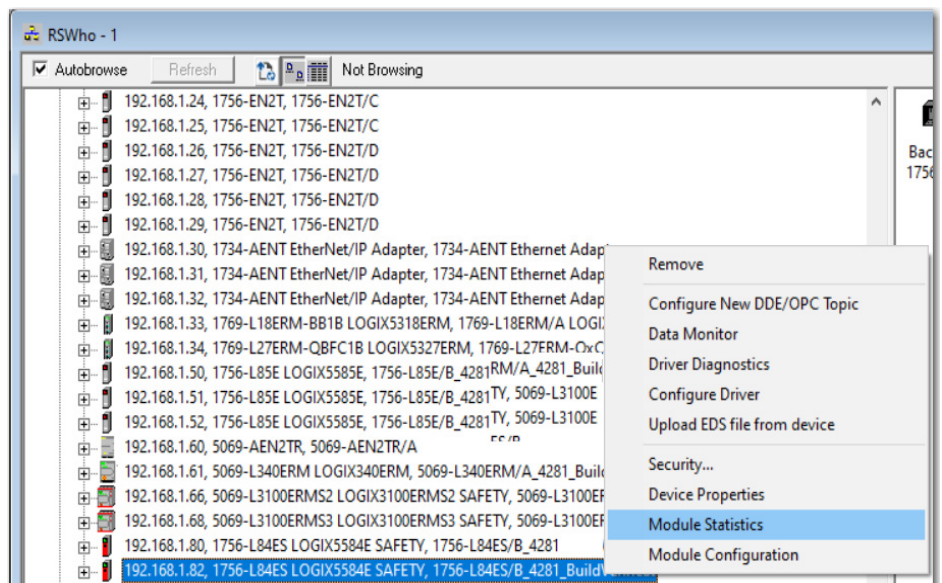
GuardLogix 5580

You can also view diagnostic information in Linux-based software.

1. From the Communications menu, select RSWho.

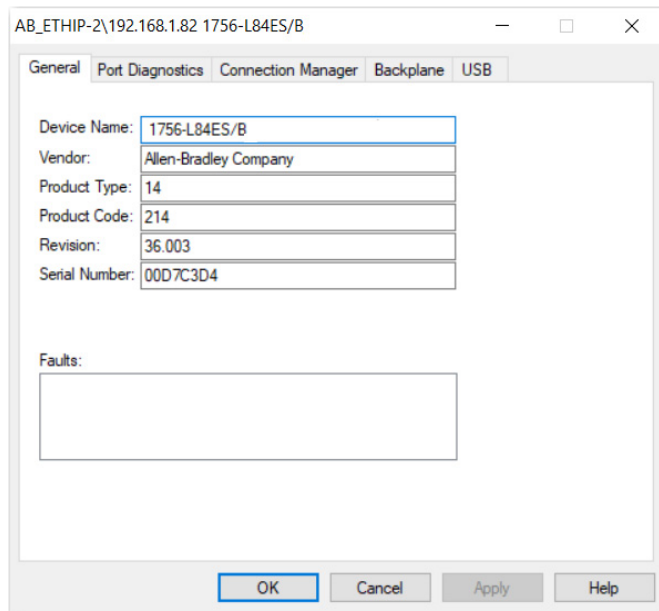


2. Navigate to the Ethernet network.
3. Right-click the controller and choose Module Statistics.



The Module Statistics dialog box shows this information:

- The General tab shows device information, and any faults on the controller.
- The Port Diagnostics tab shows information for the EtherNet/IP™ port.
- The Connection Manager Tab shows information on connection requests.
- The Backplane tab shows general status and diagnostic-related information about the ControlLogix® backplane.
- The USB tab shows information about the USB port.



Controller Webpages

Applies to these controllers:

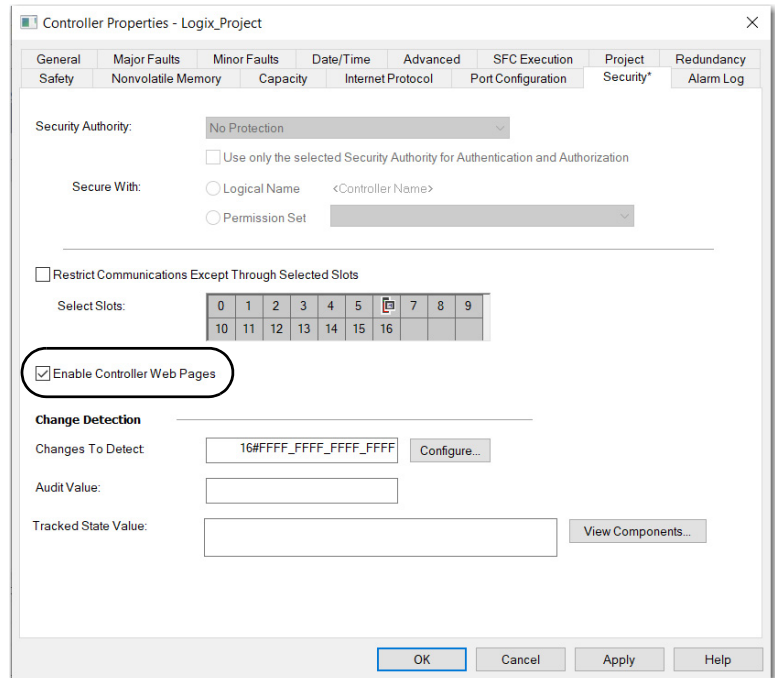
ControlLogix 5580

GuardLogix 5580

The controller provides diagnostic webpages that track controller performance, network performance, and backplane performance. Controller webpages are read-only.

IMPORTANT With the Studio 5000 Logix Designer application version 33 or later, controller webpages are disabled by default.

- 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.

To access the diagnostic webpages, open the Diagnostics folder in the leftmost navigation bar, and click the link for each diagnostic webpage you monitor.

- The home page provides device information and controller status.
- The Faults webpage shows major and minor faults on the controller.
- The Diagnostics webpages provide communications and messaging data for the controller.
- The Advanced diagnostics webpages provide data about the TCP/IP Network and Precision Time Protocol.

Home Webpage

With Studio 5000 Logix Designer application version 32 or later, the Home webpage also shows:

- Current 4-character display messages
- Controller status indicators state
- EtherNet/IP status indicators state
- Safety Signature, Safety Locked Status, Safety Status (for GuardLogix® 5580 and Compact GuardLogix 5380 controllers)

To set the refresh rate of the webpages, input the number of seconds into the Refresh field at the bottom of the webpage.

Figure 53 - ControlLogix 5580 Home Webpage

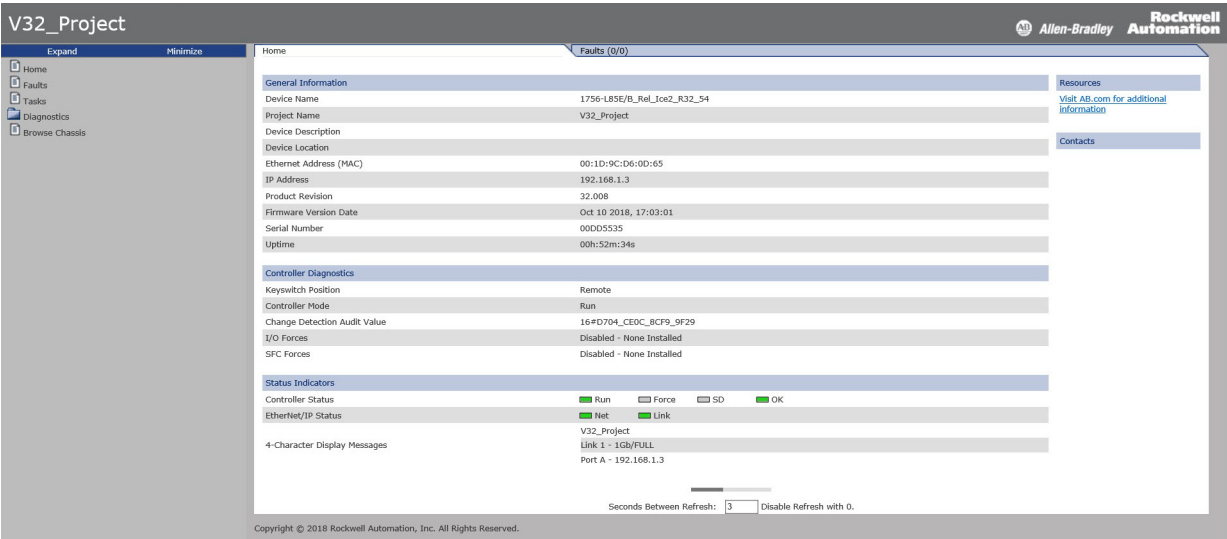
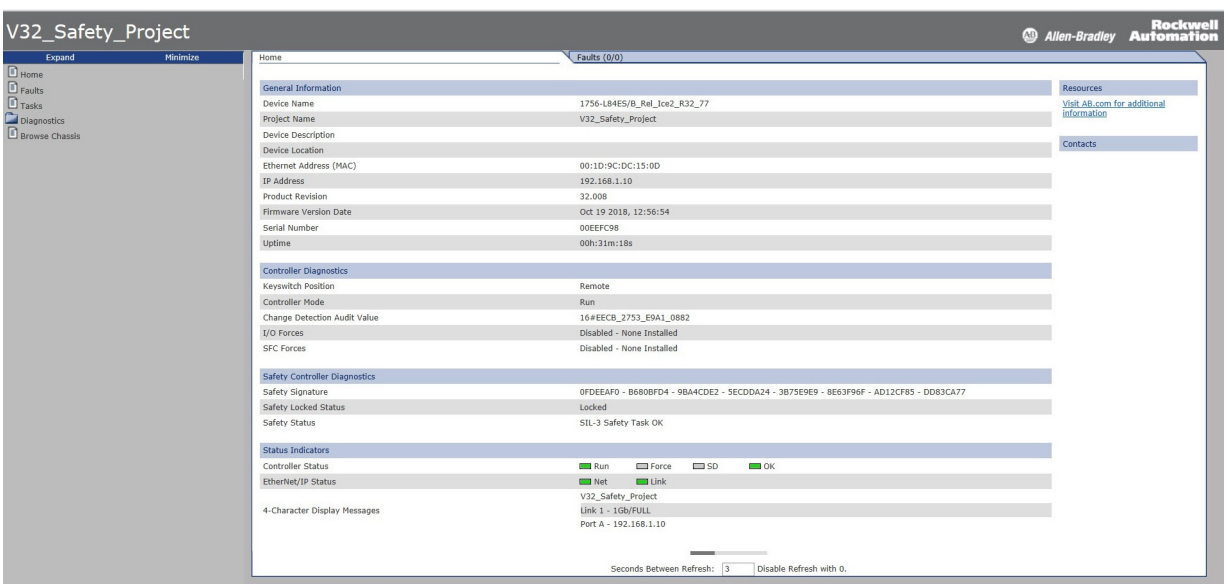


Figure 54 - GuardLogix 5580 Home Webpage



Faults Webpage

With Studio 5000 Logix Designer application version 32 or later, the Faults webpage shows major and minor faults on the controller.

ControlLogix 5580 Faults Webpage

The screenshot shows the 'V32_Project' interface with the 'Faults' tab selected. The left sidebar contains 'Home', 'Faults', 'Tasks', 'Diagnostics', and 'Browse Chassis'. The main content area displays a table of faults.

Major faults (2)				
2018-10-24 12:55:30	Type 04	Program Fault (can be trapped by a fault routine)	Code 20	Array subscript too large, or CONTROL data type POS or LEN invalid.
2018-10-24 12:55:30	Type 04	Program Fault (can be trapped by a fault routine)	Code 20	Array subscript too large, or CONTROL data type POS or LEN invalid.

Minor faults (8)				
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.
2018-10-24 12:55:27	Type 04	Program Fault	Code 35	PID delta time was less than 0.

Seconds Between Refresh: 3 Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

GuardLogix 5580 Faults Webpage

The screenshot shows the 'V32_Safety_Project' interface with the 'Faults' tab selected. The left sidebar contains 'Home', 'Faults', 'Tasks', 'Diagnostics', and 'Browse Chassis'. The main content area displays a table of faults.

Major faults (1)				
1999-01-01 05:30:40	Type 14	Safety Task Fault	Code 01	Task watchdog expired. May have been caused by infinite loop, complex program, higher priority task, or removal of Safety partner.

Minor faults (0)				
No faults found.				

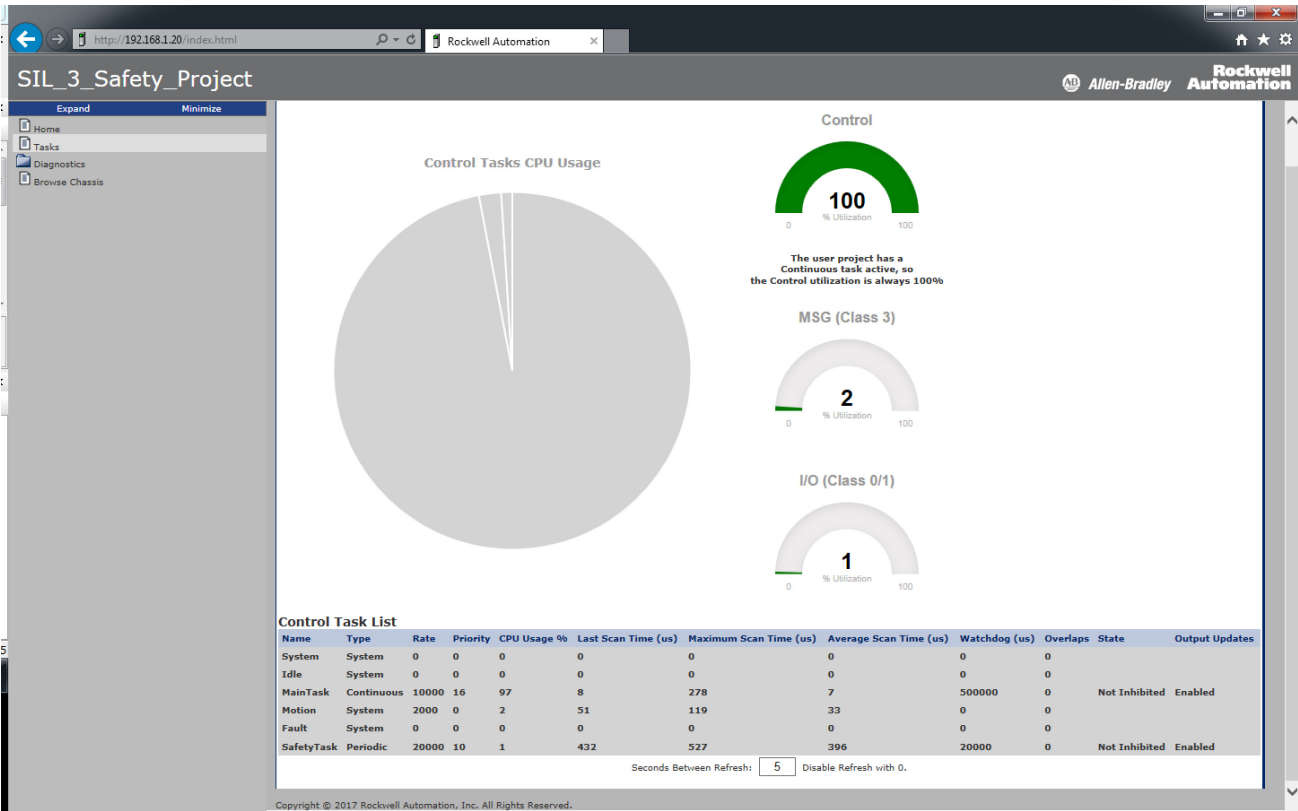
Seconds Between Refresh: 3 Disable Refresh with 0.

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

Tasks Webpage

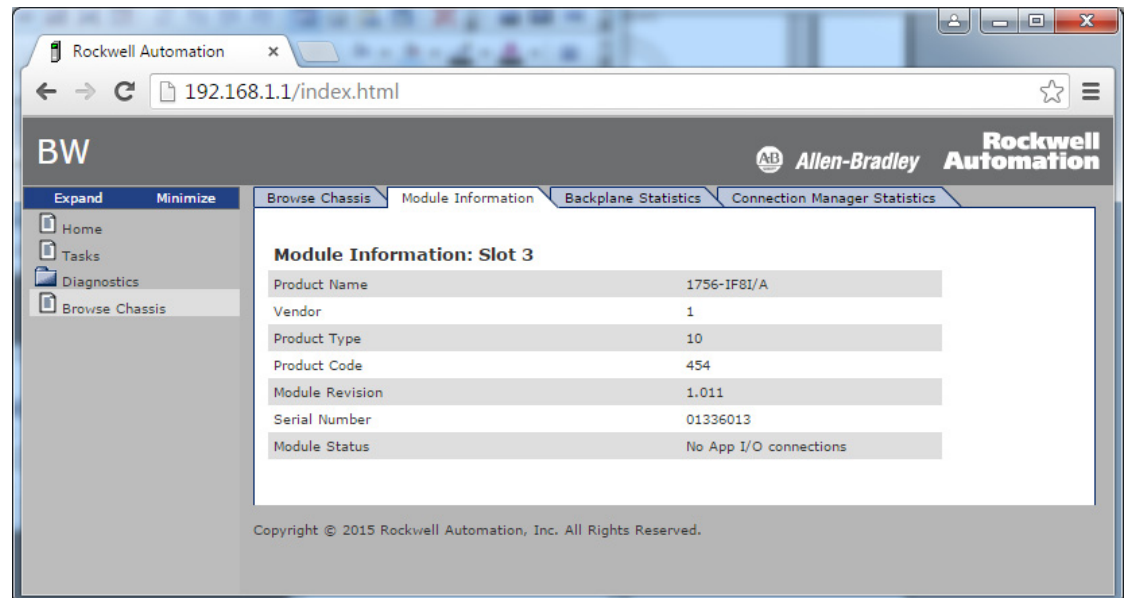
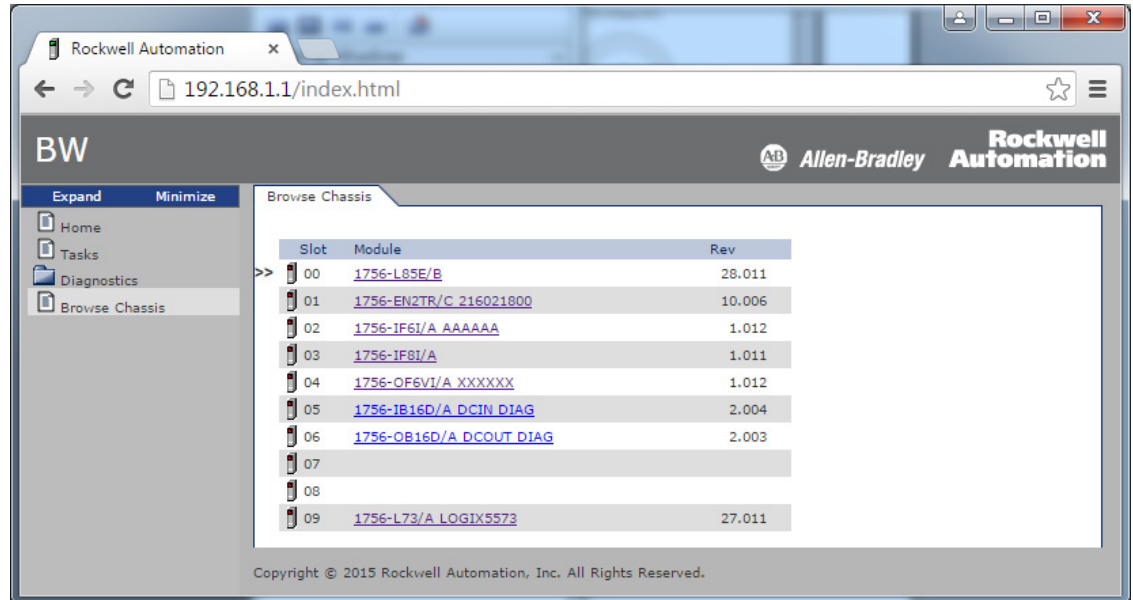
On the Tasks webpage, the pie chart shows the percentage of the control core's CPU consumed by the tasks that are on that core. The gauges show the CPU utilization of the control and communications cores. The table shows the tasks that are running on the control core (all system tasks are summarized as one task).

This example shows the Tasks webpage from a GuardLogix 5580 controller:



Browse Chassis Webpage

Browse Chassis lets you view module information, backplane statistics, and connection statistics for modules in the local chassis.

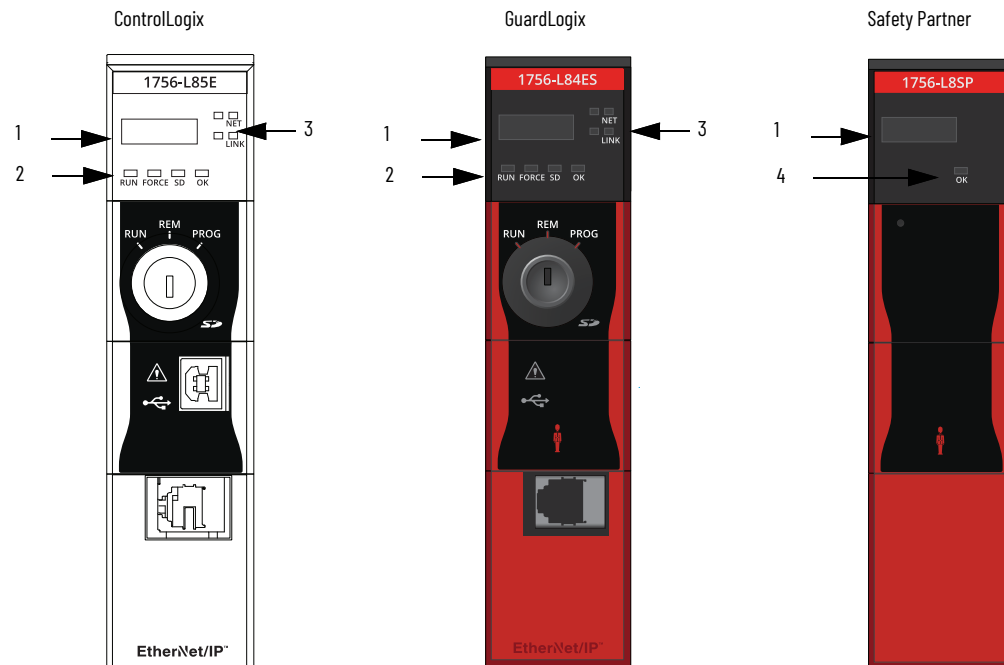


Notes:

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.

Status Display and Indicators



Item	Description
1	4-Character Scrolling Status Display You can disable some of these messages, see Disable the 4-character Status Display on page 167 .
2	Controller Status Indicators, see page 203
3	EtherNet/IP™ Status Indicators, see page 205
4	Safety Partner OK Status Indicator, see page 204

General Status Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The scrolling messages that are described in [Table 45](#) are typically indicated upon powerup, powerdown, and while the controller is running to show the status of the controller.

Table 45 - Controller General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Check the OK indicator to determine if the controller is powered and determine the state of the controller.
Identity Mismatch—Contact Tech Support	Beginning with firmware revision 34.011, if a firmware update identifies the controller as not authentic, the hardware is permanently disabled.
Missing Vendor Certificate—Contact Tech Support	
Bad Vendor Certificate—Contact Tech Support	
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. You can also view the SD Indicator (see page 204) for more status information. Allow the save to complete before: <ul style="list-style-type: none"> 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. You can also view the SD Indicator (see page 204) for more status information. Allow the load to complete before doing the following: <ul style="list-style-type: none"> 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. You can also view the SD Indicator (see page 204) for more status information. If you do not want the firmware to update upon powerup, change the Load Image property of the controller.
Rev XX.xxx	The major and minor revision of the firmware of the controller.
1756-L8XX	The controller catalog number and series.
Link Down	Message appears when the EtherNet/IP port does not have a connection. Message scrolls continuously during operation.
Link Disabled	Message appears when you have disabled the EtherNet/IP port. Message scrolls continuously during operation.
DHCP- 00:00:XX:XX:XX:XX	Message appears when the controller is set for DHCP, but not configured on a network. The message shows the MAC address of the controller. 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/IP port has a connection. 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	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. Message scrolls continuously during operation.
No Project	No project is loaded on the controller. To load a project, do one of the following: <ul style="list-style-type: none"> Use the Studio 5000 Logix Designer® application to 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.

Table 45 - Controller General Status Messages (Continued)

Message	Interpretation
Corrupt Certificate Received	The security certificate that is associated with the firmware is corrupted. Go to http://www.rockwellautomation.com/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 http://www.rockwellautomation.com/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 in the event of a powerdown. 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 in the event of a powerdown. If you see this message, then save your program to the SD card before you remove power, and then replace the controller.
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.

GuardLogix Status Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

In addition to the general status messages in [Table 45](#), a GuardLogix® 5580 controller display can show these scrolling messages.

Table 46 - Safety Controller 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 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/PLc configuration.
Hardware Incompatible	The safety partner and primary controller hardware is incompatible. You must use the 1756-L8SP safety partner with GuardLogix 5580 Controllers. The controller displays this message only in a SIL 3/PLc configuration.
Firmware Incompatible	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/PLc 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

Applies to these controllers:

GuardLogix 5580

The safety partner display can show these scrolling messages.

Table 47 - Safety Partner Status Messages

Message	Interpretation
L8SP	Standard display text. If there is a major non-recoverable fault, then the fault code scrolls across the display.
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.

Fault Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

If the controller displays a fault, these scrolling messages can appear on the status display.

Table 48 - Fault Messages

Message	Interpretation
Major Fault TXX: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. For details about major recoverable faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
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. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
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 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. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
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 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. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
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. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .

Major Fault Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The Major Fault TXX:CXX message on the controller scrolling display indicates major faults.



This manual links to Logix 5000 Controller and I/O Fault Codes, publication, [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

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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 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 manual links to Logix 5000 Controller and I/O Fault Codes, publication, [1756-RD001](#); the file automatically downloads when you click the link.

For suggested recovery methods for I/O faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication [1756-PM014](#).

Controller Status Indicators

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The status indicators are below the status display on the controller. They indicate the state of the controller as described in these tables.

IMPORTANT

Safety Consideration

Status indicators are not reliable indicators 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 indicator shows the current mode of the controller.

To change the controller mode, you can use the keyswitch on the front of the controller or the Controller Status menu in the Logix Designer application.

Table 49 - RUN Indicator

State	Description
Off	The controller is in Program or Test mode.
Steady green	The controller is in Run mode.

FORCE Indicator

The Force indicator shows if I/O forces are enabled on the controller.

Table 50 - FORCE Indicator

State	Description
Off	No tags contain I/O force values, and I/O force values are not enabled.
Solid amber	I/O forces enabled. If any I/O force values exist they are active. IMPORTANT: Use caution if you change any force values. In this state, the changes take effect immediately.
Flashing amber	I/O forces exist in the application, but are not active because I/O forces are not enabled. IMPORTANT: Use caution if you enable I/O forces. All existing I/O force values take effect immediately.

SD Indicator

The SD indicator shows if the SD card is in use.

Table 51 - SD 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.
Solid green	IMPORTANT: 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.
Flashing red	The SD card does not have a valid file system.
Solid red	The controller does not recognize the SD card.

OK Indicator

The OK indicator shows the state of the controller.

Table 52 - ControlLogix® and GuardLogix Controllers OK Indicator

State	Description
Off	No power is applied to the controller.
Flashing red	One of the following is true: <ul style="list-style-type: none"> 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 Update Controller Firmware on page 30. 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.
Solid red	One of the following is true: <ul style="list-style-type: none"> The controller is completing power-up diagnostics. The charge of the capacitor in the ESM is being discharged 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.
Solid green	The controller is operating normally.

Safety Partner OK Indicator

Applies to these controllers:

GuardLogix 5580

The safety partner has an OK status indicator.

Table 53 - 1756-L8SP Safety Partner OK Indicator

Sate	Description
Off	No power is applied.
Green	The safety partner is operating with no faults.
Red	One of the following is true: <ul style="list-style-type: none"> 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 indicator receives power. Once the safety partner cools down to an acceptable temperature, then full power is applied.
Flashing Red	Controller is configured for SIL 2 operation but a safety partner is installed.

EtherNet/IP Indicators

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The EtherNet/IP indicators show the state of the EtherNet/IP port and communications activity.

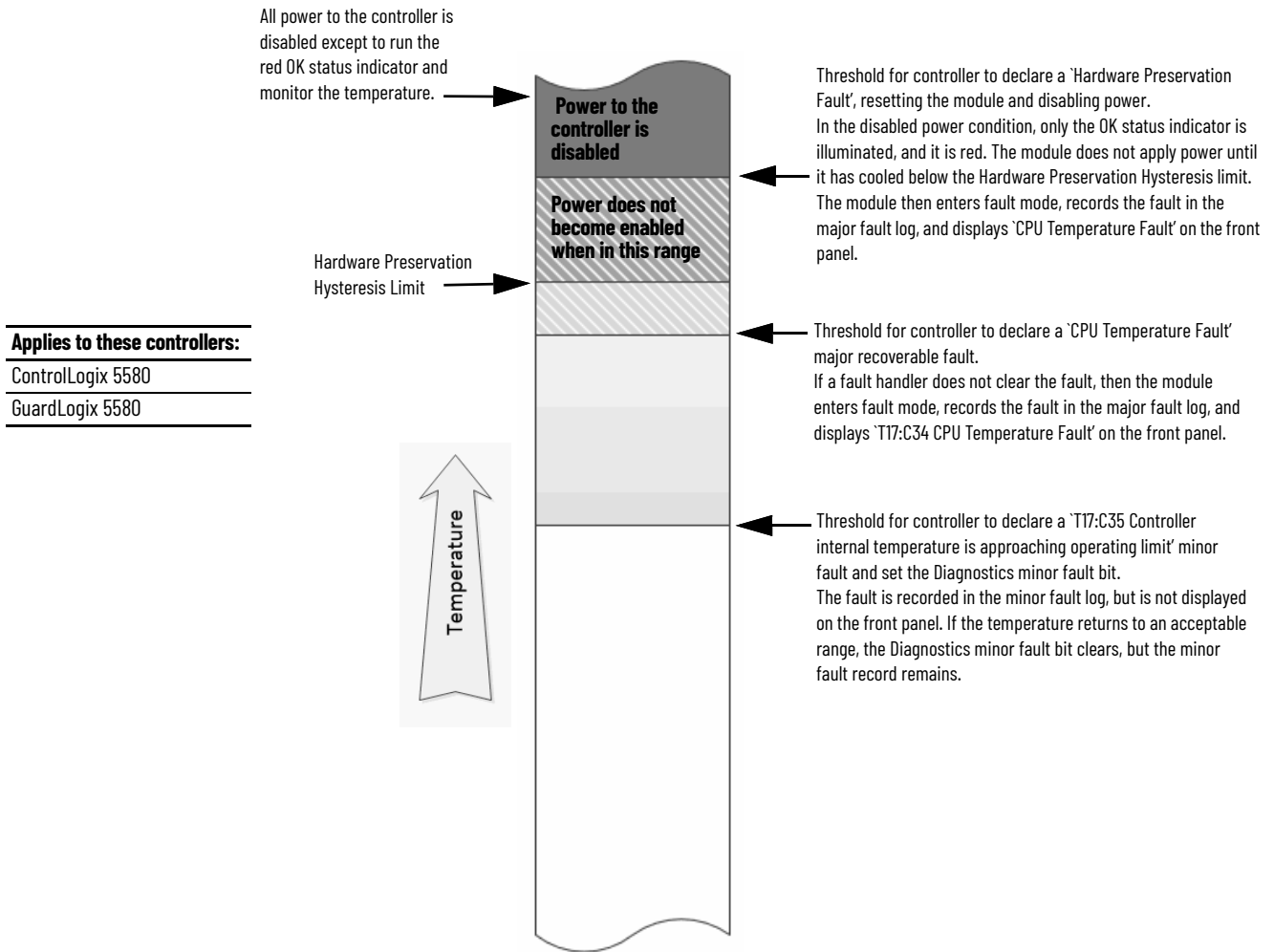
Table 54 - EtherNet/IP Indicators

Indicator	State	Description
NET	Off	<ul style="list-style-type: none"> The controller is not configured, or does not have an IP address. The port is administratively disabled.
	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: <ul style="list-style-type: none"> 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.
	Flashing green	Activity exists on the port.

Thermal Monitoring and Thermal Fault Behavior

The controllers can monitor internal module temperatures, and take actions as the temperature increases, as in this graphic.

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 Controllers Technical Data, publication [1756-TD001](#).



IMPORTANT The presence of any temperature warning indicates that measures need be taken 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 be used to 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.

Change Controller Type

Because safety controllers have special requirements and do not support certain standard features, you must understand the behavior of the system when changing the controller type from standard to safety or from safety to standard in your controller project.

Changing controller type 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

Change from a Standard to a Safety Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Upon confirmation of a change from a standard controller to a safety controller project, safety components are created to meet the minimum requirements for a safety controller:

- 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 request a change from a standard to a safety controller, the project does not convert and stays with the standard controller.

- Safety components are created (safety task, safety program, and so forth).
- 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 controller features that are not supported by the safety controller, such as redundancy, are removed from the Controller Properties dialog box (if they existed).

Change from a Safety to a Standard Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Upon confirmation of a change from a safety controller project to a standard controller, 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 -unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, 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 controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

Change Safety Controller Types

When you change from one safety controller type to another, class of tags, routines, and programs remain unaltered. Any I/O devices that are no longer compatible with the target controller are deleted.

The representation of the safety partner is updated to appear appropriately for the target controller.

History of Changes

This appendix contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

1756-UM0580-EN-P, February 2023

Change
Updated the controller minimum requirements.

1756-UM058N-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-UM058M-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
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 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 o "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-UM058L-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-UM058K-EN-P, August 2020**Change**

Added ControlLogix NSE, ControlLogix-XT, and ControlLogix Process controllers

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-UM058J-EN-P, October 2019**Change**

Added links to access Controller and I/O fault code information from the Knowledgebase Support Center

1756-UM058I-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-UM058H-EN-P, August 2018**Change**

Updated the ControlLogix and ControlLogix-XT™ Chassis and Slots tabl

1756-UM058G-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 Numbersection

Updated the Set the SNN of a Safety I/O Device section

1756-UM058F-EN-P, February 2018**Change**

Added GuardLogix® 5580 and Safety information

1756-UM058E-EN-P, December 2016**Change**

Updated tables with new maximum number of EtherNet/IP nodes supported in Version 30 or later

Added the 1756-IF16IH module to the list of supported HART devices

1756-UM058D-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-UM058C-EN-P, November 2015**Change**

Updated the diagram for multiple controllers in one chassis

Notes:

Numerics

10/100/1000 27
1756-CN2
 uses 42
1756-CN2R
 uses 42
1756-CN2RXT
 uses 42
1756-CNB
 uses 42
1756-CNBR
 uses 42
1756-DHRIO 43
 communication via 44
 uses
 remote I/O 45
1756-DHRIOXT
 uses 43, 45
1756-DNB
 uses 43
1756-EN2F
 uses 39
1756-EN2T
 uses 39
1756-EN2TR
 uses 39
1756-EN2TRXT
 uses 39
1756-EN2TSC
 uses 39
1756-EN2TXT
 uses 39
1756-EN3TR
 uses 39
1756-ENBT
 uses 39
1756-EWEB
 uses 39
1756-IF8H
 uses 48
1756-N2 98
1756-N2XT 98
1756-RIO
 uses 45
1784-SD1
 load from 82
1784-SD2
 load from 82
1788-CN2DN
 uses 43
1788-CN2FFR
 uses 47
1788-EN2DNR
 uses 43
1788-EN2FFR
 uses 47

A

add
 local I/O 99
 remote I/O 103, 105
Add-On Instructions 22, 208
 in project 137
allow communication 87
API 91
application
 elements 129
 networks and 35
audit value 157
AutoFlash
 update 32
automatic diagnostics 181
axes
 consumed 177
 virtual 177
axis
 obtain information 179

B

behavior
 thermal fault 206
block communication 87

C

cache
 message options 90
 messages
 about 89
changing controllers 208
chassis
 ControlLogix
 list 98
CIP Safety 26, 128
CIP Safety I/O
 adding 113
 node address 113
CIP Security ports
 disable 162
communication
 allow 87
 block 87
 Data Highway Plus 43, 44
 Foundation Fieldbus 47
 HART 48
 network options 20, 21
 path
 set 59
 universal remote I/O 45
configuration owner 121
 resetting 121, 122
configuration signature
 components 120
 copy 120
configure
 motion 177

configure change detection 156

audit value 157

configure trusted slot 151

restrict communication 151

select slots 152

connection

DeviceNet

network 43

EtherNet/IP 85

message, required 89

scheduled

ControlNet 89

unscheduled

ControlNet 89

consume

data 88

continuous task 131**control data** 87**controller security** 146**ControlFLASH Plus software** 31, 62**ControlFLASH software** 31, 62**controller**

available modes 71

behavior 87

change type 207

communication path

set 59

ControlLogix 5580

communication options 20, 21

design system with 19

firmware 30

obtain 31

go online 59

match 61

monitor

connections 140

operation mode

change with keyswitch 72

change with Logix Designer 73

program 133

routine 135

serial number 61

serial number mismatch 63, 67

status indicators 203

tags 136

tasks 130

upload a project 68

controller log 158**controller web pages** 193

disable 172

ControlLogix

chassis

list 98

design system 19

I/O

remote 102

selection 97

remote I/O

local 98

slot filler 98

ControlLogix 5580 process controller 12**ControlLogix No Stored Energy (NSE)**

Controllers 12

ControlLogix Redundant Controllers 13**ControlLogix system**

minimum requirements 11

ControlLogix-XT

chassis

list 98

ControlNet

example 41

module 41

network 40

scheduled connection

scheduled connection 89

unscheduled connection

unscheduled connection 89

create a fault routine 152**D****Data Highway Plus** 43**data-only connection** 121**design**

system 19

develop

applications 129

motion applications 177

DeviceNet

connection use 43

network 42

DH+ 43**diagnostic coverage** 26**diagnostics**

with Logix Designer 182

port configuration category 187

time sync category 189

with RSLinx software 191

disable the 4-character status display 167**disable the CIP Security ports** 162**disable the controller web pages** 172**disable the Ethernet port** 76, 159

on port configuration tab 159

with a MSG instruction 160

disable the SD card 166**disable the USB port** 165**DNS addressing** 29**double data rate (DDR)** 39**download**

effect of controller match 61

effect of firmware revision match 62

effect of safety status 62

duplicate IP address

detection 28

resolution 28

E**electronic keying**

about 97

elements

control application 129

safety signature 24

enable license-based protection 154**Ethernet** 27**Ethernet port**

diagnostics

Logix Designer 187

disable 76, 159

EtherNet/IP

- connections 85
- link speeds 36
- network 36
- nodes 85

EtherNet/IP network

- integrated motion 20, 21
- network communication rates 36
- number of nodes supported 21
- optimize network performance 36

event task 131**F****fault**

- cpu temperature 206
- hardware preservation 206
- recoverable 206

fault code

- use GSV to get 141

fault messages 202

- I/O 203

features 20

- controller
 - communication 20
- programming 20

filler slot

- slot filler 98

firmware

- controller 30
- obtain 31
- required 31
- update with AutoFlash, use 32

firmware revision

- match 62
- mismatch 63, 67

firmware upgrade kit 62**FORCE indicator** 203**Foundation Fieldbus** 47**G****general status messages** 200**GSV**

- fault code 141
- monitor
 - connection 141

H**handshake** 87**HART. See Highway Addressable Remote Transducer.****Highway Addressable Remote Transducer** 48**I****I/O**

- ControlLogix
 - remote 102
 - selection 97
- determine data update 109
- fault codes 203
- remote 102

I/O configuration

- add
 - local I/O 99
 - remote I/O 103, 105
 - while online 108

indicator 203

- FORCE 203
- OK 204
- SD 204

instruction

- motion 178

integrated motion

- on the EtherNet/IP network 20, 21

integrated STO mode 17, 18**IP addresses**

- duplicate address detection 28
- duplicate address resolution 28

J**jump to the fault routine** 153**K****keyswitch**

- change controller operation mode 72
- position 71

L**license-based source and execution protection**

- 153

- enable license-based protection 154

link speeds

- EtherNet/IP 36

load

- from memory card 82

load a project

- on corrupt memory 79
- on power up 79
- user initiated 79

local

- I/O
 - add 99
 - remote I/O 98

Logix Designer

- change controller operation mode 73

Logix Designer application

- Add-On Instructions 137
- program 133
- routine 135
- tags 136
- tasks 130

M**match project to controller** 61**memory card** 78

- load from 82
- other tasks 84

message

- about 89
- cache 90

- determine if 90
- fault 202
- status display 200
- messages**
 - safety status 201
- minimum requirements** 11
- Monitor Safety I/O Device Status** 122
- motion**
 - about 177
 - application 177
 - instructions 178
 - program 178
- MVI56-HART**
 - uses 48

N

- network**
 - application and 35
 - controller options 20, 21
 - ControlNet 40
 - Data Highway Plus 44
 - DeviceNet 42
 - DH+. See Data Highway Plus.
 - EtherNet/IP 36
 - Foundation Fieldbus 47
 - HART 48
 - universal remote I/O 45
- network address**
 - DNS addressing 29
- network address translation (NAT)**
 - set the IP address 115
- network communication rates**
 - on an EtherNet/IP network 36
- network status**
 - indicator 125, 126
- no stored energy** 12
- node address** 113
- nodes on an EtherNet/IP network** 85
- nonvolatile memory**
 - tab 77
- NSE controllers** 12

O

- obtain**
 - axis information 179
 - firmware 31
- OK indicator** 204
- online**
 - add
 - to I/O configuration 108
 - go 59
- optimize EtherNet/IP network performance** 36
- out-of-box** 124
 - reset module 121

P

- password**
 - set 51
- path**
 - set
 - communication 59

- Performance Level** 26
- periodic task** 131
- port diagnostics** 187
- primary controller**
 - description 16
- priority**
 - task 132
- probability of failure on demand (PFD)**
 - definition 26
- probability of failure per hour (PFH)**
 - definition 26
- process controllers** 12
- produce**
 - data 88
- produce/consume**
 - data 88
- program**
 - in project 133
 - scheduled 134
 - unscheduled 134
- programming languages** 137
- project**
 - Add-On Instructions 137
 - elements 129
 - go online 59
 - program 133
 - routine 135
 - tags 136
 - tasks 130
 - upload 68
- protect signature in run mode** 52

R

- receive**
 - messages 89
- remote**
 - I/O 102
- remote I/O** 43
 - add 103, 105
 - ControlLogix
 - local 98
 - universal 45
- required**
 - connections
 - messages 89
- reset**
 - module 121
 - ownership 121
- reset button** 74
 - safety partner reset 76
 - stage 1 reset 75
 - stage 2 reset 76
- reset module** 121, 122
- restrict communication**
 - configure trusted slot 151
- RIO. See universal remote I/O**
- routine**
 - in project 135
- RSlinx software**
 - controller diagnostics 191
- RSWho**
 - set
 - path 59

S

safe torque-off

- configurations
 - integrated 17, 18

safety network number

- automatic assignment 54
- copy 56
- definition 26
- description 23, 53
- managing 53
- manual assignment 54
- paste 56
- set 116

safety signature

- about 24
- effect on download 62
- effect on upload 62
- storing a project 78

safety signature elements 24

safety status

- effect on download 62
- view 62

safety tab

- configuration signature 120
- module replacement 123
- view safety status 62

safety-lock

- effect on download 62
- effect on upload 62

scheduled

- program 134

SD card 22

- disable 166

SD indicator 204

secure applications 145

- configure change detection 156
 - audit value 157
- configure trusted slot 151
- controller log 158
- controller security 146
- disable the 4-character status display 167
- disable the CIP Security ports 162
- disable the controller web pages 172
- disable the Ethernet port 159
 - on port configuration tab 159
 - with a MSG instruction 160
- disable the SD card 166
- disable the USB port 165
- license-based source and execution
 - protection 153
 - enable license-based protection 154
- user-definable major faults 152

Secure Digital (SD) card 22, 78

- disable 166
- load from 82
- other tasks 84

secure socket object 91

selection

- I/O 97

send

- messages 89

serial number 61

simple network management protocol 92

slots, Trusted 151

snmp 92

socket interface 91

specifications 9, 19, 206

status

- fault messages 202
- indicators 203
- messages 201
 - display 200
- monitor
 - connections 140

store a project 78

system 20

T

tag

- consume 88
- in project 136
- produce 88

tags

- naming 122

task

- continuous 131
- event 131
- in project 130
- periodic 131
- priority 132

temperature

- limit 206
- warning 206

terminology 26

TLS 91

Trusted slots 151

U

universal remote I/O 45

- communicate via 46

unscheduled

- program 134

update

- determine frequency 109

update firmware

- AutoFlash, use 32

upload

- effect of controller match 61
- effect of safety signature 62
- effect of safety-lock 62
- project 68

USB port

- disable 165

use a fault routine 152

user-definable major faults 152

- create a fault routine 152
- jump to the fault routine 153
- use a fault routine 152

V

view

- safety status 62

W

web pages 193

webpages
 disable 172

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)



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





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

Allen-Bradley, ArmorBlock, ArmorPOINT, Block I/O, Compact 5000, CompactLogix, ControlBus, ControlFLASH, ControlFLASH Plus, ControlLogix, ControlLogix-XT, Data Highway Plus, DH+, DriveLogix, expanding human possibility, FactoryTalk, FLEX I/O, FLEX 5000, Guard I/O, GuardLogix, Kinetix, Logix 5000, On-Machine, PanelConnect, PanelView, PLC-2, PLC-3, PLC-5, POINT I/O, POINT Guard I/O, PowerFlex, QuickView, Rockwell Automation, RSFieldbus, RSLinx, RSNetWorx, RSView, SLC, Stratix, Studio 5000, Studio 5000 Logix Designer, and SynchLink are trademarks of Rockwell Automation.

CIP, CIP Motion, CIP Safety, CIP Security, CIP Sync, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

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, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication 1756-UM543P-EN-P - November 2023

Supersedes Publication 1756-UM543D-EN-P - February 2023

Copyright © 2023 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.