



ControlLogix 5590 Controller User Manual

Bulletin 1756



Allen-Bradley

by ROCKWELL AUTOMATION

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

Important User Information

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

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

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

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

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

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

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

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



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



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

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

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



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



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



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

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



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

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

ControlLogix 5590 Controllers.....	12
Available ControlLogix 5590 Controllers.....	14
ControlLogix 5590 Controller Features.....	15
ControlLogix 5590 High Availability Systems.....	18
ControlLogix 5590 Safety Systems.....	20
Peer-to-peer Safety Communication.....	21
HMI Considerations in Safety Systems.....	22
ControlLogix 5590 Functional Safety.....	24
ControlLogix 5590 Safety Data.....	25
ControlLogix 5590 SIL Requirements.....	27
Safety Application Requirements.....	27
Secure Controller Systems.....	28
Connect to the Controller.....	30
Methods to Set the IP Address.....	30
Duplicate IP Address Detection.....	31
DNS Addressing.....	32
Controller Firmware and Logix Designer Application Compatibility.....	32
Obtain Controller Firmware.....	33
Use ControlFLASH Plus Software to Update Firmware.....	33
Use AutoFlash to Update Firmware.....	34
Firmware Upgrade Guidelines for Safety Controllers.....	36
EtherNet/IP Network.....	38
Nodes on an EtherNet/IP Network.....	38
Star Topology.....	40
Linear Topology.....	41
Device Level Ring Topology.....	42
EtherNet/IP Network Communication.....	43
EtherNet/IP Modes.....	46
Dual-IP Mode.....	46
Overlapping IP Address Ranges.....	48
Configure Dual-IP Mode in the Logix Designer Application.....	49
Configure Dual-IP Mode in FactoryTalk Linx.....	51
Linear/DLR Mode.....	52
Configure Linear/DLR Mode in the Logix Designer Application.....	54
Configure Linear/DLR Mode in FactoryTalk Linx Software.....	56
Change the EtherNet/IP Mode.....	58

Change the EtherNet/IP Mode in the Logix Designer Application.....	59
Change the EtherNet/IP Mode in FactoryTalk Linx Software.....	60
DNS Requests.....	62
SMTP Server.....	63
Socket Object in Dual-IP Mode.....	63
Message Instructions By Ethernet Port.....	63
Create a Controller Project.....	64
Safety Project Configuration.....	65
Set the Safety Level.....	66
Passwords for Safety-locking and Unlocking.....	67
Protect the Safety Signature in Run Mode.....	67
Automatic Assignment of Time-based Safety Network Number.....	68
Manual Assignment of Safety Network Number.....	69
Copy a Safety Network Number.....	70
Paste a Safety Network Number.....	72
Use the Network Browser to Go Online with the Controller.....	72
Use a Recent Communication Path to Go Online with the Controller.....	73
Considerations for Going Online with the Controller.....	74
Considerations for Going Online with a Safety Project.....	75
Use the Network Browser to Download to the Controller.....	77
Use the Controller Status Menu to Download to the Controller.....	78
Download Considerations for a Safety Project.....	79
Use the Network Browser to Upload from the Controller.....	80
Use the Controller Status Menu to Upload from the Controller.....	81
Considerations for Upload from a Safety Controller.....	81
Controller Operation Modes.....	82
Change the Operation Mode.....	85
Use the Logix Designer Application to Change the Operation Mode.....	85
Use the Memory Card.....	87
Store to the Memory Card.....	88
Load from the Memory Card.....	93
Other Memory Card Tasks.....	95
Manage Controller Communication.....	97
Controller Communication Interaction with Control Data.....	97
Produce and Consume (Interlock) Data.....	98
Send and Receive Messages.....	99
Socket Interface.....	100

Use a CIP Generic MSG to Enable SNMP on the Controller.....	101
Use a CIP Generic MSG to Disable SNMP on the Controller.....	104
Trusted Slots on the Controller.....	106
Manage Controller I/O Connections.....	108
Electronic Keying.....	109
Connect to Local I/O.....	110
Connect to Remote I/O.....	111
Connect to Safety I/O.....	111
Connect to Replacement Safety I/O.....	114
Determine When I/O Data Is Updated.....	117
Develop Standard Applications.....	119
Tasks.....	119
Programs.....	123
Routines.....	124
Parameters and Local Tags.....	125
Programming Languages.....	126
Add-On Instructions.....	127
Extended Properties.....	128
Module Object.....	129
Controller Status.....	130
I/O Connections.....	131
Sample Controller Projects.....	132
Develop Motion Applications.....	134
Program Motion Control.....	134
Obtain Axis Information.....	136
Develop Secure Applications.....	137
Controller Security Features.....	137
Requirements for Identification and Authorization.....	138
Requirements for Use Control.....	139
Requirements for System Integrity.....	140
Requirements for Data Confidentiality.....	141
Requirements for Restricted Data Flow.....	142
Requirements for Timely Response to Events.....	142
Requirements for Resource Availability.....	143
Configure User-definable Major Faults.....	144
Create a Fault Routine.....	144
Configure the Program to Use the Fault Routine.....	144

Jump to the Fault Routine.....	144
CIP Bridging Control.....	145
License-based Source and Execution Protection.....	145
Enable License-based Protection.....	146
Change Detection.....	148
Component Tracking.....	149
Controller Logging.....	150
Controller Ethernet Port.....	150
Disable an Ethernet Port on the Port Configuration Tab.....	151
Disable an Ethernet Port with an MSG Instruction.....	152
Disable CIP Security Ports via FactoryTalk Linx.....	154
Disable CIP Security Ports via a CIP Generic MSG Instruction.....	155
Disable the Controller USB Port.....	157
Disable the Controller Memory Card.....	159
Controller 4-character Status Display.....	161
Disable All Categories of Messages.....	162
Disable Individual Categories of Messages.....	164
Controller Webpage Default Settings.....	165
Disable Controller Webpages via Controller Properties.....	166
Manage Controller Webpages Via CIP Generic MSG Instructions.....	166
Privacy Aspects.....	171
Develop Safety Applications.....	173
Safety Applications.....	173
Controller Data Flow Capabilities.....	176
Safety Task.....	177
Safety Programs.....	179
Safety Routines.....	180
Safety Tags.....	180
Safety Signature Elements.....	182
Produced/Consumed Safety Tags.....	182
Configure the SNN for a Peer Controller Connection.....	183
Produce a Safety Tag.....	189
Consume Safety Tag Data.....	190
Standard Tags in Safety Routines (Tag Mapping).....	193
Create Tag Mapping Pairs.....	194
Custom Tag Initialization During Prescan.....	195
Safety Add-On Instructions.....	198

Generate the Instruction Signature.....	200
Safety Add-On Instruction Qualification Tests.....	200
Create Signature History Entry.....	201
Export and Import the Safety Add-On Instruction.....	201
Qualification and Verification.....	201
Safety Programming Considerations.....	202
Application Development and Testing.....	202
Commissioning Lifecycle.....	203
Specification of the Safety Function.....	204
Create the Project.....	205
Generate the Safety Signature.....	205
Validate the Project.....	207
Confirm the Project.....	208
Lock the Controller.....	209
Restrict Access to Safety-lock and Safety-unlock Functionality.....	210
Download/Upload a Safety Application Program.....	212
Store and Load a Project from a Memory Card.....	212
Force Data.....	213
Inhibit a Device.....	213
Edit a Safety Application.....	214
Functional Safety Reference.....	217
Safety Signature.....	217
Safety Signature Hierarchy.....	217
View Safety Signature Elements.....	218
Safety Signature States.....	220
Archive Safety Signature Reports for Audit.....	221
Signature Authentication.....	222
Settings that Do Not Affect the Safety Signature.....	223
Programmatic Changes to the Safety Application Signature.....	223
CIP Safety Systems and Safety Network Numbers.....	223
Safety Network Numbers (SNNs).....	224
Safety Network Number (SNN) Assignment.....	224
Distinguish between Standard and Safety Components.....	225
Routable CIP Safety System.....	225
Considerations for Assigning SNNs.....	226
How SNNs Get to Safety Devices.....	227
SNN Formats.....	228

Monitor Safety Status and Handle Faults.....	230
System Status.....	230
Safety Status.....	231
Safety Faults.....	232
Fault Routine for Safety Applications.....	234
GSV/SSV Instructions in a Safety Application.....	234
Safety Partner Fault.....	235
Troubleshoot the Controller.....	236
Reset Button.....	236
Stage 1 Reset.....	237
Stage 2 Reset.....	238
Safety Partner Reset.....	238
Automatic Diagnostics.....	239
Considerations for Communication Loss Diagnostics.....	239
Controller Diagnostics with the Logix Designer Application.....	240
Notification in the Tag Monitor.....	241
Enable Major Fault on Controller.....	242
Port Diagnostics.....	243
Advanced Time Sync.....	245
Controller Diagnostics with Linux-based Software.....	248
Controller Webpages.....	249
Status Indicators.....	252
EtherNet/IP Indicators.....	255
General Status Messages.....	256
Safety Status Messages.....	258
Safety Partner Status Messages.....	258
Fault Messages.....	259
Major Fault Messages.....	260
I/O Fault Codes.....	260
Thermal Monitoring and Thermal Fault Behavior.....	260
Access Diagnostic Assembly Tags.....	263
Concurrent Connections Diagnostic Assembly.....	265
Ethernet Port Diagnostics Assembly.....	266
Home Webpage Diagnostic Assembly.....	267
Home (Safety) Diagnostic Assembly.....	268
Module Diagnostics Diagnostic Assembly.....	268
OPC UA Diagnostic Assembly.....	269

PTP Diagnostic Assembly.....	269
Faults Diagnostic Assembly.....	270
ControlLogix Backplane Statistics.....	272
Standard Network Diagnostic Assemblies.....	274
Structures for the Standard Network Diagnostics User-defined Data Types.....	275
Main Standard Network Diagnostics Assemblies.....	277
Change Controller Project Type.....	280
Change from a Standard to a Safety Project.....	280
Change from a Safety to a Standard Project.....	280
Safety Application Instructions.....	282
Safety Instructions.....	282
Metal Form Instructions.....	283
Ladder Diagram Safety Instructions.....	284
Drive Safety Instructions.....	292
Safety Reaction Times.....	295
Connection Reaction Time Limit.....	295
System Reaction Time.....	297
Logix System Reaction Time.....	297
Factors That Affect Logix Reaction-time Components.....	299
Configure the Safety Input Module Delay Time.....	300
Configure the Input and Output Safety Connection Reaction Time Limits.....	301
Configure the Safety Task Period and Watchdog.....	302
Access Produced/Consumed Tag Data.....	303
Checklists for Safety Applications.....	305
Checklist for the Controller System.....	305
Checklist for Safety Inputs.....	306
Checklist for Safety Outputs.....	306
Checklist to Develop a Safety Application Program.....	307

Preface

This manual provides information to help you design a system, operate a ControlLogix® 5590-based controller system, and develop standard and safety applications. You must be trained and experienced in the creation, operation, and maintenance of safety systems if utilizing the safety functionality of the controller.

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. Translated versions are not always available for each revision.

Topic	Page
Removed CIP Security considerations that do not apply.	ControlLogix 5590 Controller Features on page 15

Download Firmware, AOP, EDS, and Other Files

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

Additional Resources

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

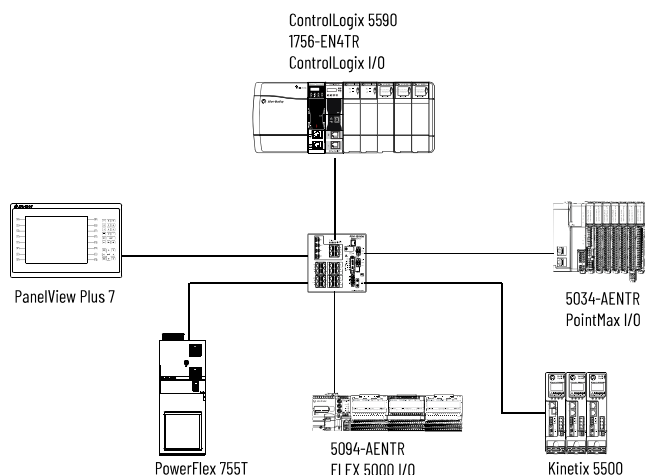
Resource	Description
ControlLogix 5590 Controllers Installation Instructions, 1756-IN900	Provides installation instructions for ControlLogix® 5590 controllers.
1756 ControlLogix Controllers Technical Data, 1756-TD001	Provides specifications for ControlLogix® controllers.
ControlLogix 5590 High Availability Systems User Manual, 1756-UM901	Describes how to set up, configure, program, monitor, and troubleshoot ControlLogix® 5590 redundancy and Logix SIS.
Logix 5000 Controllers Design Considerations Reference Manual, 1756-RM094	Provides information to help design and plan Logix 5000® systems.
Replacement Guidelines: Logix 5000® Controllers Reference Manual, 1756-RM100	Compares ControlLogix® controllers, and provides guidelines on the features, functions, instruction updates, and differences between controllers.
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.
Security Configuration User Manual, SECURE-UM001	Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.
CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001	Describes how to implement the Common Industrial Protocol (CIP™) Security standard in your control system.

Resource	Description
FactoryTalk Security Application Technique, SECURE-AT001	Describes how to use FactoryTalk® Security to implement authentication and authorization in your industrial automation system and enforce product-specific security for Studio 5000 Logix Designer® FactoryTalk® View, and FactoryTalk® AssetCentre
Industrial Automation Wiring and Grounding Guidelines, 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications .	Provides declarations of conformity, certificates, and other certification details.

ControlLogix 5590 Controllers

The ControlLogix® 5590 controller is configurable for standard, safety, redundancy, or Logix SIS (safety instrumented system) applications. The controller is chassis-based, which provides options for configuring various communications and I/O capabilities. The controller supports multiple programming languages that enable sequential, process, motion, and drive control.

Figure 1. ControlLogix 5590 System



Minimum Requirements

The controllers have these minimum requirements:

- ControlLogix® chassis, series C. Series B chassis are supported, but within a derated temperature range.
For more information on chassis usage with ControlLogix® 5590 controllers, see the ControlLogix 5590 Controllers Installation Instructions, publication [1756-IN900](#).
- ControlLogix® power supply.
- Studio 5000 Logix Designer® software, FactoryTalk® Linx communication software, and ControlFLASH Plus® software.

For compatible versions, see the [Product Compatibility and Download Center \(PCDC\)](#).

IMPORTANT: ControlLogix® 5590 controllers require a NEMA 1 or equivalent, windowless, metal enclosure.

Connectors and Status Indicators

Figure 2. Connectors and Status Indicators

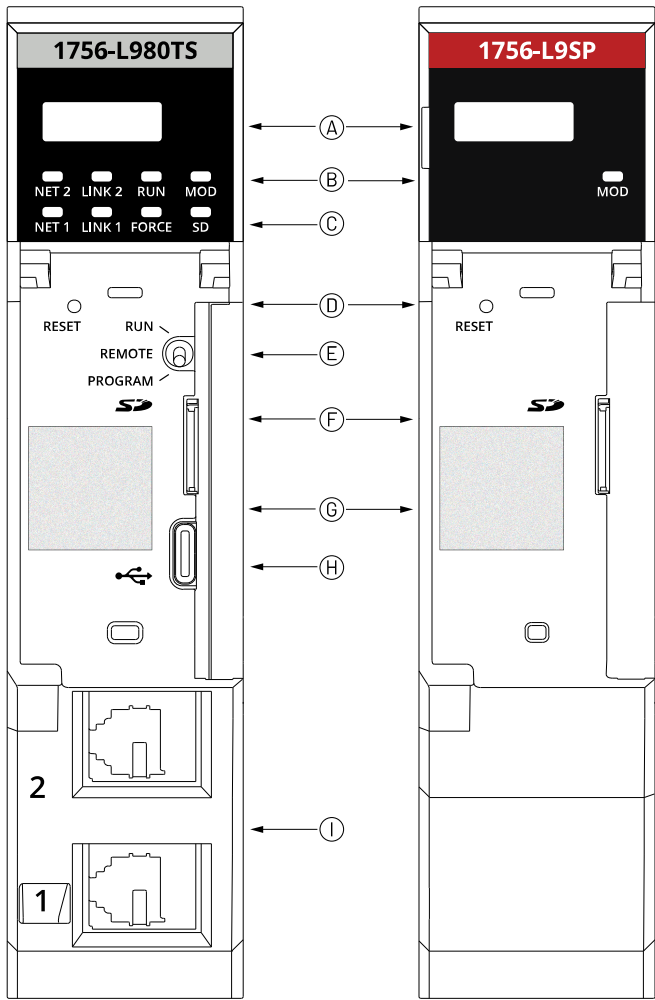


Table 1. Connectors and Status Indicators

Letter	Item	Description
A	4-character display	Scrolls information about the module.
B	Module Status Indicators	Indicates the current state of the module (MOD, RUN, FORCE, SD).
C	Ethernet Status Indicators	Indicates the current state of transmission of data on the EtherNet/IP™ network (LINK, NET).
D	Reset Button	ControlLogix® 5590 controller: Stage 1 reset clears the application program and memory, retains the IP address, and retains all network settings. Stage 2 reset returns the controller to out-of-box settings (including firmware). ControlLogix® 5590 safety partner: Returns the safety partner to out-of-box settings (including firmware).
E	Mode switch (Run, Remote, Program)	3-position toggle switch.

Table 1. Connectors and Status Indicators (continued)

Letter	Item	Description
F	microSD card slot	8 GB microSD™ Card (1784-MSD8, 1784-MSD8XT) included.
G	QR Code	Scan to access product information and support.
H	USB-C Port	Connect a USB-C cable or dongle.
I	Ethernet Ports 1 and 2	Dual, 1 Gb embedded Ethernet ports. Configurable for Dual-IP Addresses or DLR.

QR Code

IMPORTANT: A QR code is laser-etched on to the controllers and safety partners. When you scan the code, you can access product information and support.

- **Verify the QR Code:** Before scanning, check that the QR code is laser-etched directly onto the device. This ensures it is the original and has not been tampered with.
- **Avoid Modified QR Codes:** If you see any labels, stickers, or other materials covering or altering the QR code, do not use it. These modifications could lead to unsafe or incorrect links.
- **Report Suspicious QR Codes:** If you encounter a QR code that looks tampered with, report it to your support team for further investigation.
- **Use Trusted Scanning Apps:** Ensure you use a reliable QR code scanning app to avoid potential security risks.

Available ControlLogix 5590 Controllers

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

IMPORTANT: ControlLogix-XT™ 5590 controllers and ControlLogix-XT™ 5590 Process controllers are rated for extreme environmental conditions only when used properly with other system components that share the same extreme-environment ratings. The extreme-environment ratings of the controllers are nullified when used with other system components that do not share comparable attributes.

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

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



ATTENTION: Conformal Coated Products

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

ControlLogix-XT 5590 Controllers

The ControlLogix-XT™ 5590 controllers function in the same way and have the same features as standard ControlLogix® controllers. You can enable these controllers for safety and redundancy.

The controllers have an extra degree of protection when exposed to harsh, corrosive gas environments. While standard ControlLogix® controllers can withstand temperatures from 0...60 °C (33...140 °F), ControlLogix-XT™ controllers can withstand temperatures from -25...+70 °C (-13...+158 °F) when deployed as part of a ControlLogix-XT™ system.

ControlLogix-XT 5590 Process Controllers

The ControlLogix-XT™ 5590 process controllers focus 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. You can enable these controllers for safety and redundancy.

The controllers have an extra degree of protection when exposed to harsh, corrosive gas environments, and can be used in temperature extremes from -25...+70 °C (-13...+158 °F) when deployed as part of a ControlLogix-XT™ system.

ControlLogix 5590 Controller Features

This table lists the system, communication, and programming features available with ControlLogix® 5590 controllers.

Features	Description
Communication ports	One USB port, Type C 2.0. This USB port does not support powering external devices. Two EtherNet/IP™ ports: 10 Mbps, 100 Mbps, 1 Gbps link speeds
Communication options	EtherNet/IP™ is the preferred network. The controller also supports these networks: • ControlNet® • DeviceNet® • DH+™ • Universal Remote I/O • SynchLink™ • Third-party process and device networks
Controller tasks	• 32 tasks • Safety-enabled controllers have 31 standard tasks, 1 safety task • 1000 programs/task • Event tasks: all event triggers
Integrated motion	• Integrated motion on the EtherNet/IP™ network • Sercos interface • Analog options: - Encoder input - Linear displacement transducer (LDT) input - Serial Synchronous Input (SSI) • For a safety-enabled controller integrated motion is supported in the standard task and integrated safety speed and position monitoring is supported in the safety task.
Programming languages	For standard tasks, the controllers support: • Ladder Diagram (LD) • Structured Text (ST)

Features	Description
	- Function Block Diagram (FBD) - Sequential Function Chart (SFC) For a Safety-enabled controller, the safety task only supports Ladder Diagram.
Integrated safety	A Safety-enabled controller supports: - 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.
Other Features	- Data access control - Firmware Supervisor - Secure Digital (microSD™) card - Safety Connections (Safety-enabled controllers only) - Standard Connections

Controller Memory

The controller can use all of the standard memory for the standard program and all of the safety memory for the safety program at the same time, without affecting either capacity for that controller type. For example, a 1756-L915TS controller has 15 MB of standard memory and 12 MB of safety memory. You can use up to 15 MB for the standard program and up to 12 MB for the safety program at the same time.

Table 2. Controller Memory

Catalog Number	Standard Memory	Safety Memory
1756-L902TS, 1756-L902TSXT	2 MB	2 MB
1756-L905TS, 1756-L905TSXT, 1756-L905TPSXT	5 MB	5 MB
1756-L908TS, 1756-L908TSXT	8 MB	8 MB
1756-L915TS, 1756-L915TSXT, 1756-L915TPSXT	15 MB	12 MB
1756-L925TS, 1756-L925TSXT	25 MB	12 MB
1756-L950TS, 1756-L950TSXT, 1756-L950TPSXT	50 MB	12 MB
1756-L980TS, 1756-L980TSXT, 1756-L980TPSXT	80 MB	12 MB

Controller Capacity

The following table shows the number of EtherNet/IP™ and OPC/UA nodes that are supported for each controller.

Table 3. EtherNet/IP™ and OPC/UA Nodes

Catalog Number	EtherNet/IP™ Nodes	OPC/UA Nodes
1756-L902TS, 1756-L902TSXT	30	300
1756-L905TS, 1756-L905TSXT, 1756-L905TPSXT	100	1000
1756-L908TS, 1756-L908TSXT	200	2000
1756-L915TS, 1756-L915TSXT, 1756-L915TPSXT	300	5000
1756-L925TS, 1756-L925TSXT	400	20,000
1756-L950TS, 1756-L950TSXT, 1756-L950TPSXT	500	50,000
1756-L980TS, 1756-L980TSXT, 1756-L980TPSXT	Recommended maximum: 600	100,000

Features Supported via the Safety Task

In Safety-enabled controllers, the Safety task supports a subset of features that are supported in the standard task as listed in the following table.

Feature	Safety Task	Standard Task
Add-on instructions	✓	✓
Instruction-based alarms and events	—	✓
Tag-based alarms	—	✓
Controller logging	✓	✓
Event tasks (While the safety task cannot be an Event task, standard Event tasks can be triggered with the use of the Event instruction in the safety task.)	—	✓
Integrated motion	✓ Drive Safety Instructions for devices providing safe speed and position feedback.	✓
Analog motion	—	✓
Sercos motion	—	✓
Drive Safety Instructions	✓	—
Language switching	✓	✓
License-based source protection	—	✓
Online import of program components	—	✓

Feature	Safety Task	Standard Task
Online export of program components	✓	✓
Ladder Diagram (LD)	✓	✓
Structured Text (ST)	–	✓
Function block diagrams (FBD)	–	✓
Sequential function chart (SFC) routines	–	✓

IMPORTANT: Safety Consideration

ControlLogix® 5590 Safety-enabled 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. The Logix Designer application does not allow you to configure multicast connection options.

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

- If the producer in the I/O tree of this controller is a ControlLogix® 5590 Safety-enabled controller, GuardLogix® 5580 controller, 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.
- ControlLogix® 5590 Safety-enabled controllers do not produce safety tags to GuardLogix® 5570 (firmware revision 30 or earlier) controllers in the same chassis, because ControlLogix® 5590 Safety-enabled 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.

ControlLogix 5590 High Availability Systems

Availability is the percentage of time that a system is functioning and able to perform its mission. High availability is a characteristic of a system that aims to achieve an agreed level of availability for a higher than normal period.

Controller systems can achieve high availability when specific hardware and configuration requirements are met. For general guidelines for high availability systems, including redundant system components, networks, and other hardware and software considerations, see the High Availability Systems Reference Manual, [HIGHAV-RM002](#).

The following types of controller systems use a redundant chassis pair to achieve high availability:

- ControlLogix® redundancy (safety is not enabled on the controller)
- Logix SIS (safety is enabled on the controller)

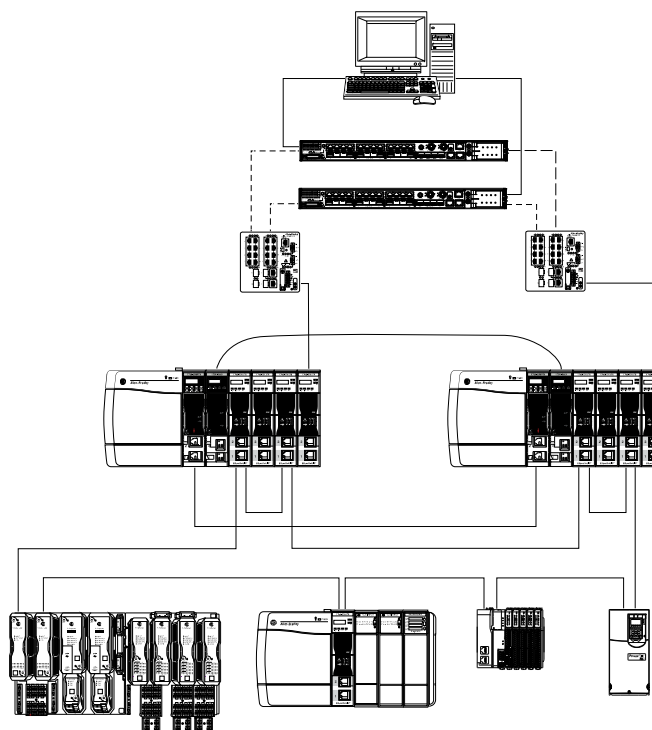
For more information, see the ControlLogix 5590 High Availability Systems User Manual, publication [1756-UM901](#).

ControlLogix Redundancy

ControlLogix® redundancy is designed for non-safety applications that require high availability. When redundant controllers are configured for redundancy, the primary controller executes standard tasks and crossloads standard data to the secondary controller.

The redundant controllers can communicate with only standard I/O modules in a remote chassis via concurrent or non-concurrent communication.

Figure 3. ControlLogix 5590 Redundancy

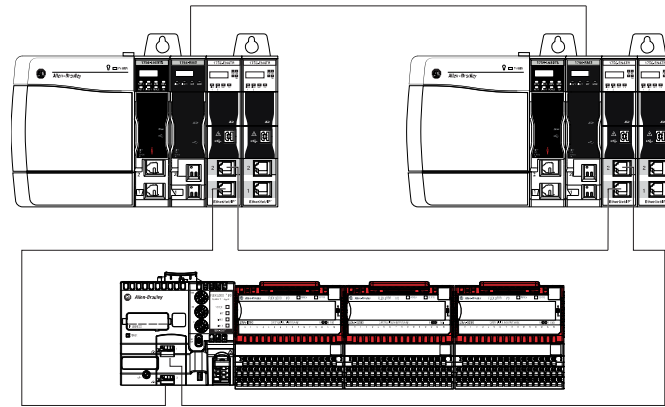


Logix SIS

Logix SIS is designed for safety applications that require high availability. Logix SIS can achieve up to SIL 2 or SIL 3 safety ratings. When redundant controllers are configured for Logix SIS, logic executes as follows:

- Both primary and secondary controllers simultaneously execute the safety task and all safety data remains synchronized.
- Only the primary controller executes standard tasks and crossloads standard data to the secondary controller.

The redundant safety-enabled controllers can communicate with a mix of standard and safety I/O modules in a remote chassis. For safety I/O communication, concurrent communication must be configured between 1756-EN4TR modules in the redundant chassis and the remote safety I/O modules.

Figure 4. ControlLogix 5590 Logix SIS

For information on Logix SIS, see the ControlLogix 5590 High Availability Systems User Manual, publication [1756-UM901](#).

ControlLogix 5590 Safety Systems

You can enable all ControlLogix® 5590 controllers for safety. A safety-enabled controller can support up to SIL 3 and PLe safety applications.

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

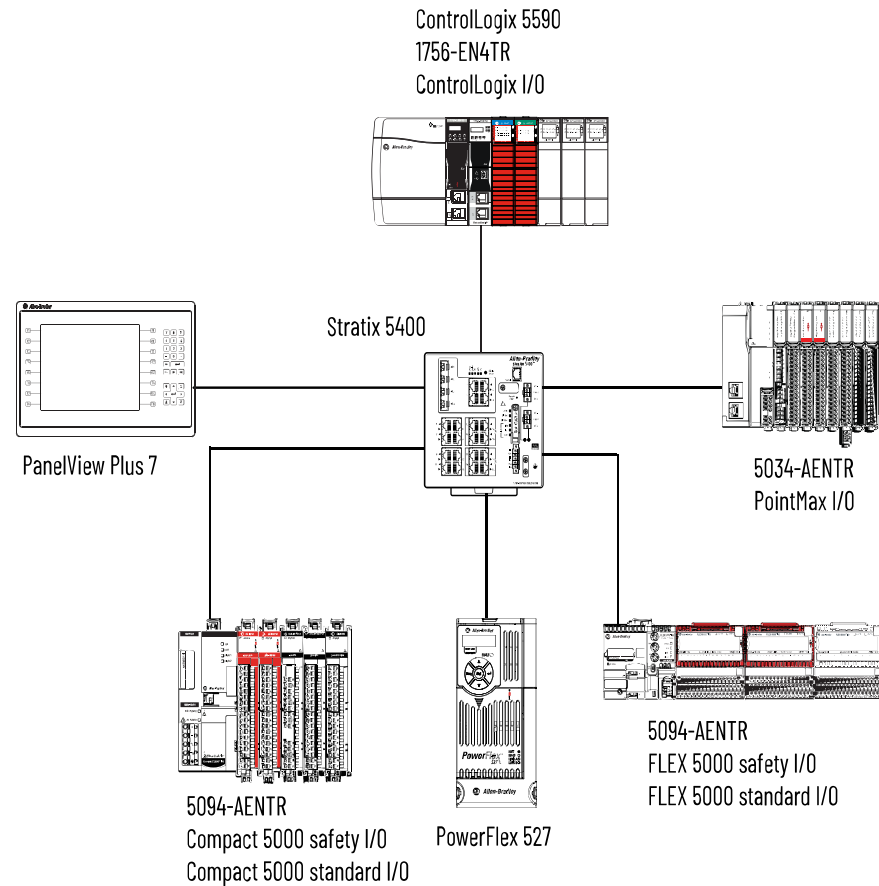
A controller that is enabled for safety can communicate with safety I/O devices via CIP Safety™ over an EtherNet/IP™ network (safety I/O modules, integrated safety drives, integrated safety components). You can interface to local standard and safety I/O in the backplane while your interface with remote safety I/O through the Ethernet ports.

For standard tasks, a safety-enabled controller supports:

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

For the safety task, safety-enabled controllers support Ladder Diagram only.

Figure 5. ControlLogix 5590 Safety System

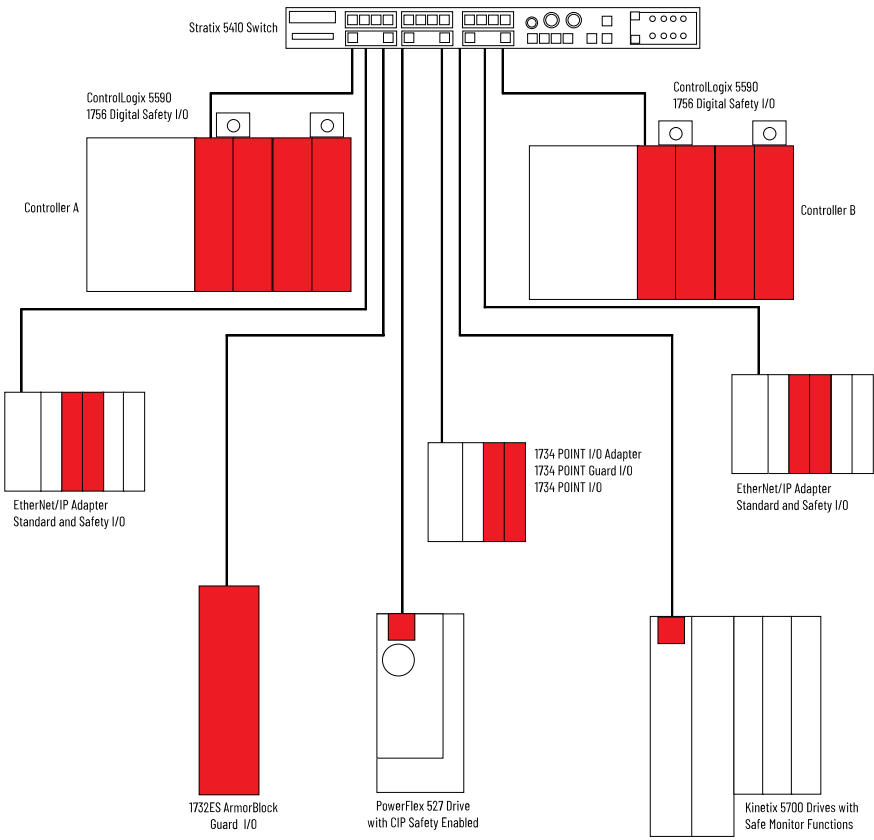


Peer-to-peer Safety Communication

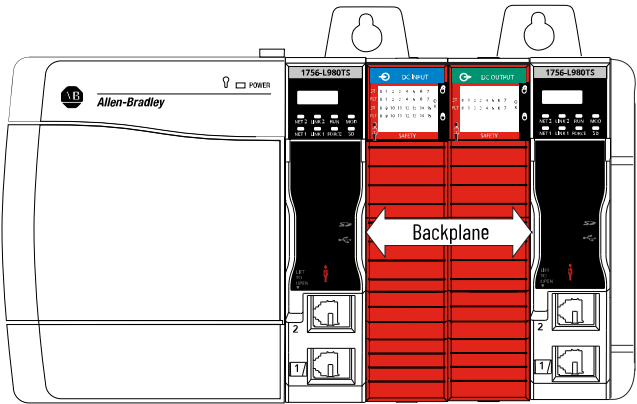
Peer-to-peer safety communication between safety-enabled controllers is possible via the EtherNet/IP™ network or across the ControlLogix® backplane. The controllers can control and exchange safety data with safety I/O devices on an EtherNet/IP™ network, via the onboard Ethernet ports or EtherNet/IP™ bridges.

IMPORTANT: A remote GuardLogix® or Compact GuardLogix® controller that has firmware earlier than revision 28 cannot consume data from a GuardLogix® 5580 or Compact GuardLogix® 5380 controller. Older consumer controllers must be updated to at least to firmware revision 28, or use a dedicated, separate EtherNet/IP™ module in the same chassis as the GuardLogix® 5580 controller, making a connection for produced/ consumed tags that bridges through the Logix backplane. See Knowledgebase Article [Safety Tags produced by a GuardLogix 5580 controller consumed by an older GuardLogix 5570 controllers](#).

Figure 6. Peer-to-peer Communication via the EtherNet/IP Network



Peer-to-peer safety communication between two safety-enabled controllers or I/O modules in the same chassis is also possible via the backplane.



HMI Considerations in Safety Systems

Follow these precautions and guidelines for HMI devices in SIL-rated safety systems.

Precautions

You must exercise precautions and implement specific techniques on HMI devices. These precautions include, but are not restricted to the following:

- Limited access and security
- Specifications, testing, and validation

- Restrictions on data and access
- Limits on data and parameters

Use sound techniques in the application software within the HMI and controller.

Access to Safety-related Systems

HMI-related functions consist of two primary activities: reading and writing data.

Reading data is unrestricted because reading doesn't affect the behavior of the safety system. However, the number, frequency, and size of the data being read can affect controller availability. To avoid safety-related spurious trips, use good communication practices to limit the impact of communication processing on the controller. Do not set read rates to the fastest rate possible.

When writing data, or changing parameters of a safety function, the objective is to minimize error and deviation from the design specification. Different methods of data checking measures can be applied to set safety-related parameters and can include, but are not limited to, the following considerations:

- Only authorized, specially trained operators can write data in safety-related systems via an HMI.
- The operator that writes data in a safety-related system via an HMI is responsible for the effect of those changes in the safety loop.
- You must clearly document the variables that are to be written.
- You must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI.
- Writing data can be accepted in a safety-related system only if the following sequence of events occurs:
 1. The new value must be sent twice to two different standard tags. Both values must not be changed with one command.
 2. The two standard tags that receive the value from the HMI must be mapped into two safety tags.
 3. Safety-related code that executes in the controller, must check both safety tags for equivalency and make sure that they are within range (boundary checks).
 4. Both new variables must be read back and displayed on the HMI device. The HMI display reads the safety tags that received the mapped tag values from the standard tags.
 5. Trained operators must visually check that both variables are the same and are the correct value.
 6. Trained operators must manually acknowledge that the values are correct on the HMI display that sends a command to the safety logic, which allows the new values to be used in the safety function. In every case, the operator must confirm the validity of the change before they are accepted and applied in the safety loop.
- Test all changes as part of the safety assessment procedure.
- Sufficiently document all safety-related changes that are made via the HMI, including the following:
 - Authorization
 - Impact analysis
 - Execution
 - Test information
 - Revision information
- Process Safety changes to the safety-related system must comply with IEC 61511 requirements.

- Machine safety changes to the safety-related system must comply with IEC 62061 requirements.
- The developer must follow the same sound development techniques and procedures that are used for other application software development, including the verification and test of the operator interface and its access to other parts of the program. In the controller application software, create a table that is accessible by the HMI and limit access to only required data points.
- Similar to the controller program, the HMI software is secured and maintained for SIL-level compliance after the system has been validated and tested.

ControlLogix 5590 Functional Safety

The Safety Integrity Level (SIL) is a discrete level for describing the capability to perform a safety function where SIL 3 has the highest level of safety integrity and SIL 1 has the lowest.

The following table provides the SIL and Performance Level (PL) standards for the controllers:

- The safety-enabled controller performs standard controller functionality and communicates with the safety partner to perform safety-related functions.
- The safety partner works with the safety-enabled controller to perform safety-related functions in a SIL 3 system.

Table 4. Safety Ratings for Safety-enabled Controllers

Controller System	IEC 61508	IEC 62061	IEC 61511	ISO 13849-1
	Type-approved and certified for use in safety applications up to and including:	Suitable for use in safety applications up to and including:	Suitable for use in safety applications up to and including:	Suitable for use in safety applications up to and including:
Safety-enabled controller without a safety partner	SIL 2	SIL CL 2	SIL 1 High demand or continuous SIL 2 Low demand	Performance Level PLd (Cat. 3)
Safety-enabled controller with a safety partner	SIL 3	SIL CL 3	SIL 2 High demand or continuous SIL 3	Performance Level PLe (Cat. 4)
Safety-enabled controller in Logix SIS	SIL 2 SIL 3	SIL CL 2 SIL CL 3	SIL 2 SIL 3	Performance Level PLe (Cat. 3)

In documentation, safety ratings are expressed as follows:

- SIL 2 represents SIL 2, SIL CL 2, SIL 2 Low demand, and PLd
- SIL 3 represents SIL 3, SIL CL 3, and PLe

TÜV Rheinland has approved ControlLogix® 5590 safety-enabled controller systems for use in safety-related applications where the de-energized state is considered to be the safe state.

All I/O examples in this manual are based on achieving de-energization as the safe state for typical machine safety and emergency shutdown (ESD) systems.

IMPORTANT: As the system user, you are responsible for these items:

- The setup, SIL rating, and validation of any sensors or actuators that are connected to the ControlLogix® 5590 safety-enabled controller system.
- Project management and functional test.
- Access control to the safety system, including password handling.
- Programming the application and the device configurations in accordance with the information in this user manual.

When applying functional safety, restrict access to qualified, authorized personnel who are trained and experienced.

Use programming software for ControlLogix® 5590 safety-enabled controllers. Only the safety task, not standard tasks, can be used for safety functions.

ControlLogix 5590 Safety Data

The following examples show probability of a dangerous failure on demand (PFD) and average frequency of a dangerous failure per hour (PFH) values for a ControlLogix® 5590 1oo1 SIL 2 safety system:

The following examples show probability of a dangerous failure on demand (PFD) and average frequency of a dangerous failure per hour (PFH) values for a ControlLogix® 5590 1oo1 SIL 2 safety system or 1oo2 SIL 3 safety system:

- 1oo1 is a single-channel system.
- 1oo2 is a dual-channel system.

Useful Life
The useful life of ControlLogix® 5590 controllers is 20 years.

Safety Data
For safety I/O devices safety data, including PFD and PFH values, see the manuals for those products, as listed in the [Additional Resources on page 10](#).

Product Failure Rates
The data in the following tables applies to mission times up to and including 20 years. Mission time (MT) is the length of time over which the device maintains the stated PFD, PFH, and λ ratings before replacement is required.

A detected failure is a failure that is identified by diagnostic tests, proof tests, operator intervention, or normal operation.

Table 5. Safety Parameters

Attribute	ControlLogix® 5590 Safety-enabled Controller	ControlLogix® 5590 Safety-enabled Controller and Safety Partner
Hardware Fault Tolerance (HFT) The hardware fault tolerance equals n , where $n+1$ faults could cause the loss of the safety function. An HFT of 1 means that 2 faults are required before safety is lost.	0	1

Table 5. Safety Parameters (continued)

Attribute	ControlLogix® 5590 Safety-enabled Controller	ControlLogix® 5590 Safety-enabled Controller and Safety Partner
No Part/ No Effect Detected Failure Rate (λ_{NPED}) [hr]	3.59E-06	6.26E-06
Safe Failure Rate (λ_S) [failures/hr]	7.33E-07	1.47E-06
Dangerous Failure Rate (λ_D) [failures/hr]	7.34E-07	1.47E-06
Dangerous Detected Failure Rate (λ_{DD}) [failures/hr]	7.26E-07	1.45E-06
Dangerous Undetected Failure Rate (λ_{DU}) [failures/hr]	7.67E-09	1.53E-08
Automatic Diagnostic Test Interval (λ_D) [hr]	< Safety Reaction Time (SRT)	< Safety Reaction Time (SRT)
Useful Life [yr]	20	20
Systematic Capability (SC) Systematic capability is defined in IEC 61508-4 as the confidence that the systematic safety integrity meets the requirements of the specified SIL rating.	3	3

NOTE:

- ControlLogix® 5590 safety-enabled controller values are product failure rates to be used when the product is represented as a block in a reliability block diagram (RBD).
- ControlLogix® 5590 safety-enabled controller failure rates are valid for ambient temperatures up to 70 °C (158 °F) and altitudes of up to 2000 m (6561.7 ft). See publications [1756-TD001](#) and [1756-IN900](#).
- The HFT value in the preceding table is the product internal HFT.

Table 6. Safety Calculations

Attribute	ControlLogix® 5590 Safety-enabled Controller	ControlLogix® 5590 Safety-enabled Controllers and Safety Partner
PFD _{ave} (Mission Time 20 yr)	6.72E-04	1.40E-05
PFH	7.67E-09	1.63E-10
STR	5.04E-06	9.18E-06
MTTF _d [yr]	155.60	77.80

Assumptions for safety calculations:

- Component failure rates are constant over the life of the product.
- All detected failures (safe and dangerous) result in the safe state (MRT=0).
- Within the specified useful life (20 years), no proof test is needed.

$$PFD_{ave} = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

$$STR = \lambda_s + \lambda_{DD} + \lambda_{NPED}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTF_d = \frac{1}{\lambda_d}$$

$$PFH = \lambda_{DU}$$

ControlLogix 5590 SIL Requirements

A risk assessment determines whether a safety function requires SIL 2 or SIL 3.

For SIL 2 and SIL 3 requirements in high availability systems, see the ControlLogix 5590 High Availability Systems User Manual, publication [1756-UM901](#).



ATTENTION: The safety signature is required for the controller to operate at a SIL 2 or SIL 3 rating. Controller operation without a safety signature is only suitable during development.

IMPORTANT: High-demand SIL 2 applications that follow the IEC 61511 standard require a Hardware Fault Tolerance of 1 and must use the guidance for SIL 3 requirements throughout this documentation.

High-demand SIL 2 applications that follow the IEC 62061 standard require a Hardware Fault Tolerance of 0 and must use the guidance for SIL 2 requirements throughout this documentation.

SIL 2 Requirements

The following applies to SIL 2 safety functions:

- A safety-enabled ControlLogix® 5590 controller requires only the primary controller.

SIL 3 Requirements

The following applies to SIL 3 safety functions:

- A safety-enabled ControlLogix® 5590 controller requires both the primary controller and the safety partner.

IMPORTANT: The safety task can contain a number of safety functions. For a particular function to be SIL 3, the entire chain of devices and programming from the sensor to the actuator must be SIL 3. Be careful that you do not use a SIL 2 input signal for a safety function that requires SIL 3.

Safety Application Requirements

IEC 61508 requires you to perform various proof tests of the equipment that is used in the system. Proof tests are performed at user-defined times. For example, proof tests can be once a year, once every 15 years, or whatever time frame is appropriate. The controllers have a useful life of 20 years, and no proof test is required. Other components of the system, such as safety I/O devices, sensors, and actuators can have different useful life times.

IMPORTANT: Your specific applications determine the time frame for the proof test interval.

Controller Specifications and Certifications

For specifications and the agency certifications for the products, see the following:

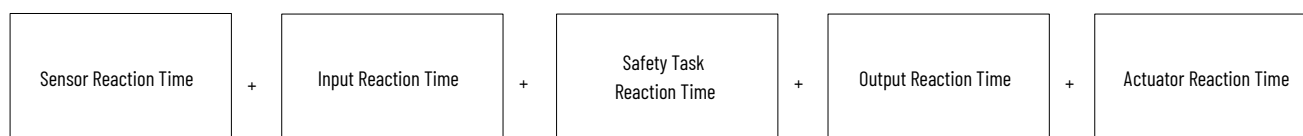
- The Specifications in the Technical Data publication for your product.
- Agency certifications on the product labels
- Declarations of conformity, certificates, and certification details at rok.auto/certifications

System Reaction Time

The system reaction time is the worst-case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safe state.

This worst-case definition includes the effects of asynchronous communications and multiple potential faults within the system. Actual reaction times are typically faster.

Figure 7. System Reaction Time



Each of the reaction times is dependent on factors such as the type of I/O device and instructions that are used in the program.

For more information about reaction time calculations, see [Reaction Times on page 295](#).

Contact Information if Device Failure Occurs

If you experience a failure with any device, contact Rockwell Automation Technical Support: rok.auto/knowledgebase

Your local Rockwell Automation sales office or Allen-Bradley distributor can also initiate the following actions:

- Return the device to us so the failure is logged for the affected catalog number and a record is made of the failure.
- Request a failure analysis to try to determine the cause of the failure.

Secure Controller Systems

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

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

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

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

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

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

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

- Rockwell Automation [Industrial Cybersecurity Solutions](#)
- CIP Security with Rockwell Automation Products Application Technique, publication [SECURE-ATO01](#) (describes the CIP Security™-capable products, minimum software versions and product firmware revisions, and publications that describe how to use the products)

Connect to the Controller

Before you can connect to the controller through the Ethernet or USB port, you must configure the EtherNet/IP™ or USB driver in 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 C receptacle. The port is USB 2.0 compatible and runs at 12 Mbps.
- Install and configure a communication module in the chassis with the controller as described in the installation instructions for the communication module.

The EtherNet/IP™ driver:

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

USB driver:

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

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

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

- The controllers ship without an IP address.
- The controller is DHCP-enabled. That is, the controller is configured to obtain an IP address via a DHCP server.
If there is no DHCP server or the DHCP server is not configured to set the IP address, you must set the IP address manually.

To set the IP address, have the following:

- EtherNet/IP™ or USB drivers that are installed on the programming workstation
- MAC ID from the device, which is on the label on the side of the device
- Recommended IP address for the device

Methods to Set the IP Address

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

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

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

IMPORTANT: The EtherNet/IP™ mode in which the controller operates affects the setting and use of IP addresses on the controller. For example, if the controller operates in Dual-IP mode, you must set an IP address for each controller Ethernet port. That is, you must complete the steps that are described in this section twice—once for each port.

Duplicate IP Address Detection

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

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

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

- Network (NET) status indicator is steady red.
- The 4-character display indicates the conflict.
The display scrolls: <IP_address_of_this_module> Duplicate IP
<Mac_address_of_duplicate_node_detected>
For example: 192.168.1.1 Duplicate IP - 00:00:BC:02:34:B4

Duplicate IP Address Resolution

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

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

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

DNS Addressing

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

IMPORTANT: Safety Considerations

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

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

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

To use DNS addressing, follow these steps.

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

IMPORTANT: Remember the following:

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

Controller Firmware and Logix Designer Application Compatibility

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

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

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

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

In the PCDC:

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

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

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

IMPORTANT: Safety Consideration

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

Obtain Controller Firmware

You can obtain controller firmware in these ways:

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

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

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

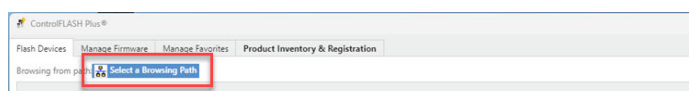
- From the PCDC, download revisions of controller firmware, and download controller firmware, associated files, and product release notes. ControlFLASH Plus® software version 2.00.00 or later provides integration with PCDC for an enhanced experience while you browse for firmware revisions, downloads,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

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

Use ControlFLASH Plus Software to Update Firmware

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

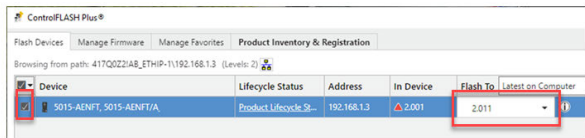
- Click Select a Browsing Path button to set up the browsing path on the network.
- If a path is already established, click Select Browsing from Path.



The network browser shows the devices in your system.

The following steps show how to select devices and firmware.

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



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

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

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

Use AutoFlash to Update Firmware

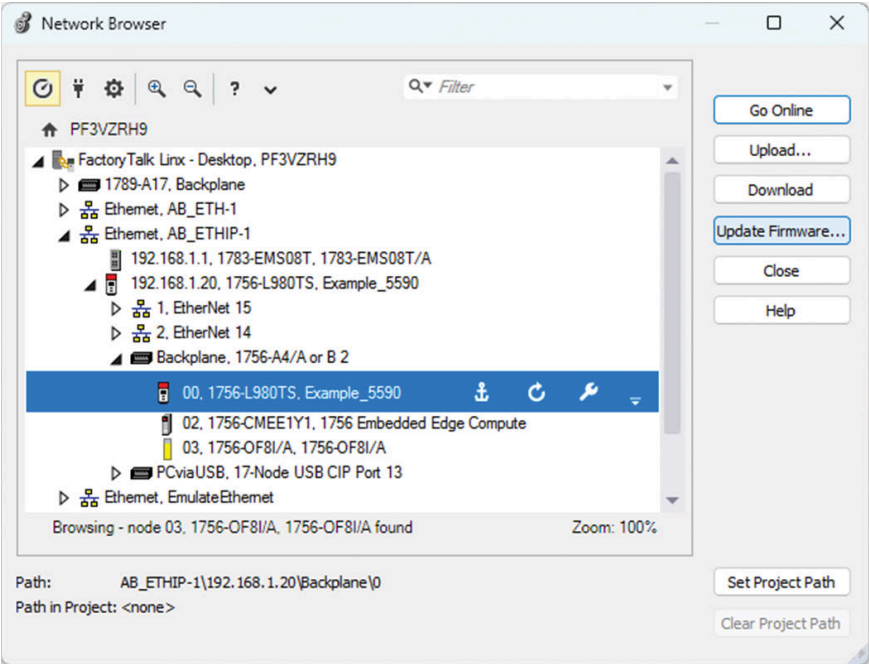
To update your controller firmware with the AutoFlash feature, complete these steps.

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

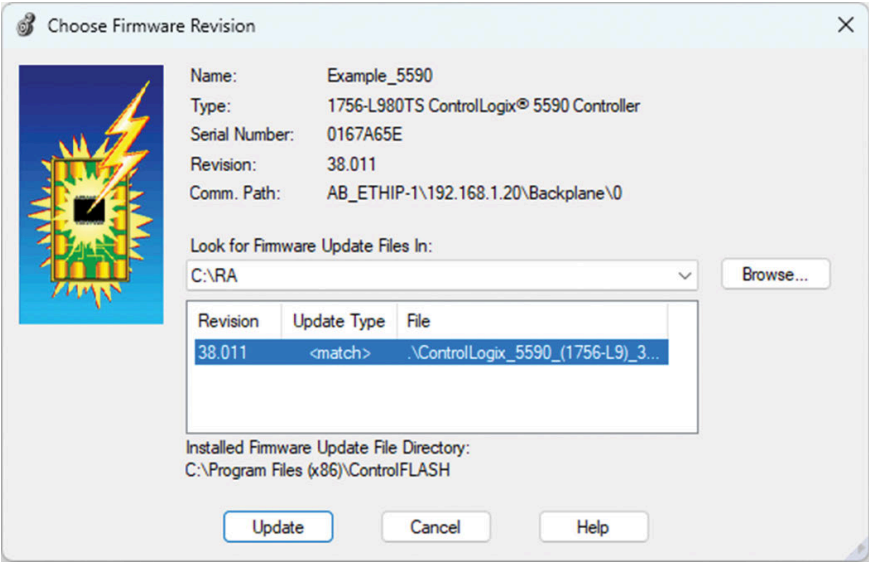
1. Verify that the network connection is made and your network driver is configured in Linux-based communication software.
2. On the Path bar in the programming software, click the Network Browser.



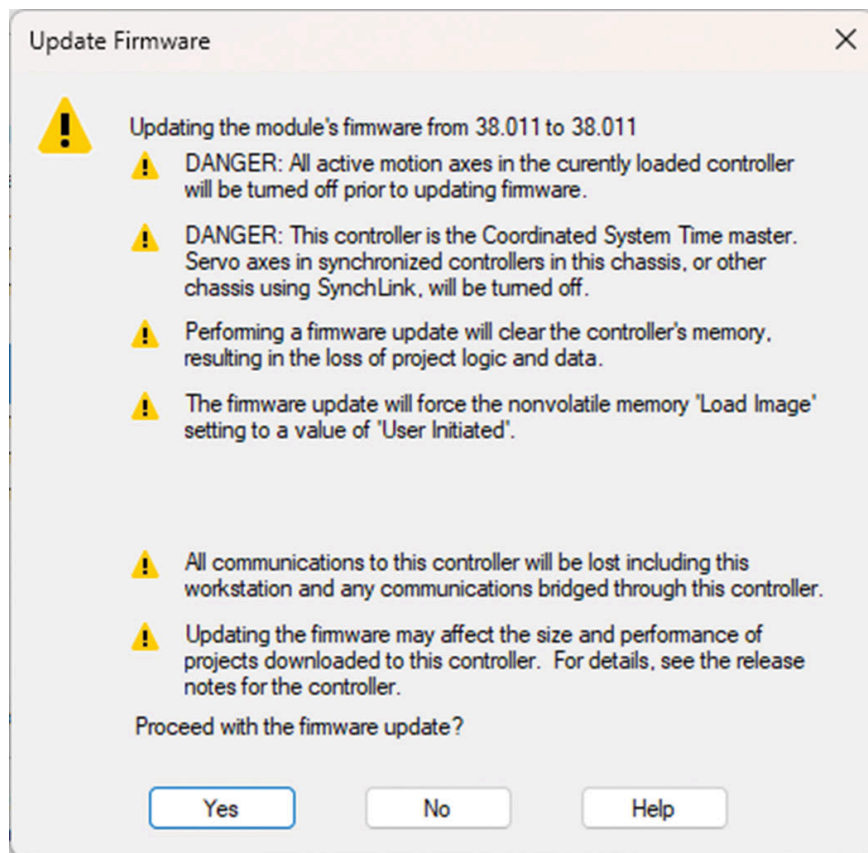
3. On the Network Browser, select your controller under the communication driver you want to use, and click Update Firmware.



4. On the Choose Firmware Revision dialog box, browse to the location of the firmware files.



5. Select the firmware revision and click Update.
6. On the Confirmation dialog box, click Yes.



The firmware update begins.

Allow the firmware update to complete without interruption. When the firmware update is complete, the process dialog box closes.

Firmware Upgrade Guidelines for Safety Controllers

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

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

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

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

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

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

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

For example:

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

EtherNet/IP Network

The controller operates on EtherNet/IP™ networks. Before your controller can operate on an EtherNet/IP™ network, you must first configure the driver in FactoryTalk® Linx software. For information on how to configure EtherNet/IP™ or USB drivers, see the EtherNet/IP Network Devices User Manual, publication [ENET-UM006](#).

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.

The controllers use socket interface transactions and conventional communication over the EtherNet/IP™ network to communicate with Ethernet devices that do not support the EtherNet/IP™ application protocol.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

EtherNet/IP Network Functionality

The controllers support the following:

- Dual built-in EtherNet/IP™ network ports - Port 1 and Port 2
- Support for these EtherNet/IP™ modes:
 - Dual-IP mode (Default)
 - Linear/DLR mode
- Support for these EtherNet/IP™ network topologies:
 - Device Level Ring (DLR)
 - Linear
 - Star
- Support for these EtherNet/IP™ network communication rates:
 - 10 Mbps
 - 100 Mbps
 - 1 Gbps
- Support for only full-duplex operation
- Support for CIP Sync™ technology that is based on Time Synchronization using the IEEE-1588 Precision Time Protocol
- Duplicate IP address detection

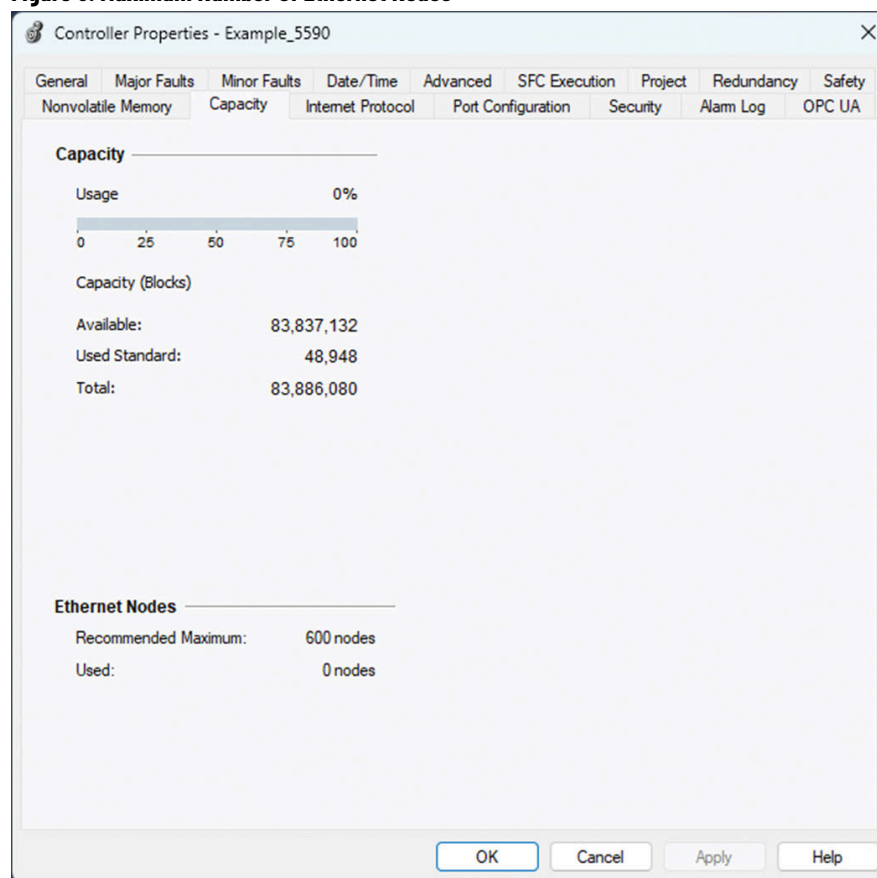


ATTENTION: 10 Mbps Ethernet automatic negotiations are functional, however, they are not fully supported or intended for normal use. Use 10 Mbps Ethernet connections, only if necessary, during temporary setup.

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

Nodes on an EtherNet/IP Network

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.

Figure 8. Maximum Number of Ethernet Nodes

Devices Included in the Node Count

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

- Remote communication adapters
- Remote controllers
- Devices with an embedded EtherNet/IP port
- EtherNet/IP™ devices that are added to the I/O tree under a communication module in the local chassis, even though the communication module in the local chassis does not count as a node
- HMI devices that are added to the I/O tree
- 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 controller, you do not count Ethernet devices that exist on the EtherNet/IP™ network but are not added to the I/O configuration section of the project.

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

- Computer
- Communication modules in the local chassis
- HMIs that are not added to the I/O configuration section

- Devices that are the target of MSG Instructions
 - Standard Ethernet devices with which the controller communicates via a socket interface
- The following example shows five nodes in the I/O tree.

Figure 9. Ethernet Nodes Example

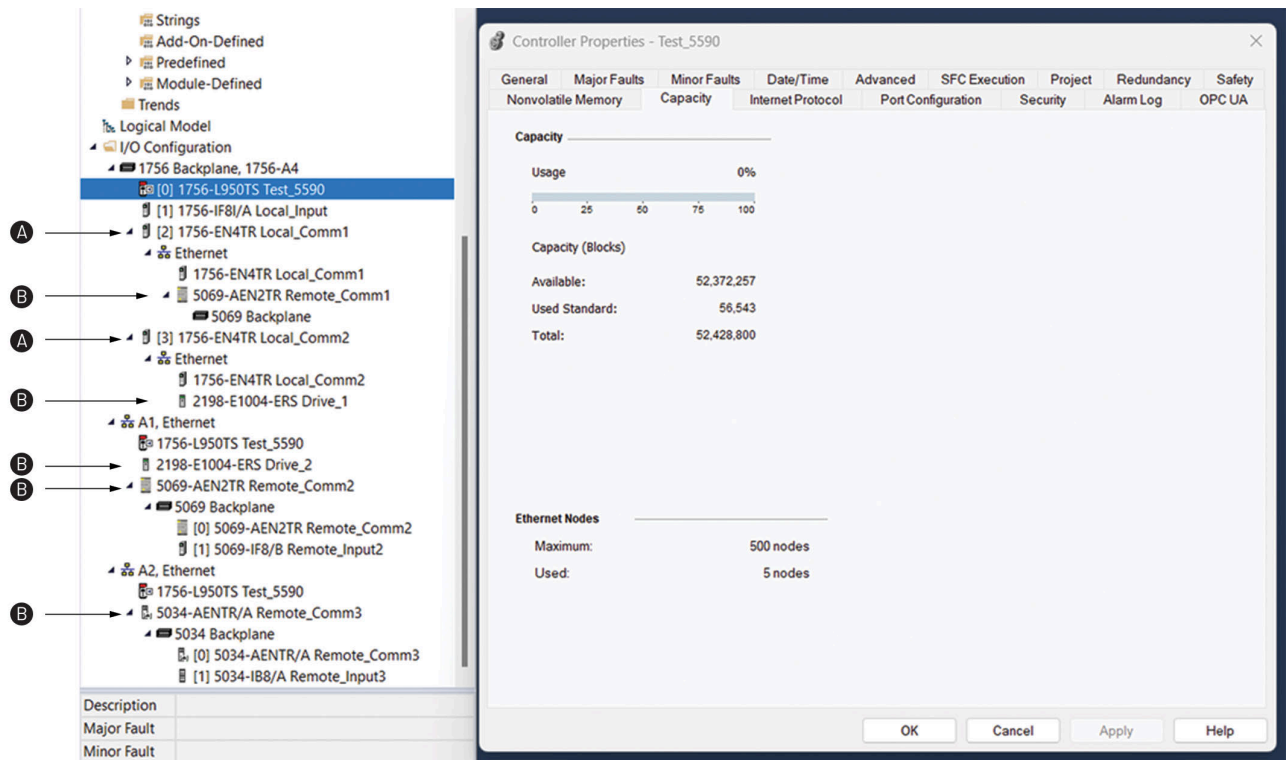


Table 7. Item Description

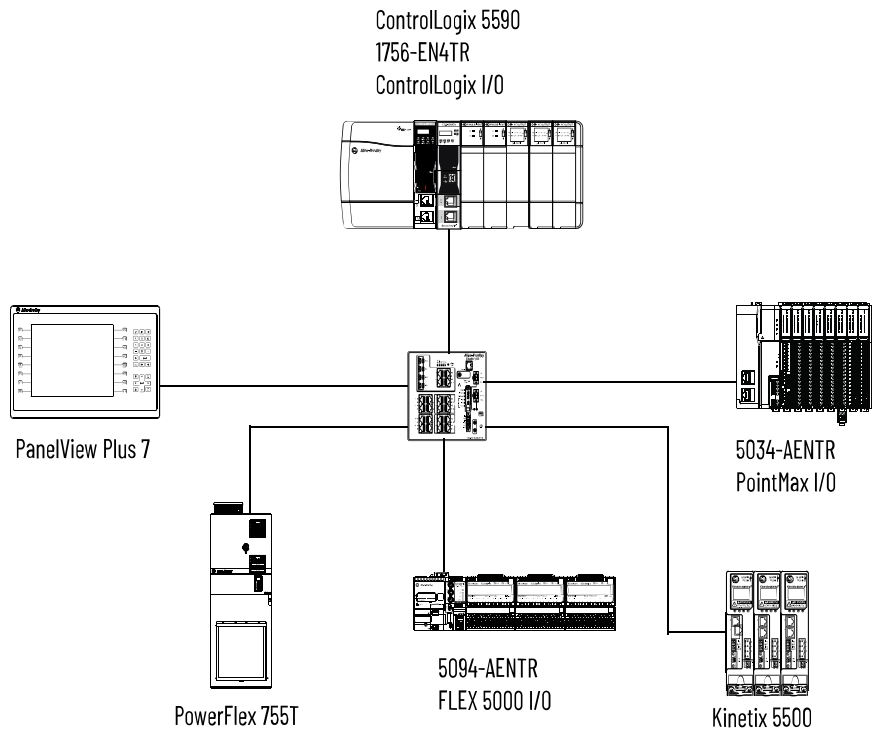
Item	Description
A	Not a node. Module is in the local chassis.
B	Node

Star Topology

A star network topology is a traditional EtherNet/IP™ network that includes multiple devices that are connected to each other via an Ethernet switch. The controller can operate in Linear/DLR or Dual-IP mode when it is connected to a star network topology.

If the controller operates in Dual-IP mode, the Ethernet ports have unique IP configurations and must be connected to different subnets.

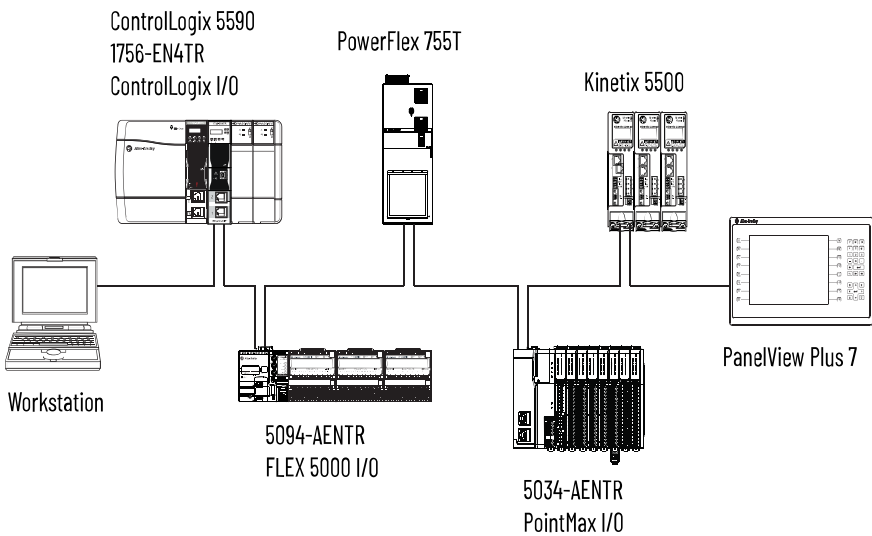
Figure 10. Star Network Topology Example



Linear Topology

A linear network topology is a collection of devices that are daisy chained together across an EtherNet/IP™ network. Devices that can connect to a linear network topology use embedded switch technology to remove any need for a separate switch, as required in star network topologies.

Figure 11. Linear Network Topology Example



Device Level Ring Topology

Device Level Ring (DLR) is an EtherNet/IP™ protocol that is defined by ODVA. DLR provides a means to detect, manage, and recover from a single fault in a ring-based network.

A DLR network includes the following types of ring nodes.

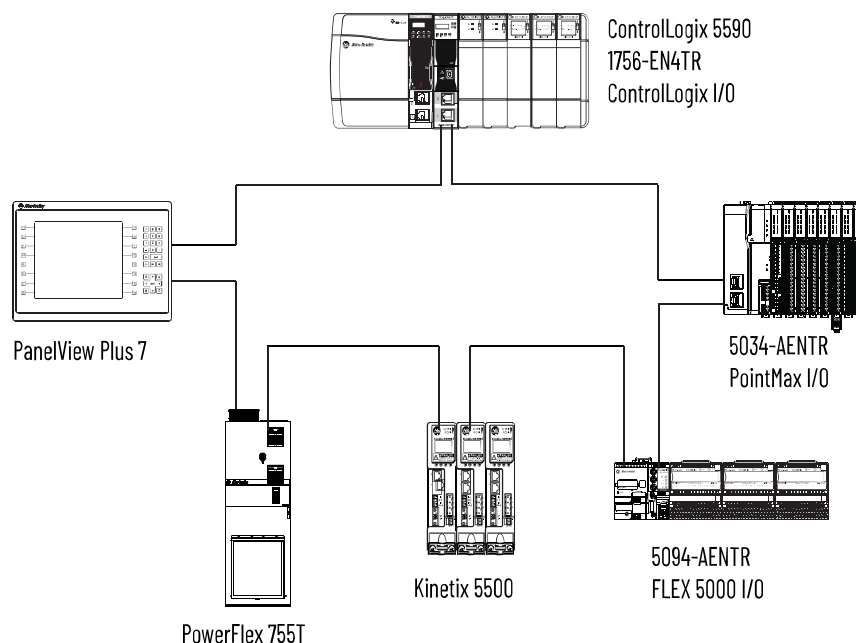
Table 8. DLR Nodes

Node	Description
Ring supervisor	A ring supervisor provides these functions: • Manages traffic on the DLR network • Collects diagnostic information for the network A DLR network requires at least one node to be configured as ring supervisor. By default, the supervisor function is disabled on supervisor-capable devices.
Ring participants	Ring participants provide these functions: • Process data that is transmitted over the network. • Pass on the data to the next node on the network. • Report fault locations to the active ring supervisor. When a fault occurs on the DLR network, ring participants reconfigure themselves and relearn the network topology.
Redundant gateways (optional)	Redundant gateways are multiple switches that connect to a DLR network and also connect together through the rest of the network. Redundant gateways provide DLR network resiliency to the rest of the network.

Depending on their firmware capabilities, both devices and switches can operate as supervisors or ring nodes on a DLR network. Only some devices, such as switches, can operate as redundant gateways.

For more information about DLR, see the EtherNet/IP Device Level Ring Application Technique, publication [ENET-AT007](#).

Figure 12. DLR Network Topology Example



EtherNet/IP Network Communication

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

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

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

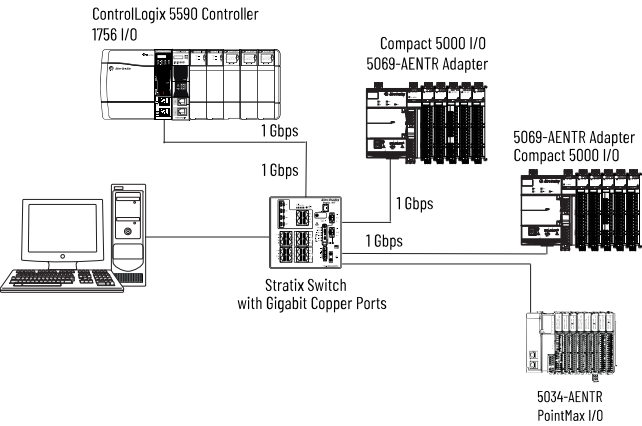
Network performance in the controller system is optimal if the 1 Gbps speed is used. However, legacy Ethernet devices do not support the 1 Gbps speed. Instead, they support a maximum rate of 100 Mbps.

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

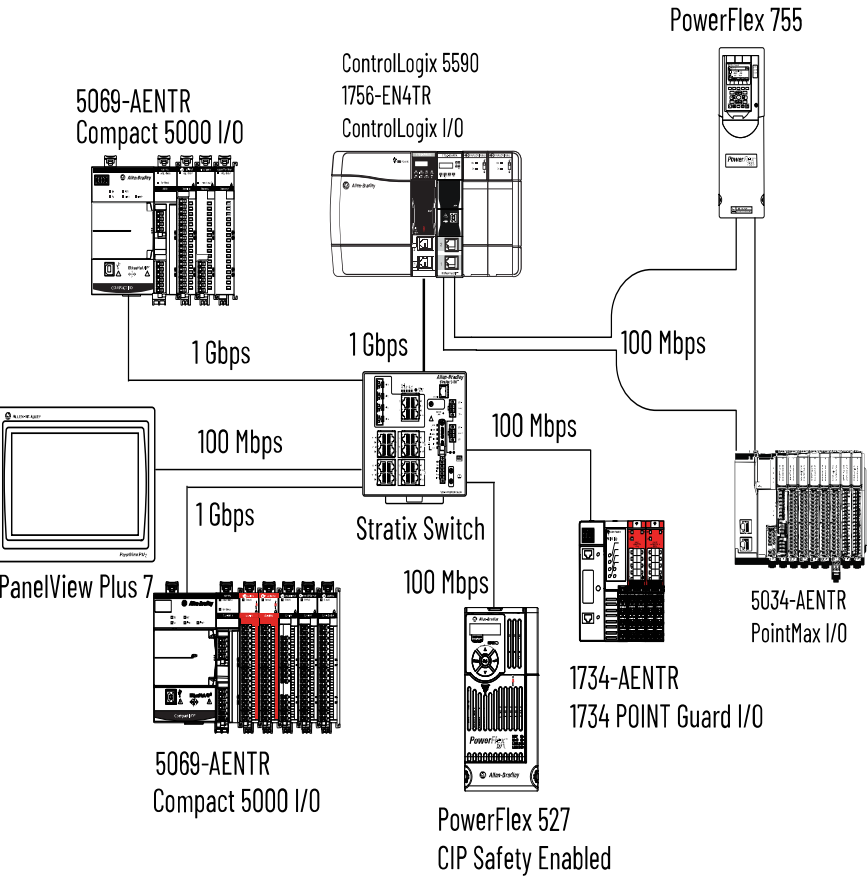
When you design a controller system and consider using the 1 Gbps rate on the controller, remember the following:

- You can use the 1 Gbps speed on the controller port when all network devices support 1 Gbps.

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



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



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

IMPORTANT: To help prevent bursts of traffic and DLR traffic reversal due to a ring break, do not use different speeds on device ports in the same EtherNet/IP™ network without a managed switch.

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

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

EtherNet/IP Modes

Two EtherNet/IP™ modes are available on the controller.

- Dual-IP (Default)
- Linear/DLR

The controller can connect to these EtherNet/IP™ network levels:

- Enterprise-level Network
- Device-level Network

The advantage of connecting to separate network levels is that you can segment the networks and isolate the communication on each. For example, communication that is required for the controller to execute a task is restricted to the device-level network.

Network segmentation and the resulting communication isolation can help provided enhanced security in your application. Additionally, the option to connect to separate network levels helps you organize the networks in your application in a more logical manner.

Enterprise-level Network

Port 1 can only be connected to an enterprise-level network.

IMPORTANT: When you set the IP address and subnet mask, you establish an IP address range for the port. Make sure that the IP address ranges that are established for each port on the controller do not overlap. For more information on overlapping IP address ranges, see [Overlapping IP Address Ranges on page 48](#).

When you connect port 1 to an enterprise-level network, you configure the following parameters:

- IP address (required)
- Subnet mask, also called the network mask (required)
- Gateway address (optional)
- Host name (optional)
- Domain name (optional)
- Primary DNS server address (required if your controller makes DNS requests.)
- Secondary DNS server address (required if your controller makes DNS requests.)

Device-level Network

Remember the following when you connect to device-level networks:

- You are not required to connect the controller to an enterprise-level network to connect to device-level networks.
- You can connect port 1, port 2, or ports 1 and 2 to device-level networks.

When you connect a port to a device-level network, you configure the following parameters:

- IP address (Required)
- Subnet mask, also called the network mask (Required)
- Gateway address (Optional)
- Host name (Optional)

Dual-IP Mode

Out-of-the-box, the EtherNet/IP™ mode is Dual-IP mode.

IMPORTANT: Parallel Redundancy Protocol is not currently supported.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2

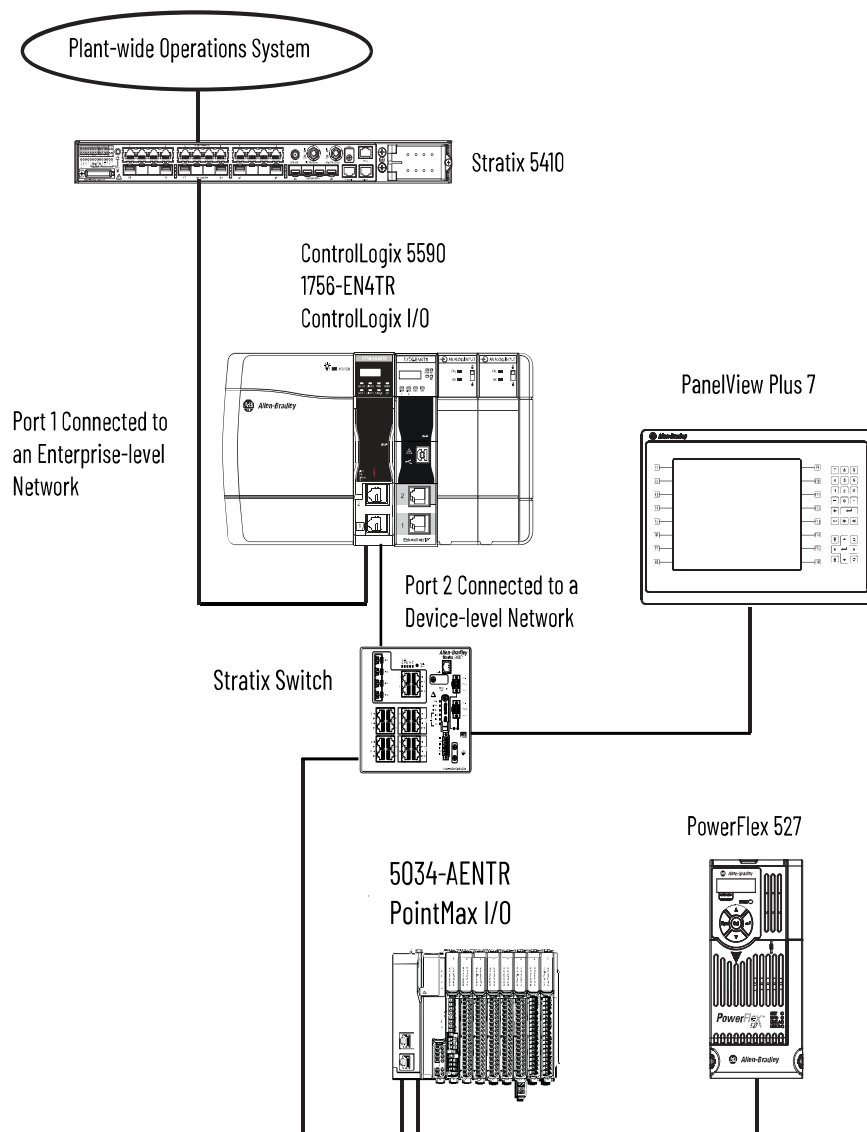
Dual-IP mode lets you connect ports 1 and 2 to separate networks. In this mode, port 1 can connect to an enterprise-level network or a device-level network. Port 2 can only connect to a device-level network.

In this mode, each port requires its own network configuration.

You must avoid overlapping IP address ranges when you configure the Ethernet ports in Dual-IP mode. For more information, see [Overlapping IP Address Ranges on page 48](#).

The following figure shows a controller using Dual-IP mode with connections to an enterprise-level network and a device-level network.

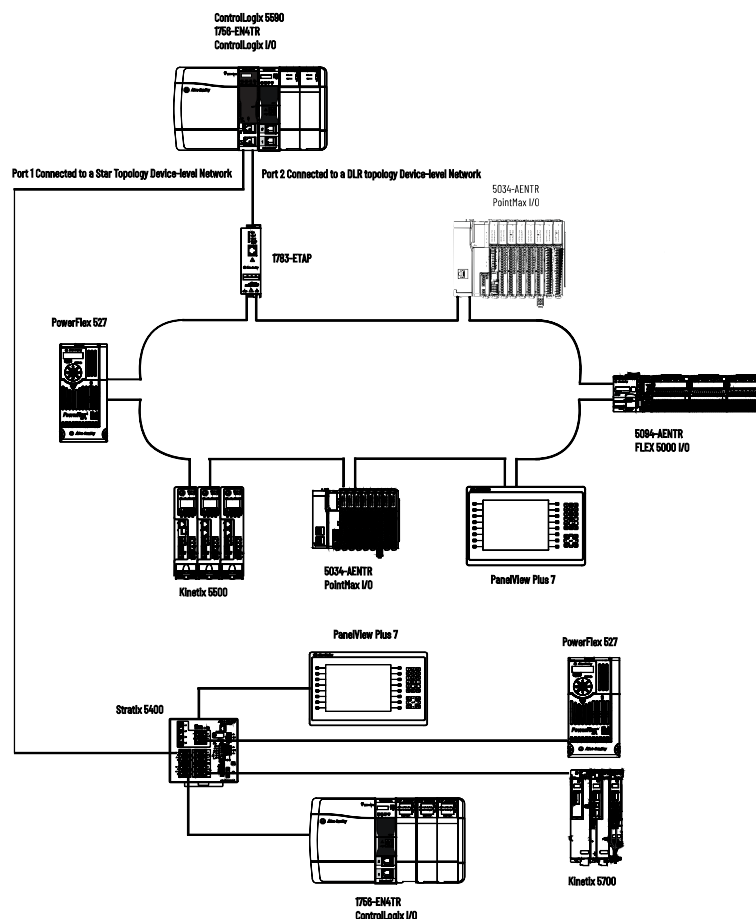
Figure 13. Controller in Dual-IP Mode with Enterprise-level and Device-level Connections



The following figure shows a controller using Dual-IP mode in with connections to separate device-level networks, including a DLR network.

IMPORTANT: If a controller is using Dual-IP mode, it can connect to a DLR network topology through a 1783 Ethernet tap or a Stratix® switch that supports DLR.

Figure 14. Controller in Dual-IP Mode with Device-level Network Connections Only



Controller Functionality Considerations in Dual-IP Mode

Remember the following controller functions when you use Dual-IP mode:

- The controller does not support these functions:
 - TCP routing or switching between the two separate networks.
 - CIP™ bridging of I/O connections (including produce/consume) between the two separate networks
- The controller supports these functions:
 - CIP™ bridging for non-I/O connections such as HMI, messaging, or sockets between the two separate networks.
 - CIP™ bridging for UnconnectedCIP™ messages between the two separate networks.

Overlapping IP Address Ranges

IMPORTANT: Overlapping IP address ranges only applies when the controller operates in Dual-IP mode.

The IP address and subnet mask values that you assign to an Ethernet port establish an IP address range for the port. The subnet mask value is used to establish the network part of the IP address.

Overlapping IP address ranges occurs when any IP address from one range is also present in the other IP address range. When a controller uses Dual-IP mode, the network parts cannot overlap between the Ethernet ports.

The following examples describe conditions in which IP address ranges that overlap or do not overlap.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

The key difference between the port configurations in the examples is the Subnet Mask/ Network Mask value for port 1. In the first example, the value is 255.255.255.0. In the second example, the value 255.255.252.0.

Example - IP Address Ranges That Do Not Overlap

The following table describes port 1 and port 2 configurations that use IP address ranges that do not overlap.

None of the IP addresses in either port's address range exists in the IP address range for the other port.

Port Number	IP Address	Subnet Mask/Network Mask	IP Address Range (Low to High)
1	192.168.1.5	255.255.255.0	192.168.1.1...192.168.1.254
2	192.168.2.1	255.255.255.0	192.168.2.1...192.168.2.254

Example - IP Address Ranges That Do Overlap

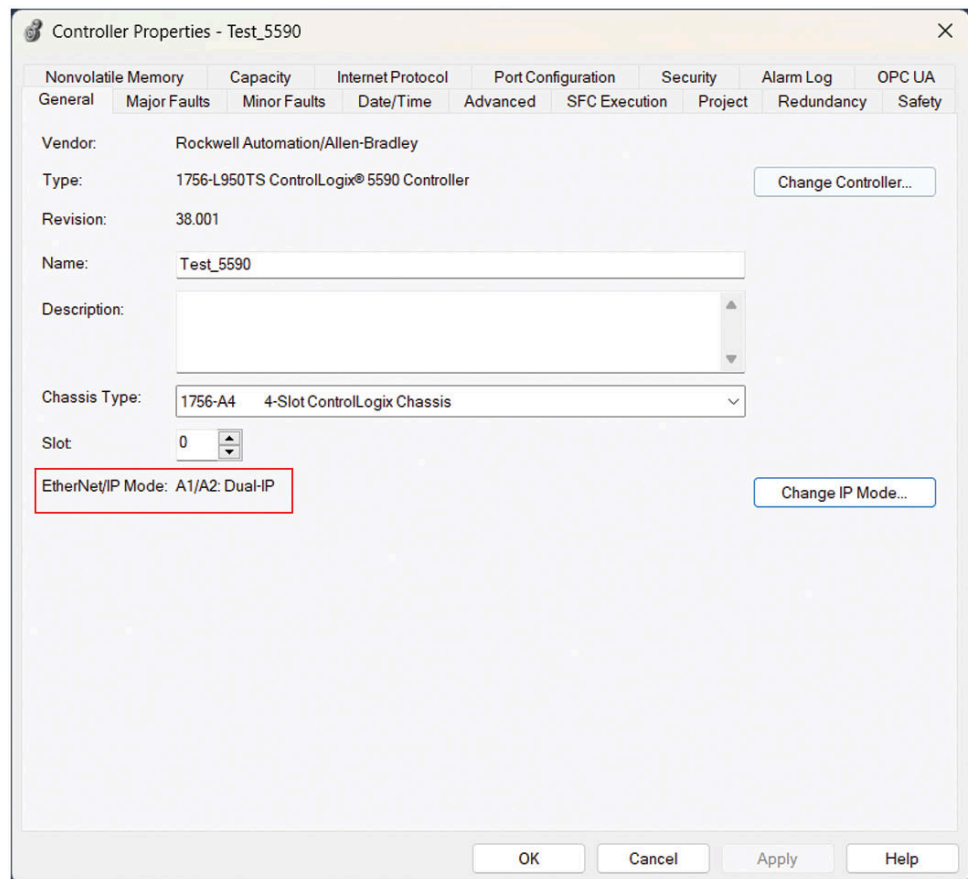
The table describes port 1 and port 2 configurations that use IP address ranges that do overlap. All IP addresses in the port 2 address range are in the port 1 address range.

Port Number	IP Address	Subnet Mask/Network Mask	IP Address Range (Low to High)
1	192.168.1.5	255.255.252.0	192.168.0.1...192.168.3.254
2	192.168.2.1	255.255.255.0	192.168.2.1...192.168.2.254

Configure Dual-IP Mode in the Logix Designer Application

You can configure the controller for Dual-IP mode with the Studio 5000 Logix Designer® application. The EtherNet/IP™ mode is Dual-IP by default and is displayed on the General tab in the Controller Properties dialog box.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.



You set the IP address and subnet mask on the Internet Protocol tab.



When you set the IP address and subnet mask, we recommend that you use a USB connection from the workstation to the controller.

Use this procedure to set the IP address on port 1 and port 2.

1. Confirm that the project is online.
2. Confirm that the controller is in one of the following modes.
 - Program
 - Remote Program
 - Remote Run

You cannot change the IP address or subnet mask if the controller is in Run mode.

3. Click the Internet Protocol tab.
4. From the Port dropdown menu, choose an Ethernet port.
5. Click Manually configure IP settings.
6. Assign the IP address and network mask values.

7. Click Apply.

Controller Properties - Diags_Test_5590

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

Port: A1

☒ Manually configure IP settings
☐ Obtain IP settings automatically using DHCP

IP Address: 10 . 60 . 1 . 1 Subnet Mask: 255 . 255 . 255 . 0
Gateway Address: 0 . 0 . 0 . 0

Domain Name: Primary DNS Server Address: 0 . 0 . 0 . 0
Host Name: Secondary DNS Server Address: 0 . 0 . 0 . 0

OK Cancel Apply Help

Configure Dual-IP Mode in FactoryTalk Linx

You can configure the controller for Dual-IP mode with FactoryTalk® Linx software. You set the IP Address and Network Mask on the Internet Protocol tab.



We recommend that you use a USB connection from the workstation to the controller when you set the IP address and Subnet Mask.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

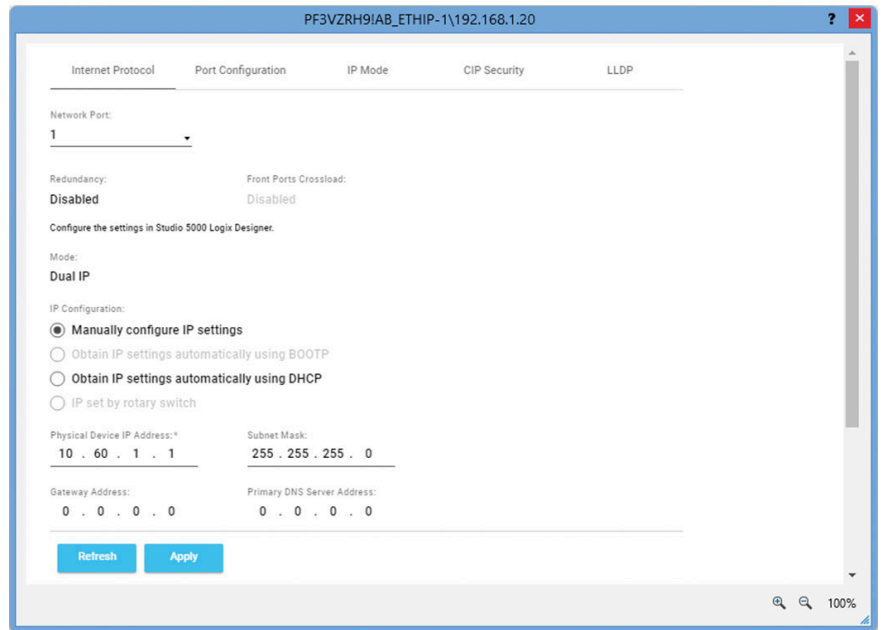
Use this procedure to set the IP address on port 1 and port 2.

1. Confirm that the project is online.
2. Confirm that the controller is in one of the following modes.
 - Program
 - Remote Program
 - Remote Run

You cannot change the IP address or subnet mask if the controller is in Run mode.

3. From the Port pull-down menu, choose an Ethernet port.
4. Choose Manually configure IP settings.
5. Assign IP Address and Network Mask values.

6. Click Apply.



Linear/DLR Mode

When controllers operate in Linear/DLR mode, they can only connect to one network with one network configuration. The two physical ports allow the controller to connect to a linear or Device level Ring (DLR) network topology.

By default, the EtherNet/IP mode is automatically set to Dual-IP mode. You must change the EtherNet/IP Mode to use Linear/DLR mode. For more information on how to change the controller to Linear/DLR mode, see the following:

- [Change the EtherNet/IP Mode in the Logix Designer Application on page 59](#)
- [Change the EtherNet/IP Mode in FactoryTalk Linx Software on page 60](#)

Figure 15. Controller in Linear/DLR Mode on a DLR Network

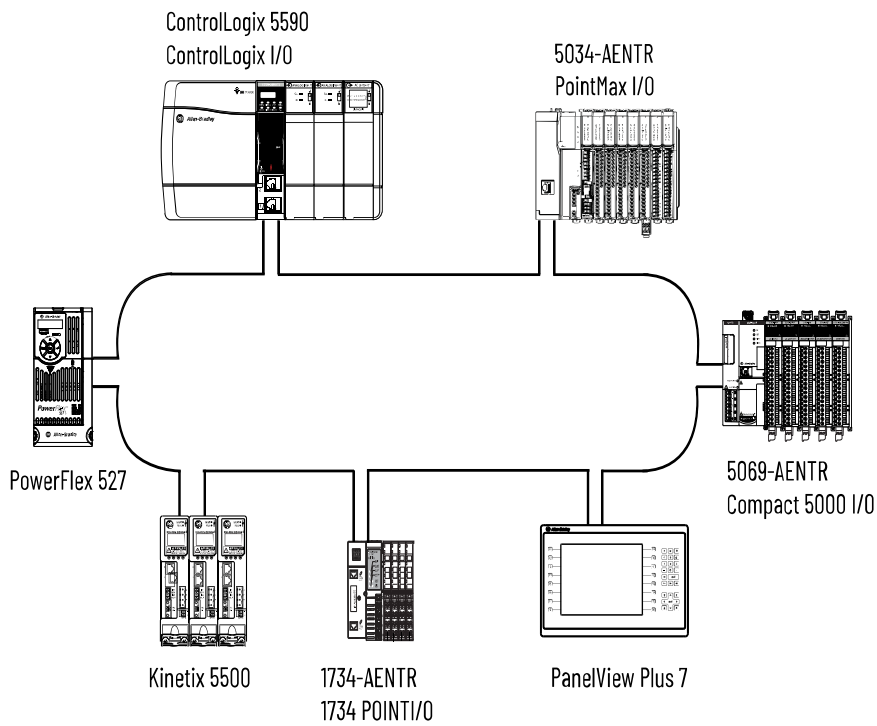


Figure 16. Controller in Linear/DLR Mode on a Linear Network

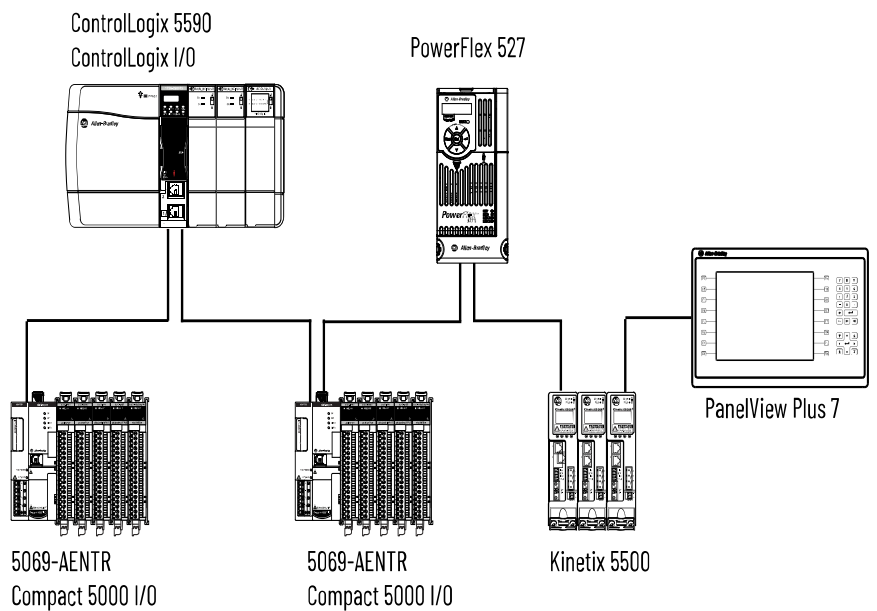
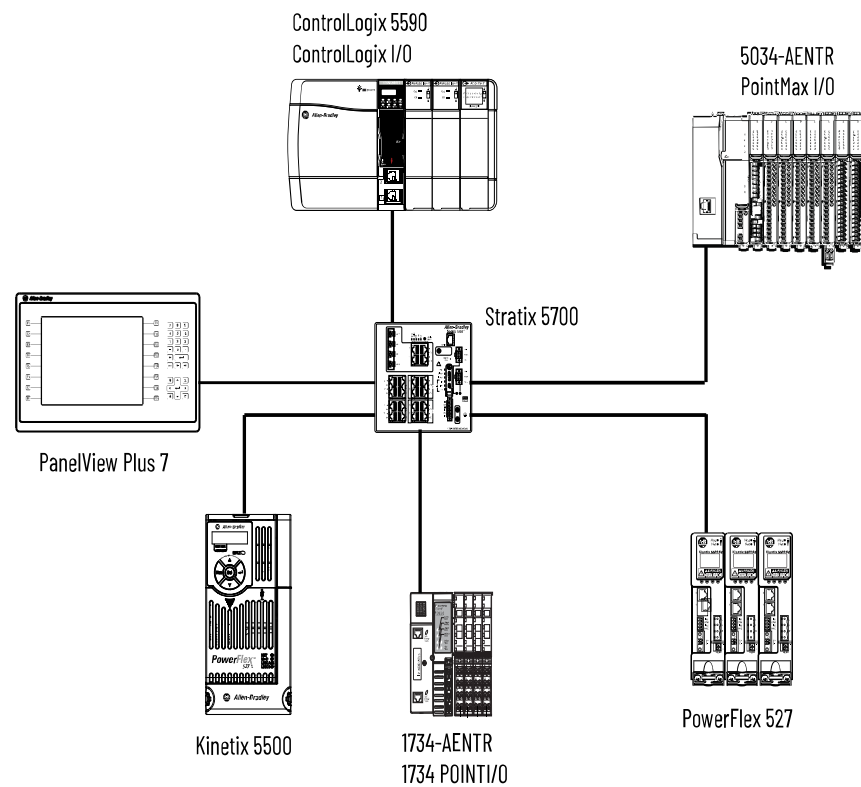


Figure 17. Controller in Linear/DLR Mode on a Star Network

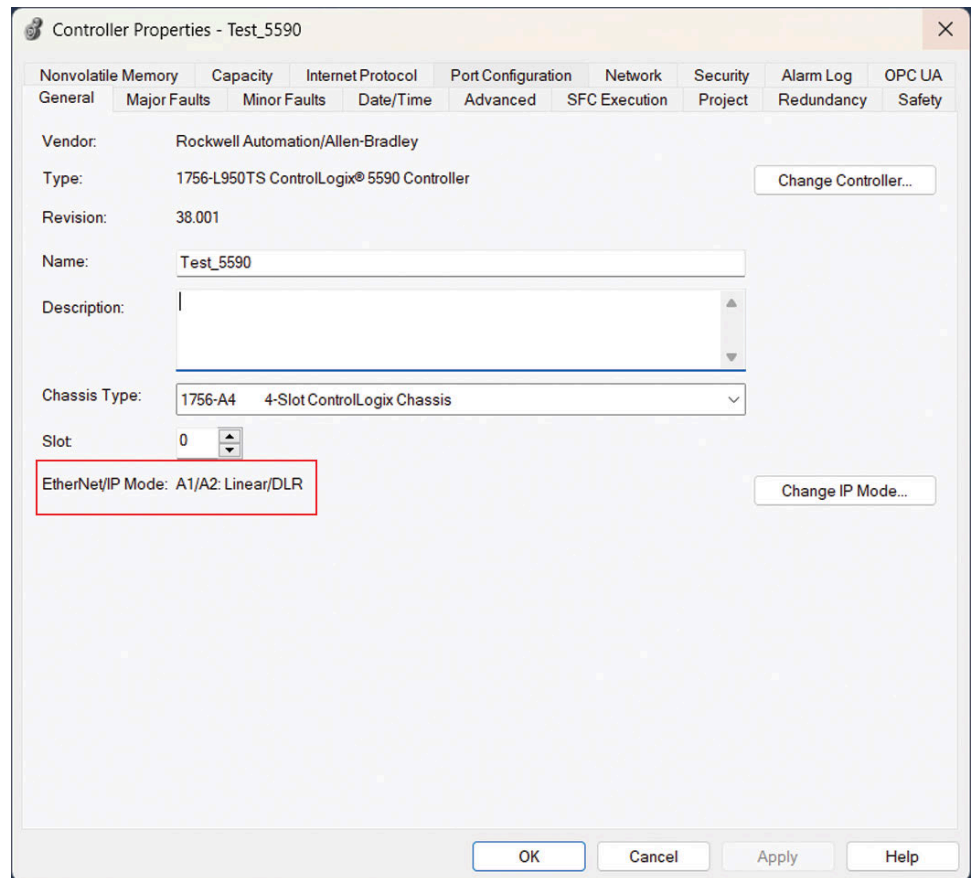


Configure Linear/DLR Mode in the Logix Designer Application

The EtherNet/IP™ mode is Dual-IP by default. You must change the EtherNet/IP™ mode to Linear/DLR with the Studio 5000 Logix Designer® application. For information on how to change the controller EtherNet/IP™ mode, see [Change the EtherNet/IP Mode in the Logix Designer Application on page 59](#).

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

After you change the EtherNet/IP™ mode to Linear/DLR mode, the new mode choice is displayed on the General tab in the Controller Properties dialog box.



You set the IP address and subnet mask on the Internet Protocol tab.



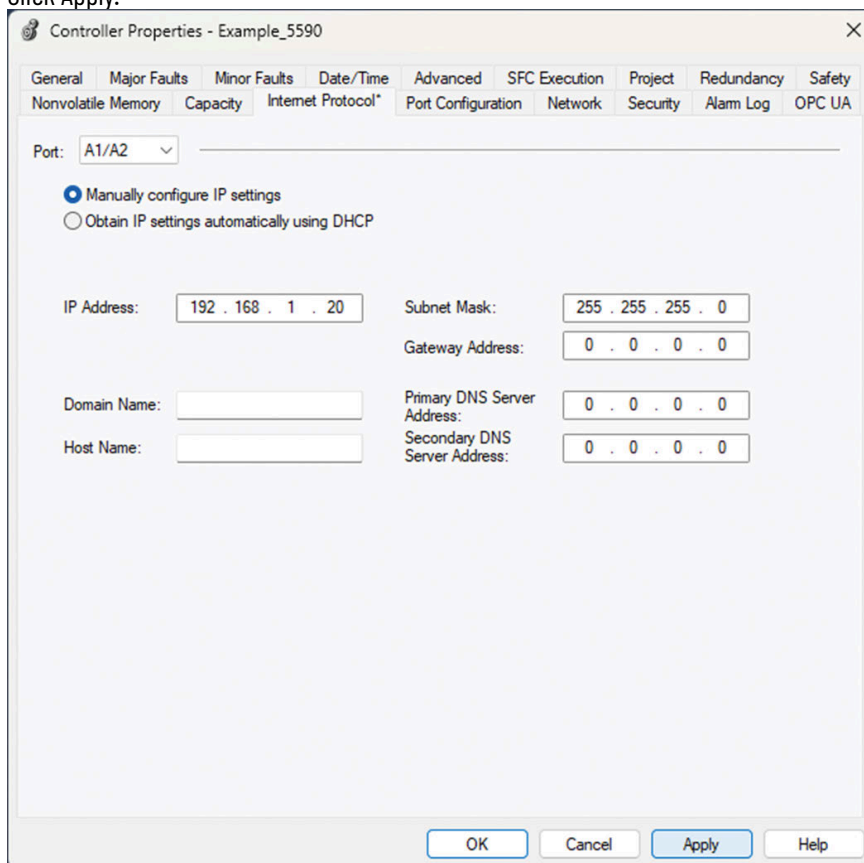
When you set the IP address and subnet mask, we recommend that you use a USB connection from the workstation to the controller.

1. Confirm that the project is online.
2. Confirm that the controller is in one of the following modes.
 - Program
 - Remote Program
 - Remote Run

You cannot change the IP address or subnet mask if the controller is in Run mode.

3. From the Port dropdown menu on the Internet Protocol tab, choose A1/A2.
4. Choose Manually configure IP settings.
5. Assign the IP address and network mask values.

6. Click Apply.



Configure Linear/DLR Mode in FactoryTalk Linx Software

You can configure the controller for Linear/DLR mode with FactoryTalk® Linx software. The EtherNet/IP mode is displayed on the .. tab. The EtherNet/IP™ mode is Dual-IP by default. You must change the EtherNet/IP™ mode to Linear/DLR. For information on how to change the controller EtherNet/IP™ mode, see [Change the EtherNet/IP Mode in FactoryTalk Linx Software on page 60](#).

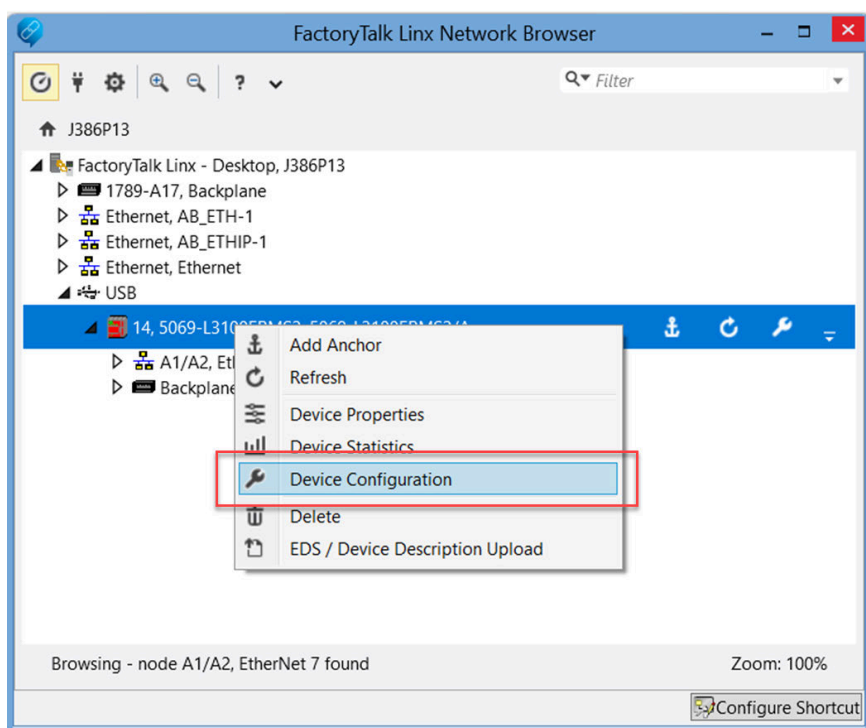
IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

You set the IP Address and Subnet Mask on the Internet Protocol tab.

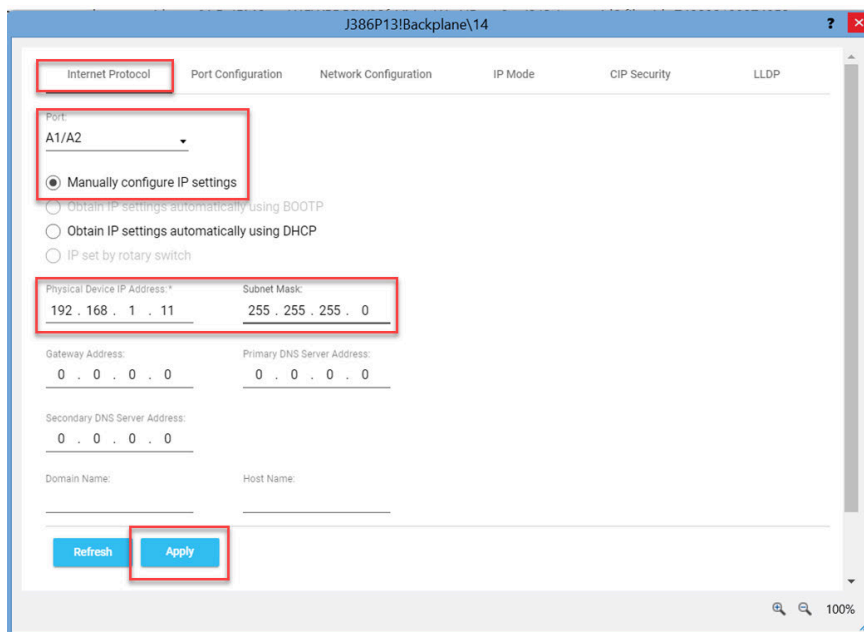
1. Confirm that the project is online.
2. Confirm that the controller is in one of the following modes.
 - Program
 - Remote Program
 - Remote Run

You cannot change the IP address or subnet mask if the controller is in Run mode.

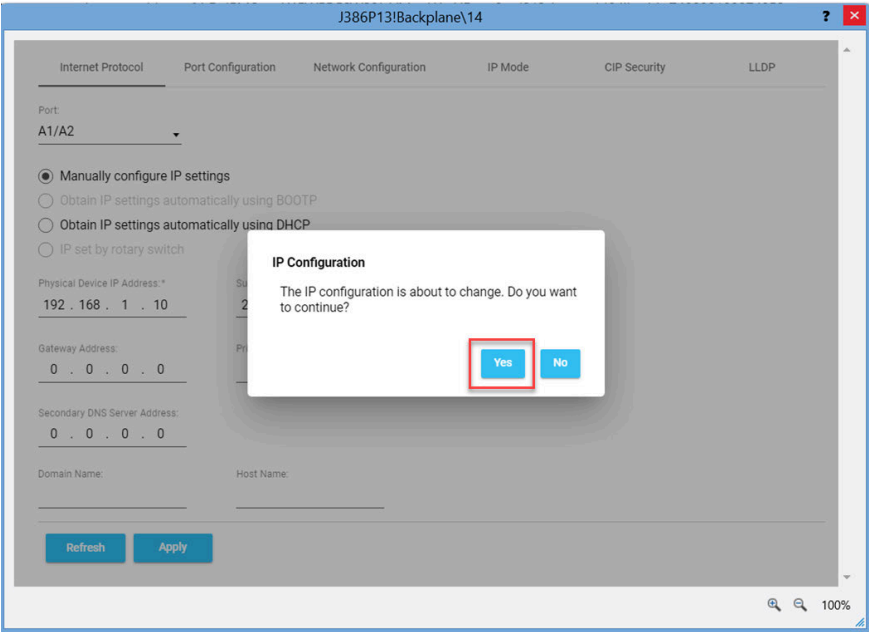
3. Right-click the controller and choose Device Configuration.



4. From the Port pull-down menu on the Internet Protocol tab, choose A1/A2.
5. Choose Manually configure IP settings.
6. Assign IP Address and Network Mask values.
7. Click Apply.



8. Click Yes on the IP Configuration dialog box.



Change the EtherNet/IP Mode

You can change the EtherNet/IP™ mode in the Studio 5000 Logix Designer® application or FactoryTalk® Linux software.

IMPORTANT: Exercise caution when you change the EtherNet/IP™ mode on your controller and consider the possible effects of the change.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

Effects of changing the EtherNet/IP Mode

The effects of changing the EtherNet/IP™ mode are different based on mode change. Make sure that you are aware of them before changing the EtherNet/IP™ mode.

Table 9. Effect of Changing the EtherNet/IP Mode

EtherNet/IP™ Mode Change	Effects
Dual-IP Mode to Linear/DLR Mode	IMPORTANT: You cannot change the controller EtherNet/IP™ mode from Dual-IP to Linear/DLR when you are connected through port 1 port. You must be connected to the controller via port 2 to change from Dual-IP mode to Linear/DLR mode. • The port 2 IP address, network mask, default gateway settings are applied to the A1/A2 port. • The MAC address of port 1 is applied to port A1/A2.

Table 9. Effect of Changing the EtherNet/IP Mode (continued)

EtherNet/IP™ Mode Change	Effects
	- Attempts to change from Dual-IP mode to Linear/DLR mode are only successful if the I/O configuration section in at least one port does not contain modules. - If the I/O configuration sections for both ports include modules, you cannot change the EtherNet/IP™ mode from Dual-IP mode to Linear/DLR mode.
Linear/DLR Mode to Dual-IP Mode	- The port A1/A2 IP address, network mask, default gateway settings are applied to port 2. - Other port A1/A2 settings, for example, DNS servers and Domain Name, are lost. - The port A1/A2 MAC address is applied to port 1. A separate MAC address is applied to port 2. - Port 1 is DHCP-enabled. - The I/O Configuration section in the Logix Designer application project is automatically assigned to port 1. - You can change the I/O configuration in the Logix Designer application project to assign it to port 2.

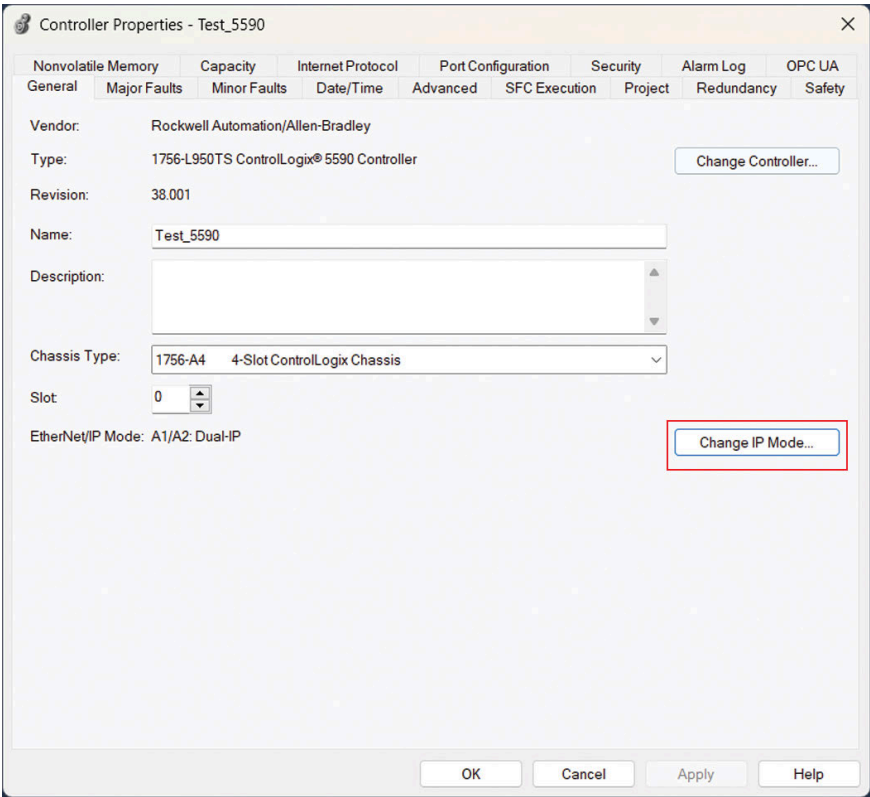
Change the EtherNet/IP Mode in the Logix Designer Application

This example shows the EtherNet/IP™ mode change from Dual-IP mode to Linear/DLR mode. The same tasks apply to change from Linear/DLR mode to Dual-IP mode

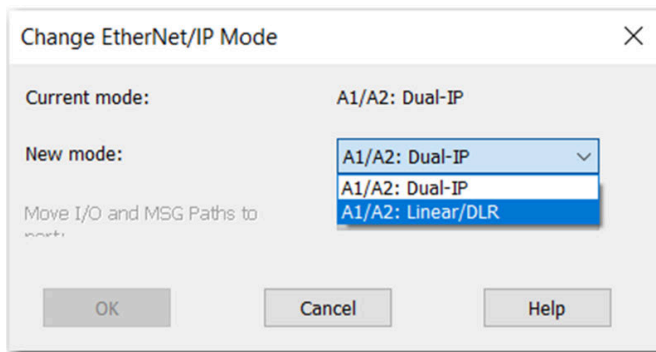
IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

Make sure that you are aware of the effects of changing the EtherNet/IP™ mode. See Change the EtherNet/IP Mode on page .

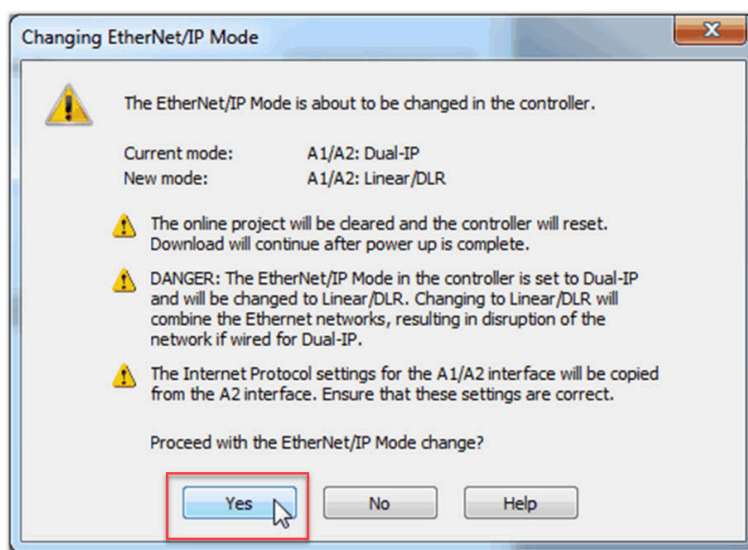
1. Confirm that the project is offline.
2. On the General tab of the Controller Properties dialog box, click Change IP Mode.



- From the New mode dropdown, choose the new mode and click OK.



- Click OK on the Controller Properties dialog box.
- Save the project.
- Download the updated project to the controller.
- When the following warning appears, read it carefully.
- Click Yes to continue.



Change the EtherNet/IP Mode in FactoryTalk Linx Software

This example shows the EtherNet/IP™ mode change from Dual-IP mode to Linear/DLR mode. The same tasks apply to change from Linear/DLR mode to Dual-IP mode.

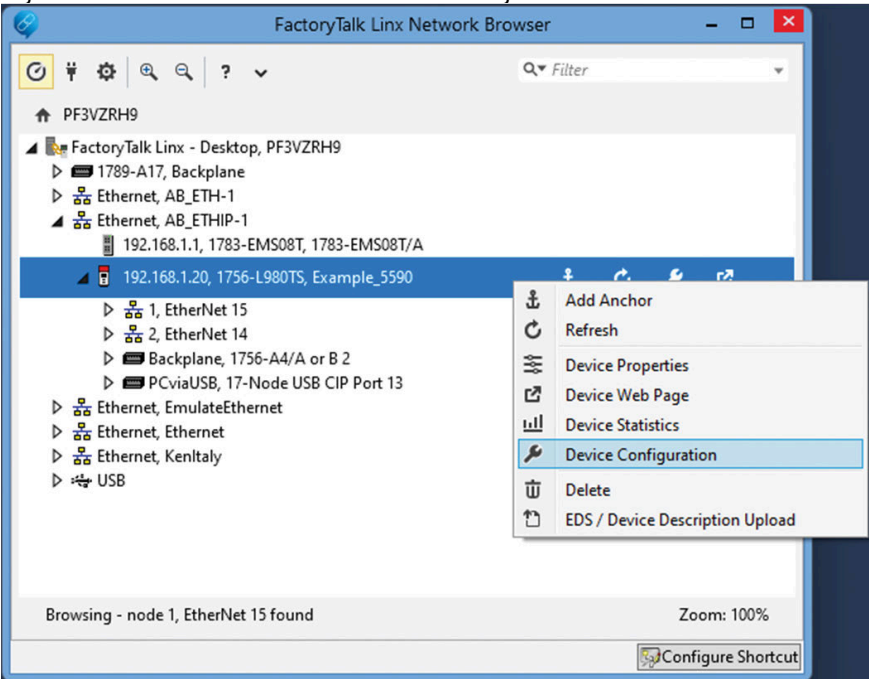
IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

Make sure that you are aware of the effects of changing the EtherNet/IP™ mode. See [Change the EtherNet/IP Mode](#) on page .

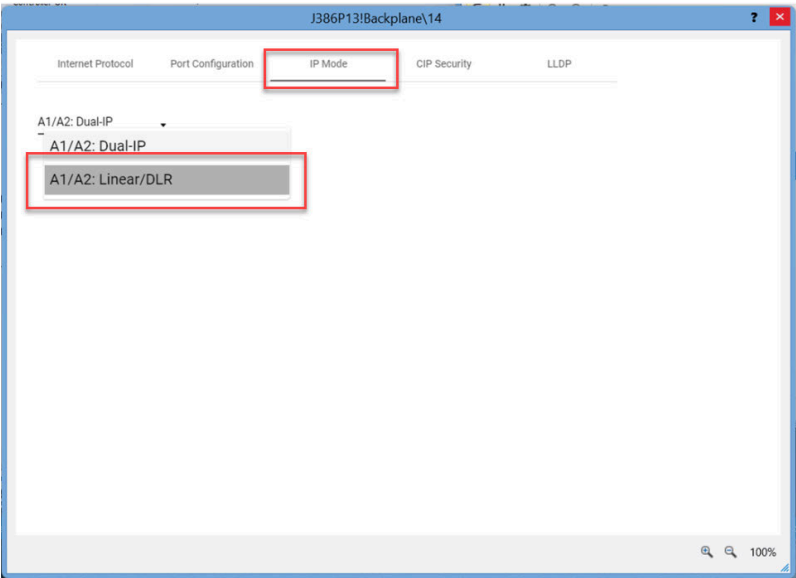
- Confirm that the controller is online and there is no project in the controller.
- Confirm that the controller is in one of the following modes:
 - Program
 - Remote Program
 - Remote Run

You cannot change the EtherNet/IP™ mode if the controller is in Run mode.

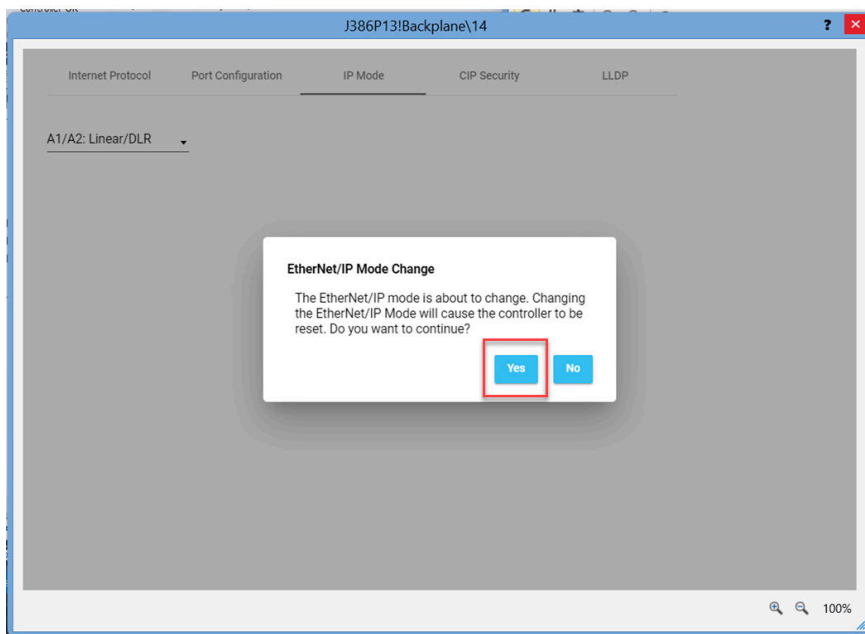
3. Right-click the controller and choose Device Configuration.



4. From the dropdown menu on the IP Mode tab, choose the new mode.



5. When the EtherNet/IP™ Mode Change warning appears, read it carefully, and click Yes.



DNS Requests

To qualify the address of a module, use DNS addressing to specify a host name for a module, which also includes specifying 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 module by host name, such as in path descriptions in MSG instructions.

For more information on DNS Addressing, see:

- [DNS Addressing on page 32](#)
- EtherNet/IP Network Configuration User Manual, publication [ENET-UM001](#)

DNS requests can be generated from port 1 or port 2.

IMPORTANT: With ControlLogix® 5590 controllers, the Ethernet ports on the controller itself are labeled 1 and 2. In programming and communication software, the ports are described as A1 and A2.

DNS Request Generated From Port 1

The following apply when port 1 generates the DNS request:

- If the DNS server address is in the local subnet of port 1, DNS requests leave through port 1.
- If port 2 is enabled and the DNS server address is in local subnet of port 2, DNS requests leave through port 2.
- If the DNS server address is outside of all local subnets, DNS requests leave through port 1 towards port 1 default gateway.

DNS Request Generated From Port 2

The following apply when port 2 generates the DNS request:

- If port 1 is enabled and the DNS server address is in local subnet of port 1, DNS requests leave through port 1.
- If the DNS server address is in local subnet of port 2, DNS requests leave through port 2.
- If port 1 is enabled and the DNS server address is outside of all local subnets, DNS requests leave through port 1 towards port 1 default gateway.
- If port 1 is disabled and the DNS server address is outside of all local subnets, DNS requests leave through port 2 towards port 2 default gateway.

SMTP Server

The SMTP server is only available via the enterprise port. Therefore, emails can only be sent on the enterprise port.

For more information on how to send emails via an Ethernet port, see the EtherNet/IP Network Configuration User Manual, publication [ENET-UM001](#).

Socket Object in Dual-IP Mode

When the controller operates in Dual-IP mode and uses a socket object, you can use an IP address with a Socket_Create service type. By default this IP address is INADDR_ANY.

Remember the following:

- If you use INADDR_ANY, IP communication that the Socket Object instance initiates follows the same routing rules as DNS request routing rules described in [DNS Requests on page 62](#).
- If you use the IP address of port 1 instead of INADDR_ANY, IP packets can only go to the port 1 subnet or via its default gateway.
- If you use the IP address of port 2 instead of INADDR_ANY, IP packets can only go to port 2 subnet or via its default gateway.
- If you use an IP address other than the port A1.

Message Instructions By Ethernet Port

You can send Message (MSG) instructions out the enterprise port or the device-level port. The only difference between the MSG instruction configurations is the path.

When you configure an MSG instruction on a controller that operates in Dual-IP mode, use these paths:

- Enterprise port (Port 1) - 3
- Device-level port (Port 2) - 4

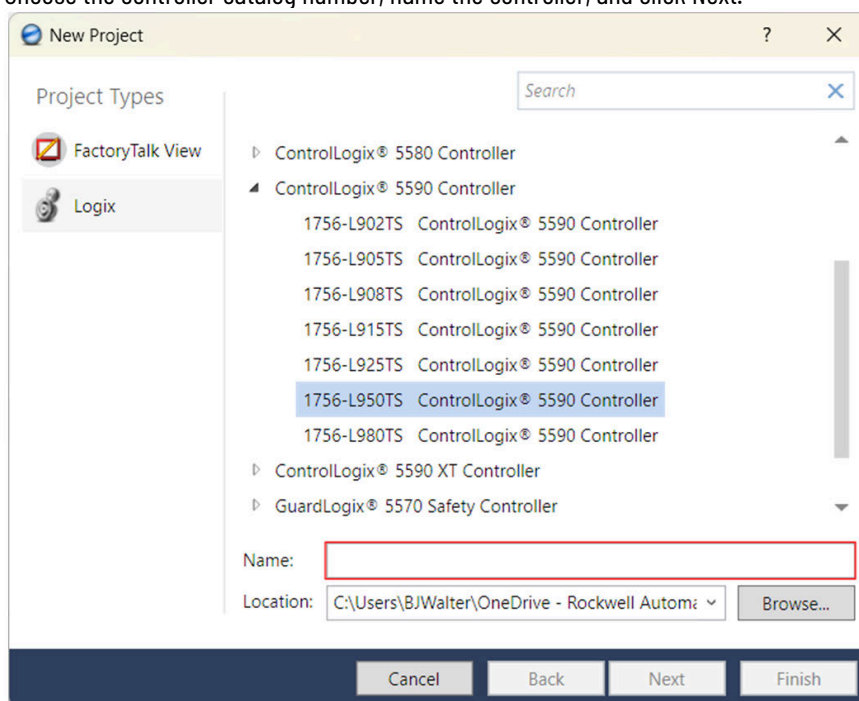
If the controller operates in Linear/DLR mode, the path is 2.

For more information on how to use MSG instructions, see the Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

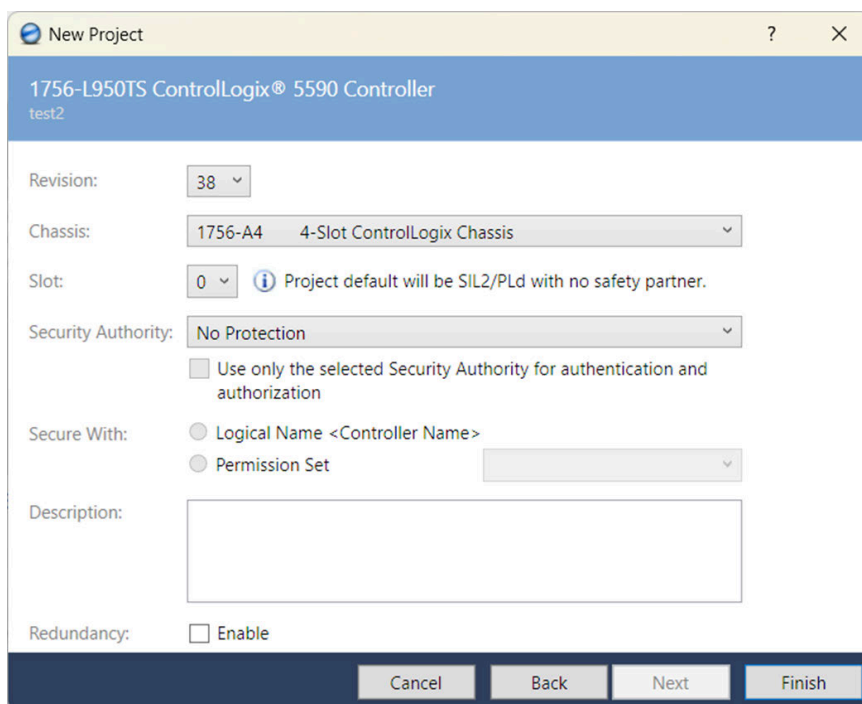
Create a Controller Project

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

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

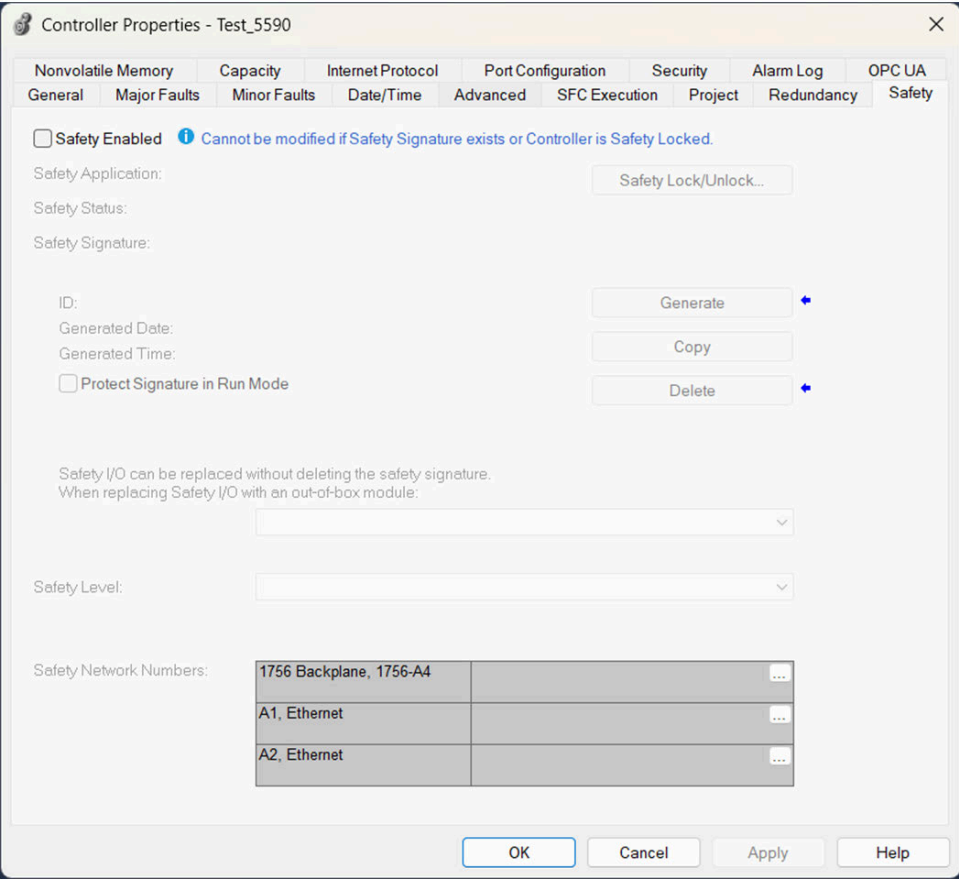


3. Define the properties of the controller, and click Finish:



For a new ControlLogix® 5590 project, the controller defaults to a safety project. To use the controller in a non-safety project, unselect the Safety Enabled checkbox on the Safety Tab in the Controller Properties dialog.

For more information on changing the project, see [Change Controller Project Type on page 280](#).



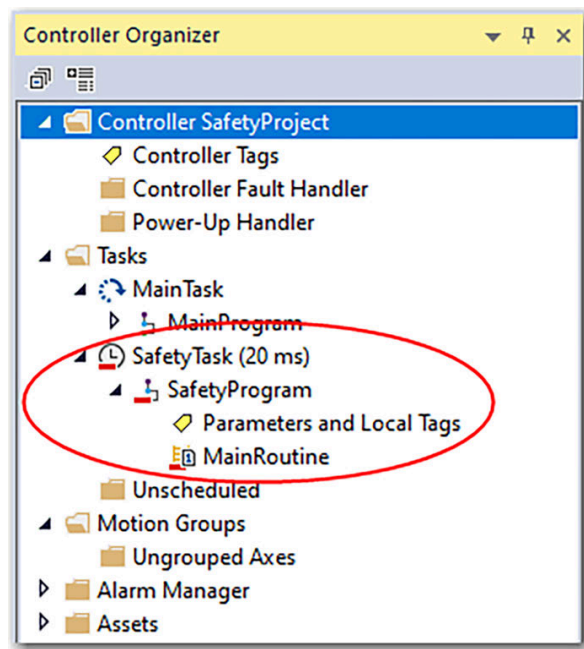
Safety Project Configuration

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

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

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

Figure 18. Safety Components



Set the Safety Level

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

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

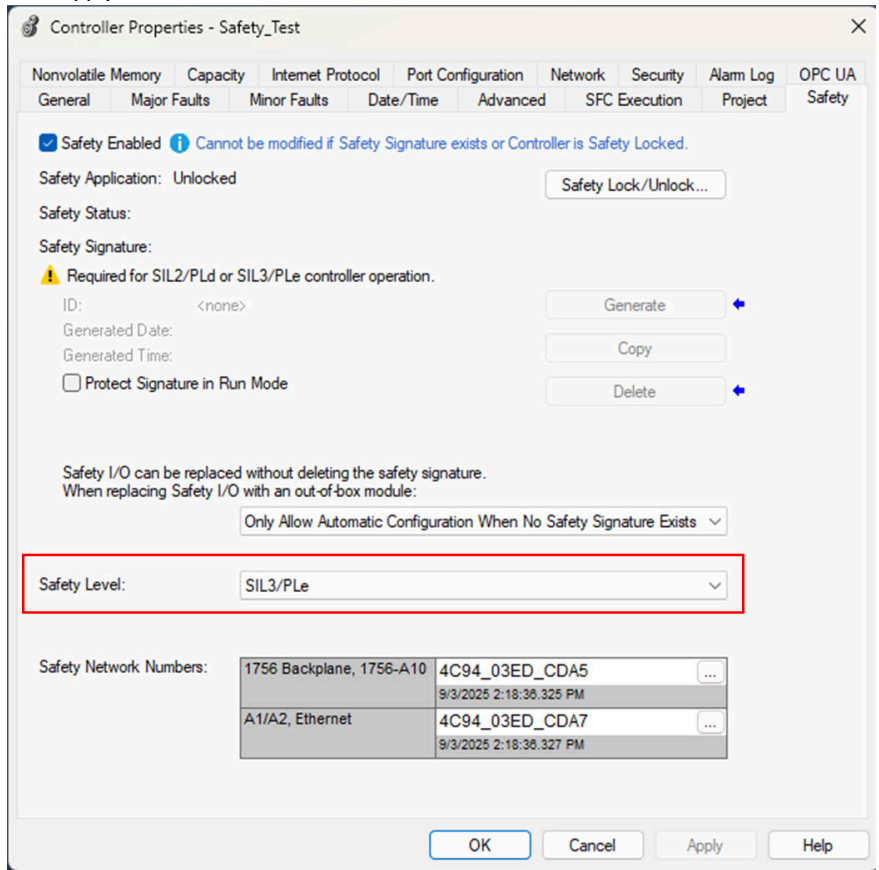
You must specify the safety level:

- The default setting is SIL 2/PLd.
- You can only modify the setting offline, when the safety application is in the Unlocked state and no safety signature exists.
- For SIL 3/PLe, you must have a 1756-L9SP safety partner that is installed to the right of the primary controller. If you select SIL 3/PLe, a safety partner appears in the Controller Organizer I/O tree. If you change the value back to SIL 2/PLd, the safety partner disappears from the I/O tree.

Perform these tasks to set the safety level.

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

4. Click Apply and then OK.



Passwords for Safety-locking and Unlocking

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

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

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

Protect the Safety Signature in Run Mode

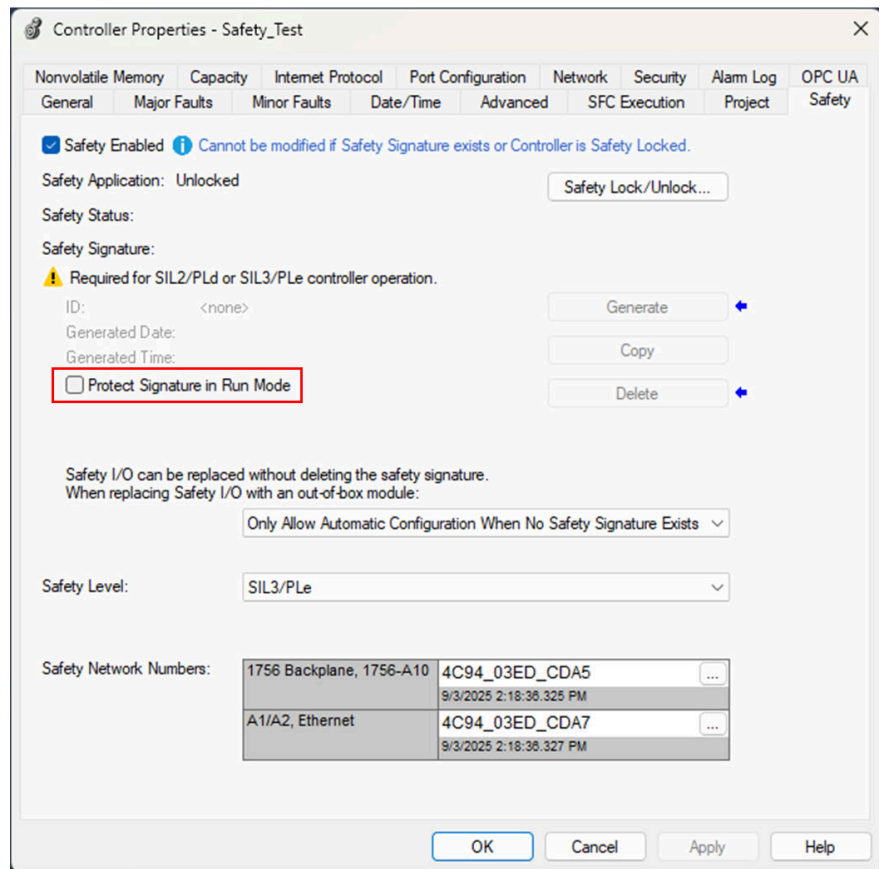
You can help prevent the safety signature from being deleted while the controller is in Remote Run mode, regardless of whether the safety application is locked or unlocked.

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

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

Follow these steps to protect the safety signature.

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



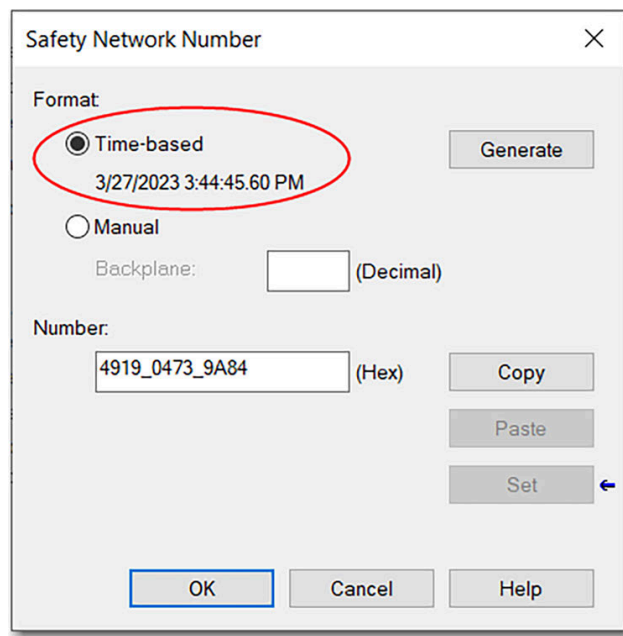
Automatic Assignment of Time-based Safety Network Number

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

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

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

Figure 19. Time-based Format



Manual Assignment of Safety Network Number

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

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

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

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

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

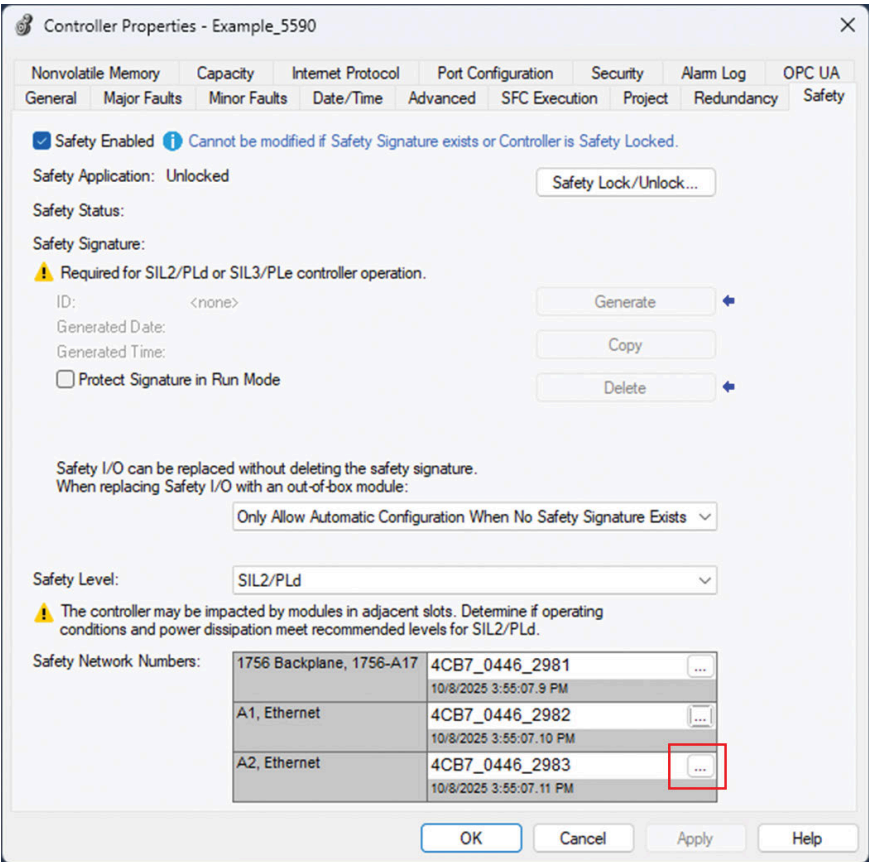
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

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

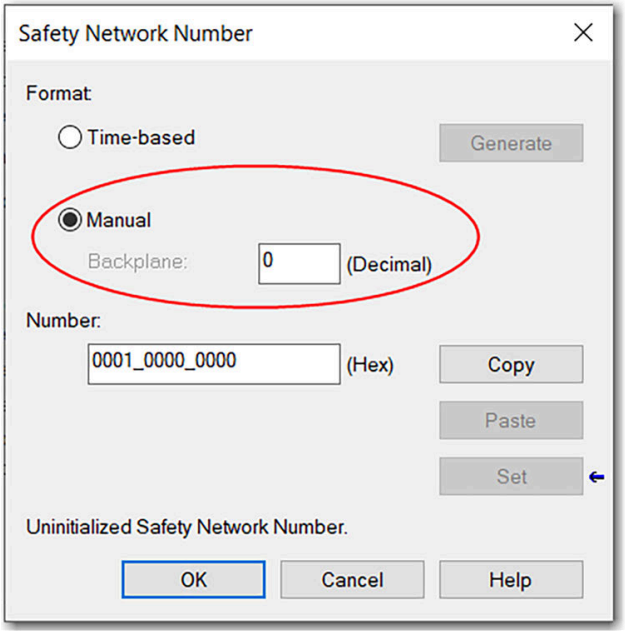
If there are duplicate unique node references, as the system user, you are responsible for proving that an unsafe condition cannot result.

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

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



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

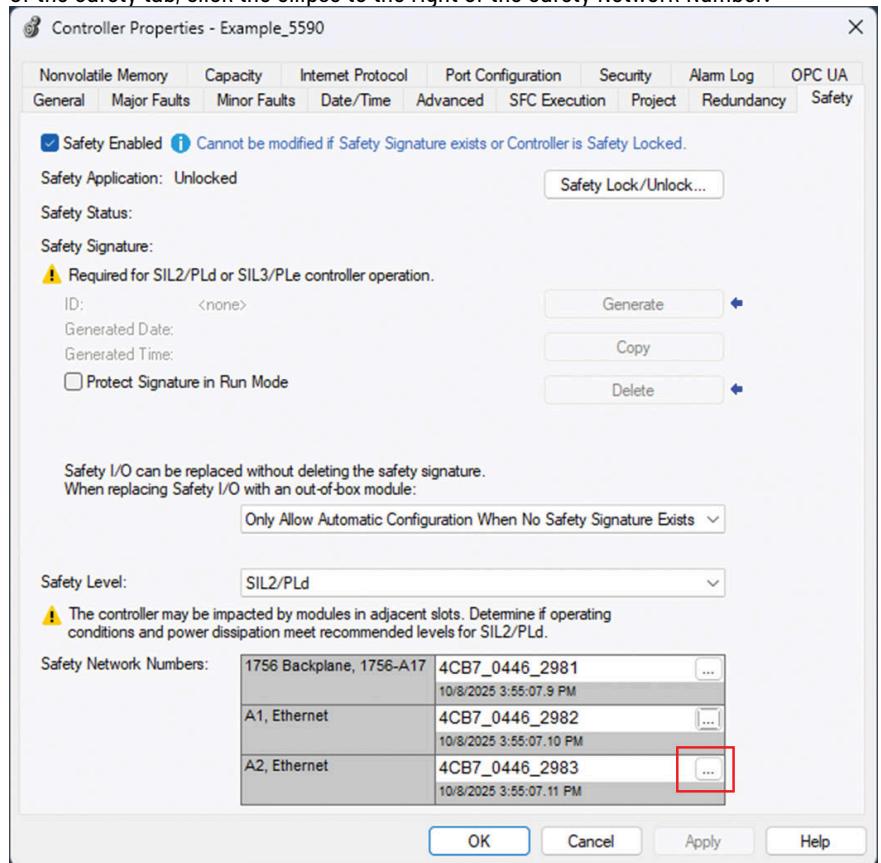


Copy a Safety Network Number

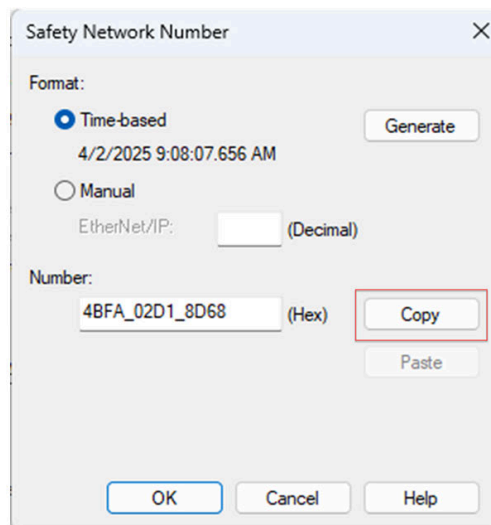
If you must apply a Safety Network Number to other controllers, you can copy and paste the SNN.

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

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



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



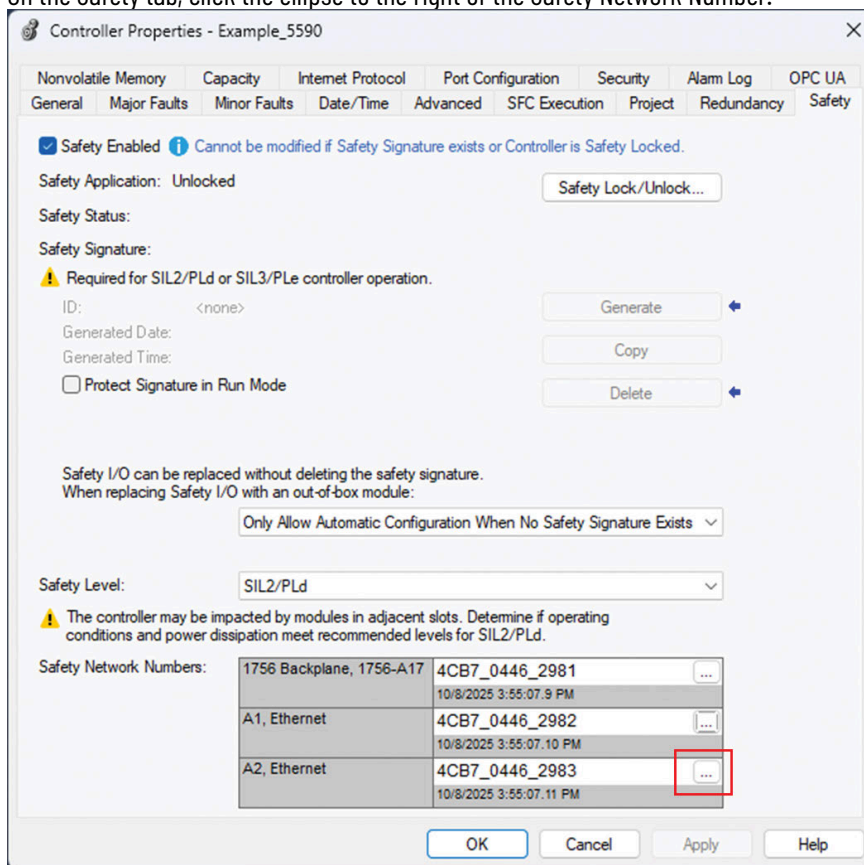
5. On the Controller Properties dialog box, click OK.

Paste a Safety Network Number

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

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

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



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

Use the Network Browser to Go Online with the Controller

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

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

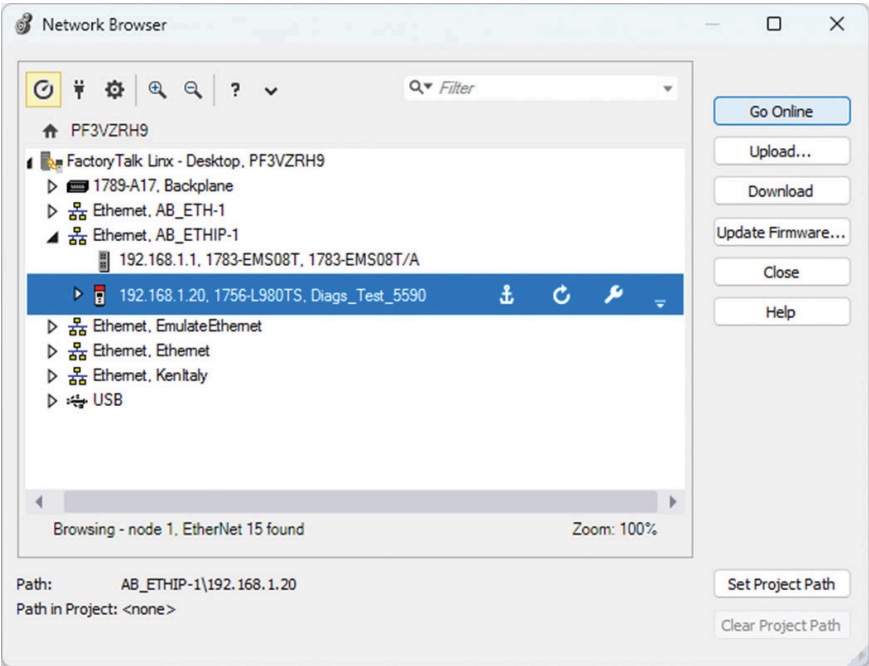


3. Expand the communication path and select the controller.
4. To store the path in the project file, click Set Project Path.



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

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



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

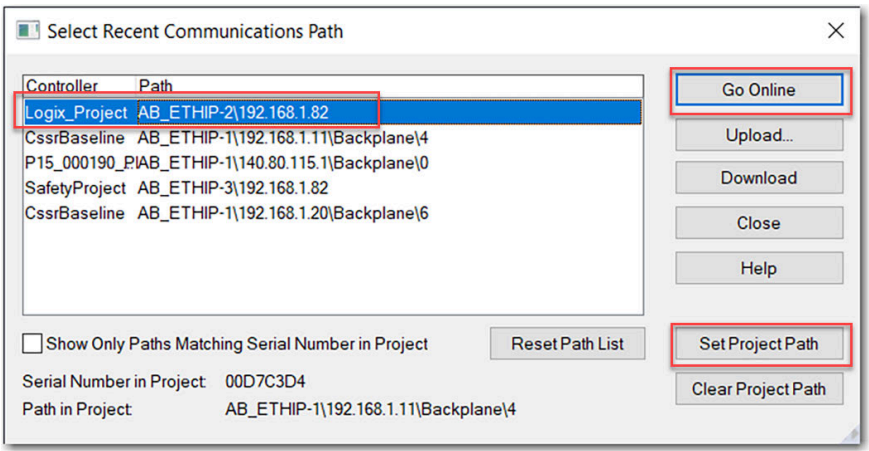
Use a Recent Communication Path to Go Online with the Controller

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

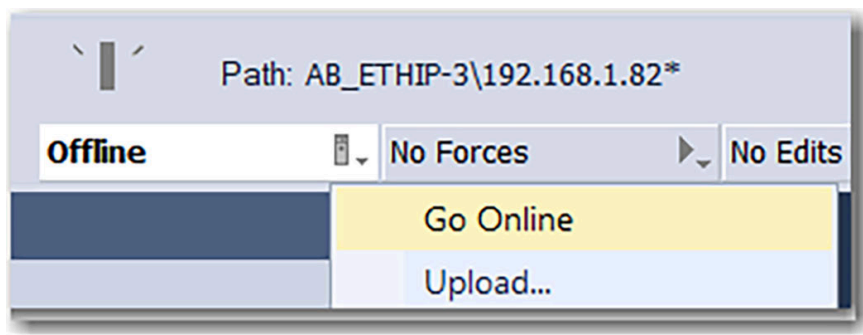
1. In the application, click the arrow that is on the Path bar.



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



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



Considerations for Going Online with the Controller

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

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

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

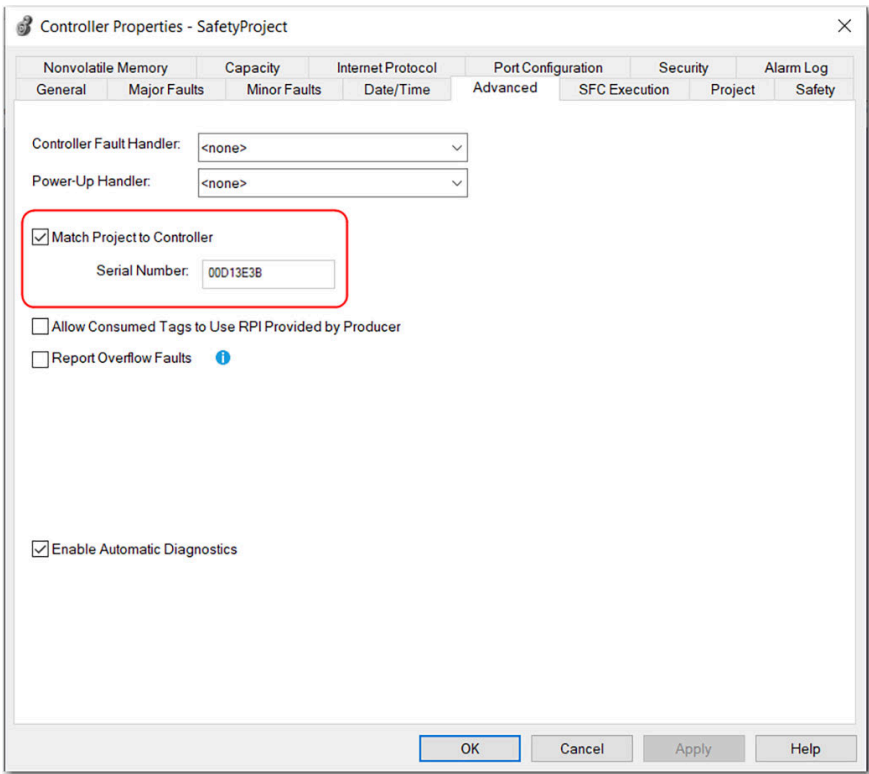
For safety controllers, additional considerations include the safety status and faults, the existence of a safety signature, and the safety-lock/-unlock status of the project and the controller.

Match Project to Controller

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

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

Figure 20. Match Project to Controller



Firmware Revision Matching

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

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

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



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

Considerations for Going Online with a Safety Project

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

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

A number of factors affect these processes, including Match Project to Controller feature and Firmware Revision Matching. For more information on these features, see [Considerations for Going Online with the Controller on page 74](#).

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

Safety Status/Faults

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

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

Safety Signature and Safety-locked and -unlocked Status

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

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

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

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

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

Table 10. Effect of Safety-lock and Safety Signature on Download Functionality

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

Checks for Going Online with a Safety Project

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

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

Table 11. Connect to the Controller with a Safety Project

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

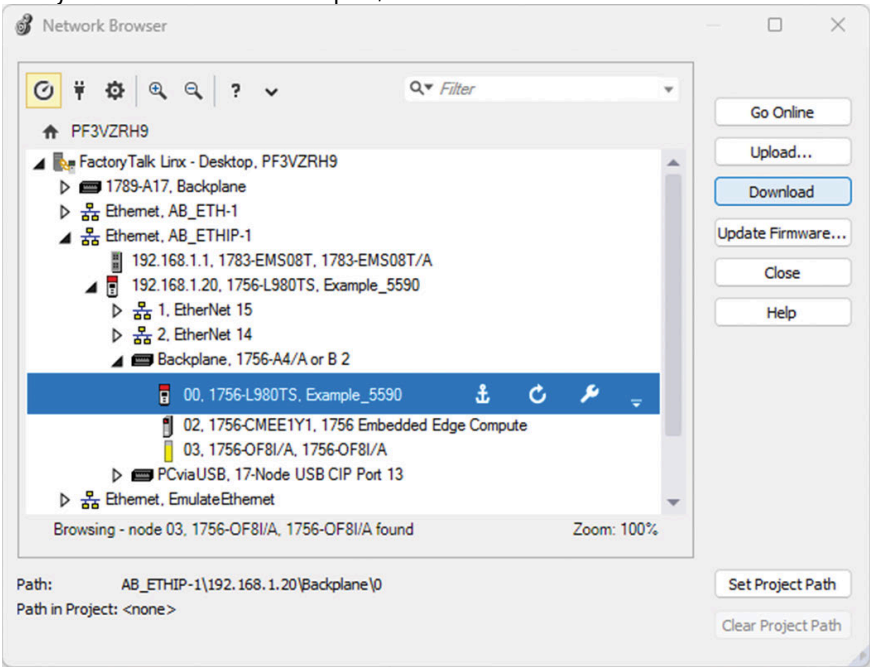
When the controller and the Logix Designer application are online, the safety-locked status and safety signature of the controller match the controller's project. The safety-lock status and safety signature of the offline project are overwritten by the controller. If you do not want the changes to the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

Use the Network Browser to Download to the Controller

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

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

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



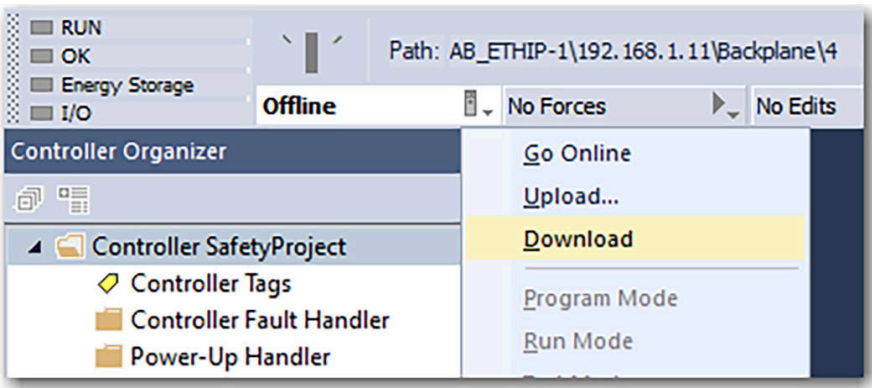
- 2. After reading the warning in the Download dialog box, click Download.

Use the Controller Status Menu to Download to the Controller

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

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

Figure 21. Download via the Controller Status Menu



Download Considerations for a Safety Project

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

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

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

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

Table 12. Status Messages

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

Table 12. Status Messages (continued)

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

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

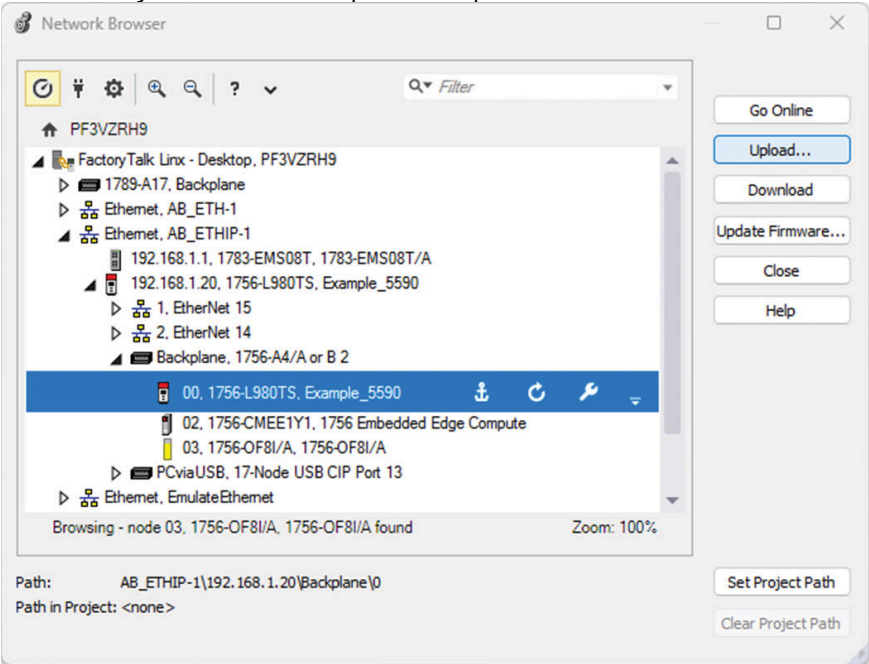
Use the Network Browser to Upload from the Controller

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

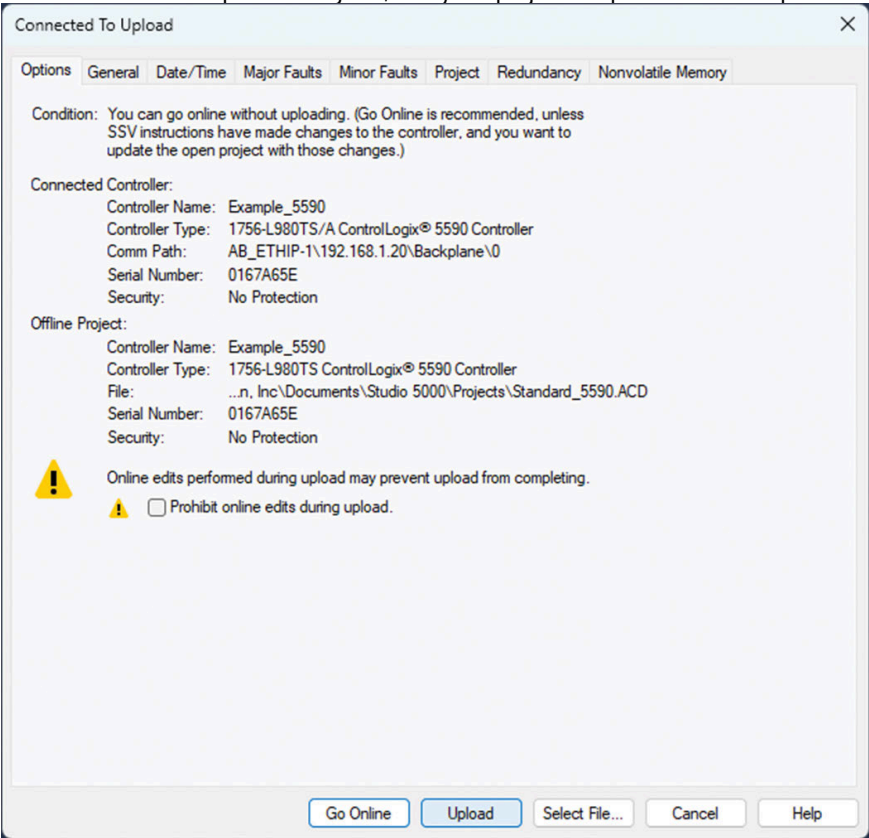
You can use the features of the Network Browser dialog box to upload from your controller after you have set the communication path.

Complete these steps to upload from the controller.

- 1. After choosing the communication path, click Upload.



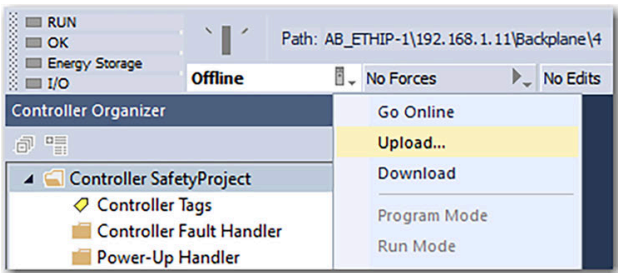
2. On the Connected to Upload dialog box, verify the project to upload and click Upload.



Use the Controller Status Menu to Upload from the Controller

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

1. From the Controller Status menu, choose Upload.



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

Considerations for Upload from a Safety Controller

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

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

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

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

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



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

Controller Operation Modes

The controller operates in the following modes:

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

Run Mode

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



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

The controller can perform these functions in Run mode:

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

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

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

Remote Run Mode

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



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

The controller can perform these functions in Remote Run mode:

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

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

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

Remote Program Mode

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



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

The controller can perform these functions in Remote Program mode:

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

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

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

Remote Test Mode

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



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

The controller can perform these functions in Remote Test mode:

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

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

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

Program Mode

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



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

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

The controller can perform these functions in Program mode:

- Turn outputs to their configured state commanded for Program mode
- Download a project

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

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

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

Change the Operation Mode

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

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

Table 13. Controller Switch Positions and Operation Modes

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

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

- To activate Remote Run mode, move the switch from RUN to REM.
- To activate Remote Program mode, move the switch from PROG to REM.
- To activate Remote Test mode, use the programming software along with the REM switch position.

When the switch on the controller is set to RUN mode, features like online editing, program downloads, and firmware updates are prohibited. For a list of prohibited features, see [Controller Operation Modes on page 82](#).

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

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

Use the Logix Designer Application to Change the Operation Mode

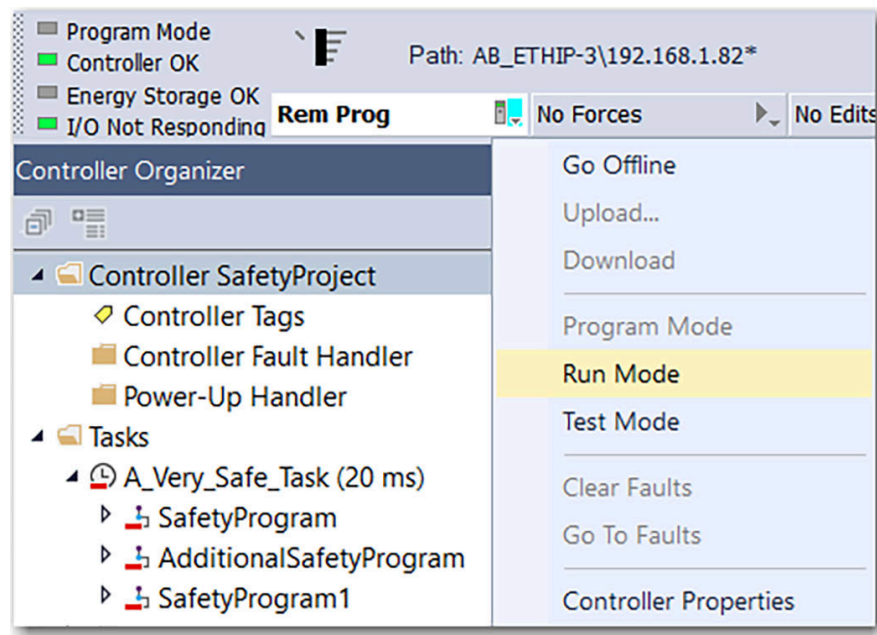
When you are online with the controller, and the switch position is set to REM, then you can use the Logix Designer application to change the operation mode.

The Controller Status menu lets you specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

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

Figure 22. Operation Modes in Logix Designer



Use the Memory Card

The controllers ship with a memory card installed.

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

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

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

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

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

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

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

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

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

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

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

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

Remember the following:

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

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

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

Safety Project Considerations

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

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

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

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

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

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

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

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

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

Store to the Memory Card

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

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

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

If Load/Store is dimmed, verify the following:

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

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

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



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

A screenshot of a software dialog box. It has three labels: "Load Image:", "Load Mode:", and "Safety Application:". Each label is followed by a dropdown menu. The "Load Image:" dropdown shows "User Initiated". The "Load Mode:" dropdown shows "On Power Up", "On Uninitialized Memory" (highlighted in blue), and "User Initiated". The "Safety Application:" dropdown shows "Unlocked".

Table 14. Choose a Load Image Setting

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

Application Requirement	Load Image Setting	Description	Safety Considerations
		is also loaded and the controller enters the selected mode, either Program or Run. - You can always use the Logix Designer application to load the project.	
Load image only from the Controller Properties dialog in the Logix Designer application	User Initiated	If the controller type and the major and minor revisions of the project in nonvolatile memory match the controller type and major and minor revisions of the controller, you can initiate a load.	- You can initiate a load, regardless of the Safety Task status. - You can load a project to a safety-locked controller only when the safety signature of the project that is stored in nonvolatile memory matches the project on the controller. - If the signatures do not match or the controller is safety-locked without a safety signature, you are prompted to first unlock the controller. When you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety signature are set to the values contained in nonvolatile memory once the load is complete. - If the firmware on the primary controller matches the revision in nonvolatile memory, the safety partner firmware is updated, if necessary, the application that is stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the Program mode. - For a ControlLogix 5590 controller in a SIL 3 safety application with a safety partner installed, the controller loads the stored project and firmware on power up.

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

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

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

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

IMPORTANT: Safety Consideration

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

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

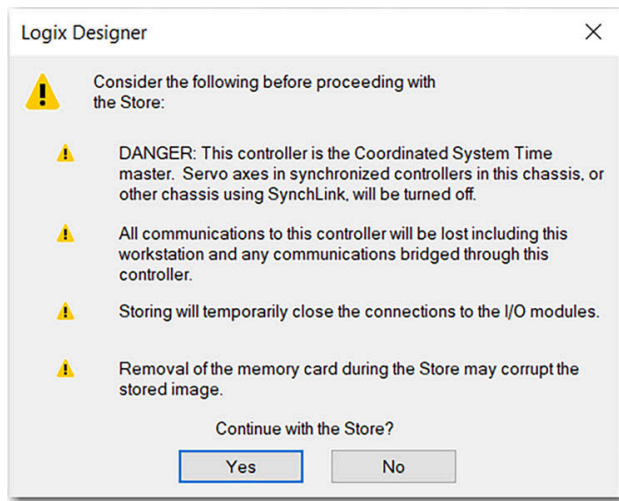
IMPORTANT: Safety Consideration

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

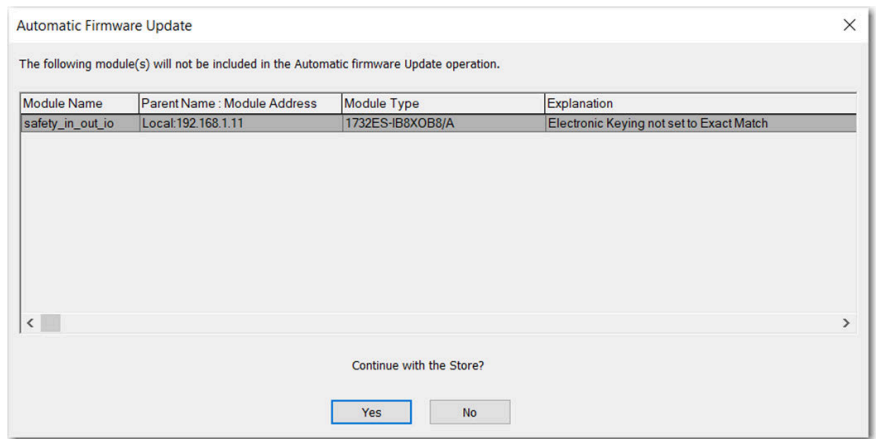
This table describes the Automatic Firmware Update options for I/O devices.

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

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



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



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

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

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

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

When the store is complete, the controller resets.

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

Load from the Memory Card

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

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

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

- Controller powerup
- User-initiated action

Controller Powerup

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

Table 15. Memory Card Behavior on Power-up for ControlLogix 5590 Controllers

Controller Application Type	Image Setting	Controller is in out-of-box condition (v1.x firmware)	Firmware > 1.x and internal nonvolatile memory is not valid ("Valid" includes the No Project condition)	Firmware > 1.x and internal nonvolatile memory is valid ("Valid" includes the No Project condition)
• Standard control • High Availability (Redundancy and Logix SIS) • SIL 2 safety	User Initiated	Loads Firmware Only	Does Nothing	Does Nothing
SIL 3 safety with Safety Partner installed	User Initiated	Loads both Firmware and Application	Does Nothing	Does Nothing
Any	On Power Up	Loads both Firmware and Application	• Loads Firmware if there is a revision mismatch • Loads Application	• Loads Firmware if there is a revision mismatch • Loads Application
Any	On Uninitialized Memory	Loads both Firmware and Application	• Loads Firmware if there is a revision mismatch • Loads Application	Does Nothing

User-initiated Action

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

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

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

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

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



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

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

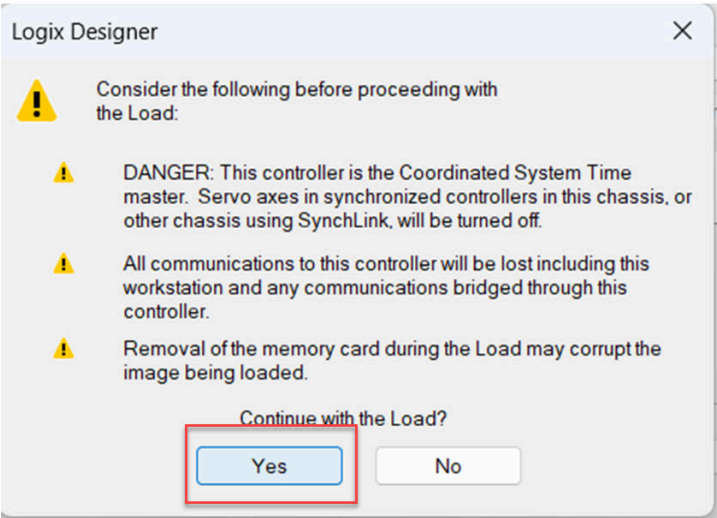
4. On the right side of the Nonvolatile Memory tab, click Load/Store.
-



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

- You have specified the correct communication path and are online with the controller.
 - The SD card is installed.
 - The controller is not in Run Mode.
-

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



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

Table 16. Controller Status Indicators

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

When the load is complete, the controller reboots.

Other Memory Card Tasks

You can perform these tasks with the memory card:

- Change the image that is loaded from the card
- Check for a load that was completed

- Clear an image from the card
- Store an empty image
- Change load parameters
- Read/write application data to the card
- View safety-lock status and safety signatures on the Nonvolatile Memory tab

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

Manage Controller Communication

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

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

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

Controller Communication Interaction with Control Data

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

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

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

Table 17. Controller Behavior

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

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

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

Good programming practice dictates the use of two unique words at the beginning and the end of data. The controller validates the words to assure the entire structure has data integrity. We recommend that the handshake data is changed and the application code validates it every

transaction before the controller application code or higher-level system reading controller data acts on it.

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

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

Table 18. Data Elements

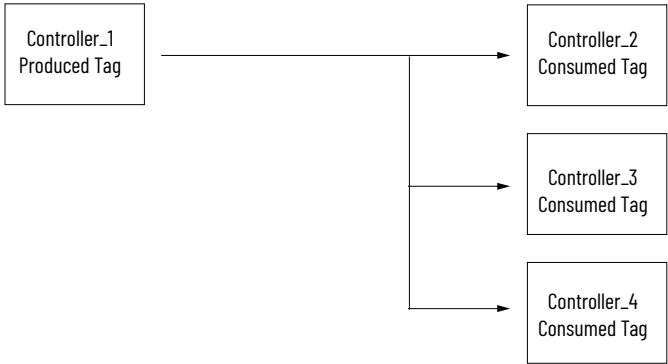
Structure	My_Recipe1	My_Recipe2	My_Recipe3
Start Data	101	102	103
Sugar	3	4	8
Flour	4	3	9
Chocolate	2	2	4
Oil	6	7	2
End Data	101	102	103

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

Produce and Consume (Interlock) Data

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

Figure 23. Illustration of Produced and Consumed Tags



The following table describes the system-shared tags.

Table 19. Produced and Consumed Tag Definitions

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

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

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

Safety controllers can also use produced and consumed safety tags.

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

Requested Packet Interval (RPI) of Multicast Tags

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

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

Send and Receive Messages

Messages transfer standard or safety data to other devices, such as other controllers or operator interfaces. The MSG instruction is a ladder logic output instruction that asynchronously reads or writes a block of data to or from another module over the backplane or a network. The size of the instruction depends on the data types and message command that you program.

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

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

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

Each message uses one connection out of the controller, regardless of how many devices are in the message path. You can connect CIP™ generic messages. However, for most applications

we recommend that you leave CIP™ generic messages unconnected. Connected messages that occur more frequently than once every 60 seconds should be cached if possible.

Table 20. Message Types

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

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

Cache Message Connections

When you configure an MSG instruction, you can choose whether to cache the connection. Cached connections transfer data faster than uncached connections. The controllers can cache 384 messages and trigger 384 messages simultaneously.

The following table describes the options for caching connections.

Table 21. Options for Caching Connections

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

Socket Interface

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

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

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

These devices support as many as 32 socket instances each:

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

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

TLS Support

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

HTTP(S) REST API Client Support

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

- raC_Impl_HTTPClient
- raC_Impl_HTTPCmdGET
- raC_Impl_HTTPCmdPOST
- raC_Impl_HTTPCmdPUT

Use a CIP Generic MSG to Enable SNMP on the Controller

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

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

1. Add an MSG instruction to your program.
-

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

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

Message Configuration

Configuration*

Communication

Tag

Message Type:

CIP Generic

Service Type:

Custom

Source

onArray

Source Length:

5

(Bytes)

Service Code:

4c

(Hex)

Class:

f5

(Hex)

Destination Element:

Instance:

1

Attribute:

0

(Hex)

New Tag...

☐ Enable

☐ Enable Waiting

☐ Start

☐ Done

Done Length: 0

Error Code:

Extended Error Code:

☐ Timed Out

Error Path: R010

Error Text:

OK

Cancel

Apply

Help

Table 22. Enable SNMP

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

Field	Description																																			
	<table><tr><th></th><th>Name</th><th>Value</th><th>Style</th><th>Data Type</th></tr><tr><td></td><td>onArray</td><td>{...}</td><td>Decimal</td><td>USINT[5]</td></tr><tr><td></td><td>onArray[0]</td><td>1</td><td>Decimal</td><td>USINT</td></tr><tr><td></td><td>onArray[1]</td><td>161</td><td>Decimal</td><td>USINT</td></tr><tr><td></td><td>onArray[2]</td><td>0</td><td>Decimal</td><td>USINT</td></tr><tr><td></td><td>onArray[3]</td><td>17</td><td>Decimal</td><td>USINT</td></tr><tr><td></td><td>onArray[4]</td><td>1</td><td>Decimal</td><td>USINT</td></tr></table> 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.		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.

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

Use a CIP Generic MSG to Disable SNMP on the Controller

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

1. Add an MSG instruction to your program.

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

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

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 'Service Code' is '4c' (Hex). The 'Instance' is '1'. The 'Class' is 'f5' (Hex). The 'Attribute' is '0' (Hex). The 'Source' is 'offArray'. The 'Source Length' is '5' (Bytes). The 'Destination Element' is empty. There is a 'New Tag...' button. 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), and 'Error Text'. There is a 'Timed Out' checkbox. At the bottom right are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Table 23. Enable SNMP

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

Field	Description																		
Class	f5																		
Attribute	0																		
Source Element	Controller tag of USINT[5] data type. In this example, the controller tag is named offArray and must match the following graphic. <table><tr><td>└─ offArray</td><td>{...} Decimal</td><td>USINT[5]</td></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> IMPORTANT: The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP is not disabled.	└─ 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.

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

Trusted Slots on the Controller

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

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

To meet IEC-62443-4-2 SL 1 certification requirements, you must not configure Trusted slots on the controller and instead use [CIP Bridging Control on page 145](#).

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

The following rules apply to Trusted slots:

- The firmware revisions of the physical modules in the Trusted slots must be compatible with the firmware revisions and electronic keying options that are configured in the I/O tree of the project. For compatibility, see [Electronic Keying on page 109](#).
- All communication is Trusted from the module as long as there is not a fault or keying mismatch.
- If no module is configured in the I/O tree for the respective Trusted slot, then all communication is Trusted regardless of which module is physically present.

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

Restrict Communication Except Through Selected Slots

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

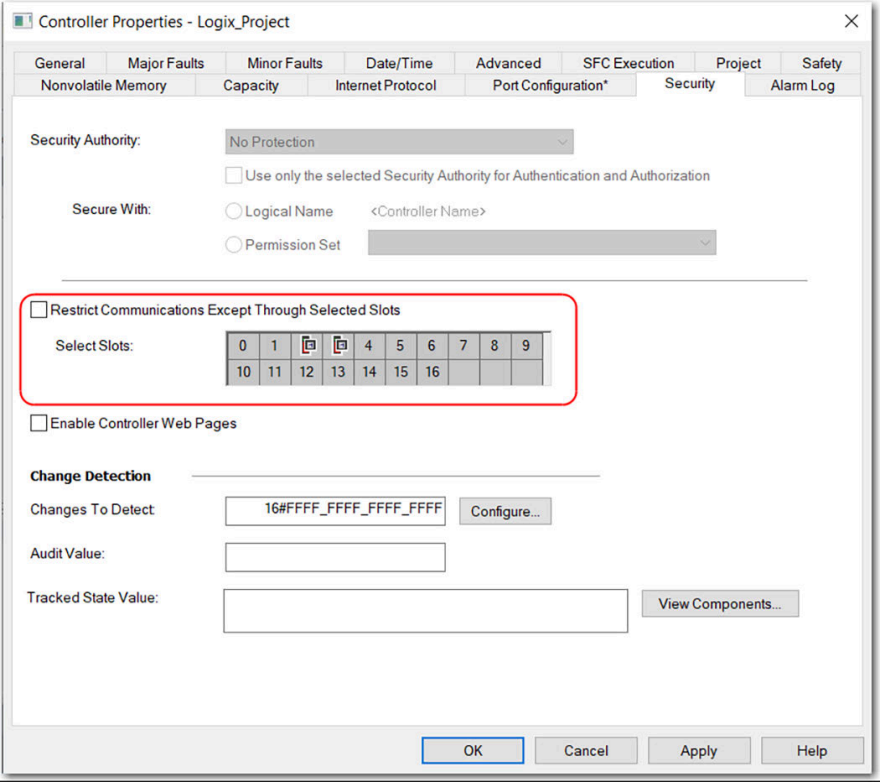
IMPORTANT: When this checkbox is selected, communication is restricted through a front Ethernet port and firmware updates are restricted to Trusted slots when using AutoFlash or ControlFLASH Plus® software. Support is restricted for tools that require access to restricted data through Class 3 connections.

Select Slots

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

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

Figure 24. Selected Slot Options



Manage Controller I/O Connections

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

- A wide variety of digital, analog, and specialty I/O modules support the following features:
 - Field-side diagnostics
 - Electronic fusing
 - Individually isolated inputs/outputs
 - Timestamping of inputs
 - Scheduling of outputs
 - Event detection of specific input patterns
 - Safety features that are TÜV certified up to SIL 3, PLe, Cat. 4
- Removable terminal blocks (RTBs) or 1492 wiring systems are required for I/O modules.
- 1492 PanelConnect™ modules and cables can be used to connect input modules to sensors.

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).
- Configuration signature.
- Reaction time limit.

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

For instructions about how to add I/O to the I/O configuration in a controller project, see the user manual for your I/O device.

Add to the I/O Configuration While Online

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

IMPORTANT: To add I/O modules when the controller is online, the controller switch 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.

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.

- 1756 controllers
- 1756 DeviceNet® bridges
- 1756 EtherNet/IP™ modules
- Compact 5000® I/O EtherNet/IP™ adapters and I/O modules
- FLEX 5000® EtherNet/IP™ adapters and I/O modules
- PointMax® EtherNet/IP™ adapters and I/O modules
- 1756 I/O modules 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

Electronic Keying

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

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

The following Electronic Keying options are available.

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

Keying Option	Description
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. IMPORTANT: For safety I/O devices, do not use Disable Keying.
Exact Match	Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.

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

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

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

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

Connect to Local I/O

The ControlLogix chassis affects how many local I/O modules you can use. Several ControlLogix chassis sizes are available to suit your configuration requirements.

Table 24. ControlLogix, ControlLogix-XT, and ControlLogix-ZXT Chassis and Slots

Chassis	Slots
1756-A4	4
1756-A7, 1756-A7XT, 1756-A7ZXT	7
1756-A10, 1756-A10XT, 1756-A10ZXT	10
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 I/O modules to the backplane of the controller. There are two methods to add I/O modules to the local chassis:

- Discover modules
- Add new modules

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

For instructions about how to add I/O to the I/O configuration in a controller project, see the user manual for your I/O device.

Connect to Remote I/O

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

- 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 5034 PointMax® I/O or 5094 FLEX 5000® I/O.
- On-Machine™ I/O families such as ArmorBlock® I/O

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

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

Connect to Safety I/O

Before you use safety I/O, do the following:

- Read, understand, and follow all safety information in the product documentation for those products.
As the range of products using the CIP Safety™ protocol continues to expand, there are variations to the typical safety I/O configuration steps. Product specific procedures and requirements can include the following:
 - Reset of ownership
 - Setting the safety network number
 - Configuration signature generation
 - Requested packet interval (RPI) limits
 - Device-specific configuration settingsFor more information, see the user manual for your I/O device.
- Commission all devices with a node or IP address and communication rate before their installation on a safety network.

Network Address Translation

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

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

With CIP Safety™, the IP address of the device is part of the unique node reference that is part of the protocol. The device compares the IP address portion of the unique node reference in CIP Safety™ packets to its own IP address, and rejects any packets where they do not match. The

IP address in the unique node reference must be the NAT'ed IP address. The controller uses the translated address, but the CIP Safety™ protocol requires the actual address of the device.

If you use NAT to communicate with a CIP Safety™ device, use the Advanced Ethernet Settings when you configure the IP address and enable 'Module and controller communicate through Network Address Translation (NAT) devices.'

Safe State

Safety I/O has most of the attributes of standard I/O except it features mechanisms that are certified to SIL 2 or SIL 3 for data integrity. A safety input is a combination of produced and consumed safety tags, mapped safety inputs, and inputs from safety modules.

Before you use safety I/O, do the following:

- Read, understand, and follow all safety information in the product documentation for those products.
- Commission all devices with a node or IP address and communication rate before their installation on a safety network.

Safety I/O devices, like sensors and actuators, can be connected to safety input and output modules. The controller monitors and controls the devices. For safety data, I/O communication is performed through safety connections by using the CIP Safety™ protocol. Safety logic is processed in the controller.



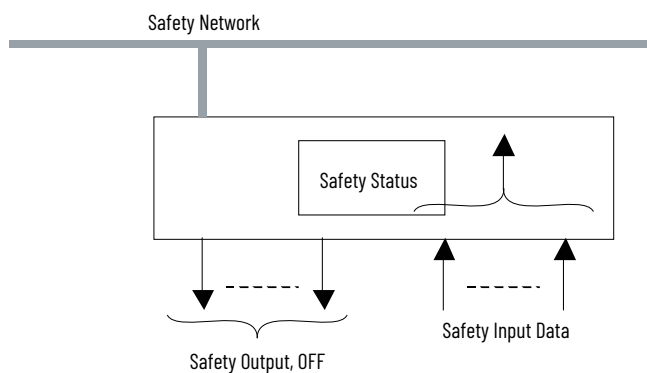
ATTENTION:

- The safe state of the outputs is defined as the off state.
- The safe state of the module and its data is defined as the off state.
- Use safety I/O modules only in applications where the off state is the safe state.

Safety I/O treats the following as the safe state:

- Safety outputs: OFF
- Safety input data to controller: OFF

Figure 25. Safe State



IMPORTANT: If you inhibit a safety module from transitioning to a safe state when a fault occurs because an I/O connection is lost, you accept responsibility for any consequences that result from your decision to inhibit. We recommend that you use other means to maintain the safe state if you inhibit the safety module from transitioning to a safe state.

Configuration Signature and Ownership

One controller owns each safety I/O device in a non-redundant safety system. Multiple controllers and multiple safety I/O devices can be used in chassis or on networks. When a controller owns an I/O device, it stores the configuration data that you define for that device. This configuration controls how the devices operate in the system.

From a control standpoint, one controller controls safety output devices. One controller also owns each safety input device. However, safety input data can be shared (consumed) by multiple controllers.

Table 25. Configuration Signature and Ownership

Configuration	Description
Configuration Signature	Each safety device has a unique configuration signature that defines the module configuration. The configuration signature includes the following: • ID number • Date • Time The configuration signature is used to verify a module’s configuration. The signature can only be considered “verified” (and configuration locked) after user testing.
Configuration Ownership	The connection between the owner-controller and the safety module is based on the following: • Safety module number • Safety module network number • Controller node or slot number • Controller safety network number • Path from the controller to the safety module • Configuration signature If any differences are detected, the connection between the owner-controller and the safety module is lost, the yellow yield icon appears in the controller project tree.

When a controller owns the I/O module configuration, other controllers can listen to the input module. In this case, the module configuration signature in the Logix Designer project for any listening controller must match the one in the owner-controller project.

- If the safety module is configured for inputs only, you can copy and paste the configuration signature from one project to the other.
- If the safety module has safety outputs, for example, the configuration signature parameter is disabled.

Safety Rating Considerations

Input and output configurations can affect safety ratings.

Table 26. Safety Rating Considerations

Configuration Type	Description
Input	Some safety input modules have safety inputs that can be configured as single or dual (Equivalent or Complement) point operation types. The selected type configures the safety module to view the inputs individually or as a pair: - A single configuration is appropriate for single channel inputs or dual channel inputs that are monitored by a dual channel safety instruction like the Dual Channel Stop (DCS). - A dual configuration configures dual channel discrepancy checking to take place at the module level. The channel data from the input module is sent to the controller as either the safe state or energized state. For example, equivalent inputs are either both low (0) or both high (1). The method of monitoring discrepancy has no impact on the safety rating. The main effect is the availability of diagnostic information: - Module level diagnostics—Status indicators, input status bit, and application code can be written to message the I/O module to monitor 1 bit for a discrepancy fault. - Dual channel instruction diagnostics—Fault codes include channel-specific discrepancy and whether the cause of a discrepancy is a delay or a change in state to a specific channel.
Output	For output modules, sourcing safety outputs can be configured as point operation type single or dual. The selected type configures the safety module to treat the outputs individually or as a pair: - A single configuration allows the outputs to turn on and off individually and to fault independently. - A dual configuration verifies that safety task logic operates both outputs as a pair. If one output has a module fault, the other output goes to the safe state. Bipolar outputs have no configuration for point operation type and must operate as a sinking sourcing pair. The point operation type affects the PFH safety rating of the module. The PFH is the average frequency of a dangerous failure per hour.

Connect to Replacement Safety I/O

The process for making a connection to replacement safety I/O is dependent upon multiple factors including the following:

- Node address
- Electronic keying compatibility
- Whether the I/O module configuration is empty (out-of-box) or previously configured
- The Automatic Configuration setting for the safety controller



ATTENTION: During replacement or functional testing of a device, the safety of the system must not rely on any portion of the affected device.

The electronic keying configuration affects the process for replacing safety I/O modules. Carefully consider the implications of each of the following electronic keying options.

Table 27. Electronic Keying Settings

Keying Setting	Description	I/O Replacement Consideration
Compatible Module	Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has the following characteristics: - Same catalog number - Same or higher major revision	To maintain the safety signature, the replacement module must meet Compatible Module requirements.

Table 27. Electronic Keying Settings (continued)

Keying Setting	Description	I/O Replacement Consideration
	- Minor revision as follows: - If the major revision is the same, the minor revision must be the same or higher. - If the major revision is higher, the minor revision can be any number.	
Disable Keying	Indicates that the keying attributes are not considered when attempting to communicate with a device. With Disable Keying, communication can occur with a device other than the type specified in the project. 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.	Many safety devices do not have a Disable Keying option. Disabled Keying is not recommended for safety applications.
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.	- To maintain the safety signature, the replacement module must be Exact Match. - After a firmware change, keying in the safety application must be updated. Updating cannot be done without removing the controller safety signature. - Exact Match is often used to meet specific industry requirements.

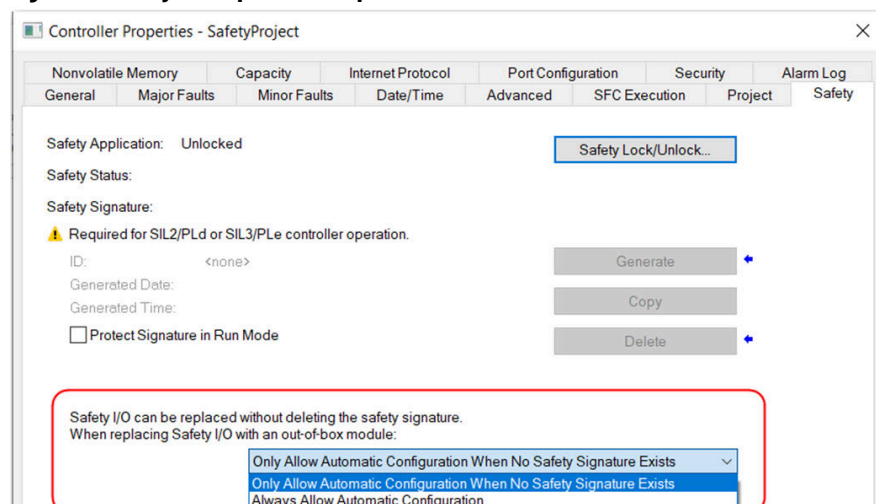
Automatic configuration enables the safety controller to establish a connection with replacement safety I/O without online user interaction. Automatic configuration is enabled when there is no controller safety signature. Allowing automatic configuration with no safety signature facilitates commissioning and maintenance activities when the safety controller is not being used for SIL-rated functions. Following I/O replacement, you must validate proper operation before using SIL-rated functions.

Two options for I/O device replacement are available on the Safety tab of the Controller Properties dialog.

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

Choosing an automatic configuration setting requires an understanding of the safety network topology and the intended use of the safety system during I/O replacement.

Figure 26. Safety I/O Replacement Options



Only Allow Automatic Configuration When No Safety Signature Exists

This option instructs the safety controller to configure a safety device when the safety task does not have a safety signature, and the replacement device is in an out-of-box condition with no safety network number.

If the controller has a safety signature, the safety controller automatically configures the replacement safety I/O device if the following are true:

- The device already has the correct safety network number.
- The device electronic keying is correct.
- The node or IP address is correct.

To set the proper safety network number (SNN) when a controller safety signature exists, manual action is required to download the proper SNN:

1. Go online with the safety controller.
2. Open the Module Properties dialog box.
3. On the General tab, click Browse (...) next to the safety network number.
4. Click Set to write the SNN to the module manually.
5. Verify that the Network Status (NS) indicator is alternating red/green on the correct device.
6. Click Yes on the confirmation dialog box to set the SNN and accept the replacement device.
7. Follow your company-prescribed procedures to functionally test the replacement I/O device and system.

For more information, follow the safety I/O device replacement procedure in the controller user manual.

Always Allow Automatic Configuration

The controller attempts to configure a replacement safety I/O device automatically if the device is in an out-of-box condition. When a safety network number does not exist in the replacement safety device, and the node number and I/O device keying matches the configuration of the controller.



ATTENTION: Select the Always Allow Automatic Configuration option only if the entire routable 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. The routable safety control system includes any device that can have safety connections opened on it by the controller.

If other parts of the safety control system are being relied upon to maintain SIL 2 or SIL 3, make sure that the Always Allow Automatic Configuration option is not selected.

It is your responsibility to implement a process to make sure that proper safety functionality is maintained during device replacement.



ATTENTION: To place a device in the out-of-box condition on a safety network when the Always Allow Automatic Configuration option is selected, follow the device replacement procedure in the controller user manual.

Automatic Configuration Use Cases

Consider the following examples of when to use a particular automatic configuration setting.

Only Allow Automatic Configuration When No Safety Signature Exists	Always Allow Automatic Configuration
- Multi-zone safety system where I/O replacement is required in one zone, while other zones maintain SIL functionality. - Multiple controllers with safety I/O on the same routable network.	- The safety system provides no safety function during I/O replacement: - Use of energy isolation or other application-specific procedure - Other application-specific safeguards are in place - The network for safety I/O communication is isolated from external safety devices.

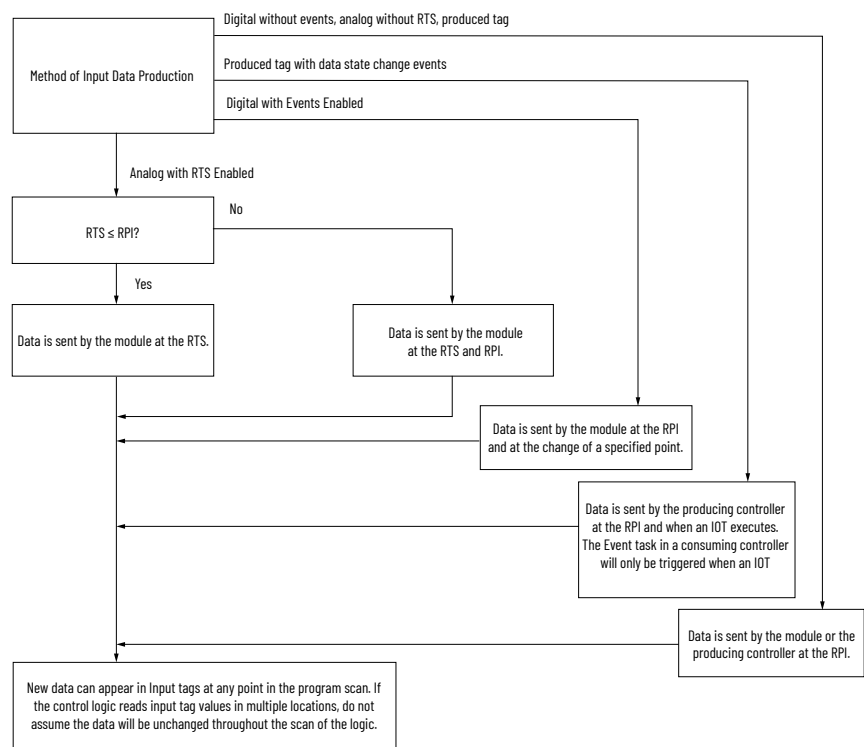
Determine When I/O Data Is Updated

ControlLogix controllers update data asynchronously with the execution of logic.

Input Data Update Flowchart

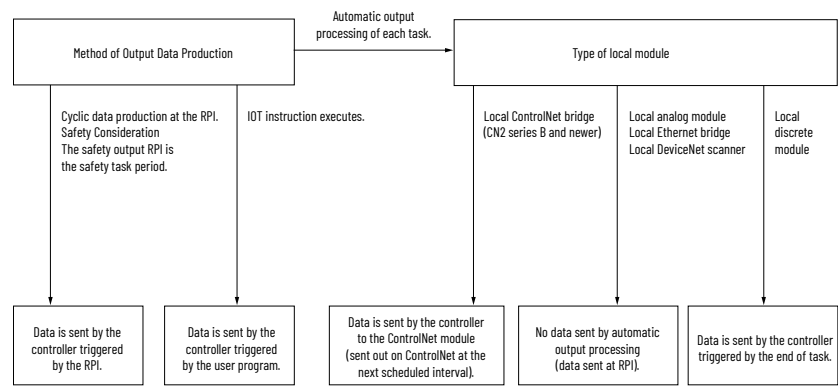
Safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution.

Figure 27. Input Data Update



Output Data Update Flowchart

Figure 28. Output Data Update



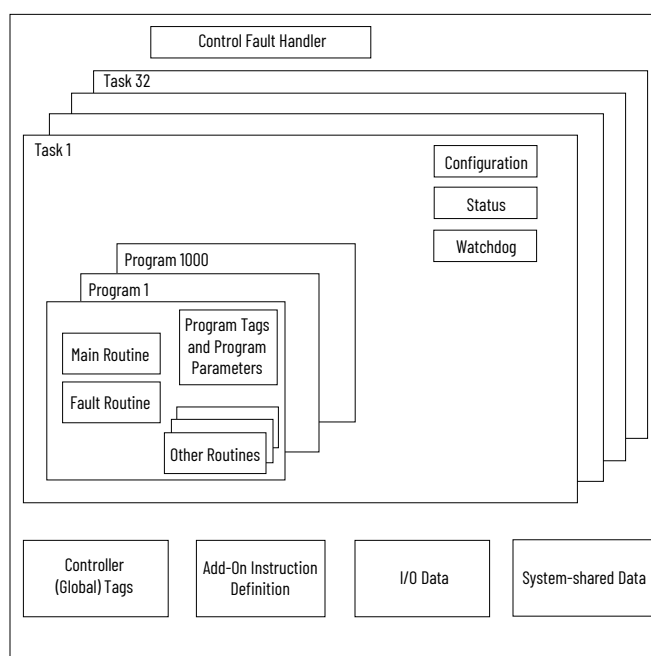
Develop Standard Applications

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

Application elements include the following:

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

Figure 29. 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 30. Task Within a Control Application

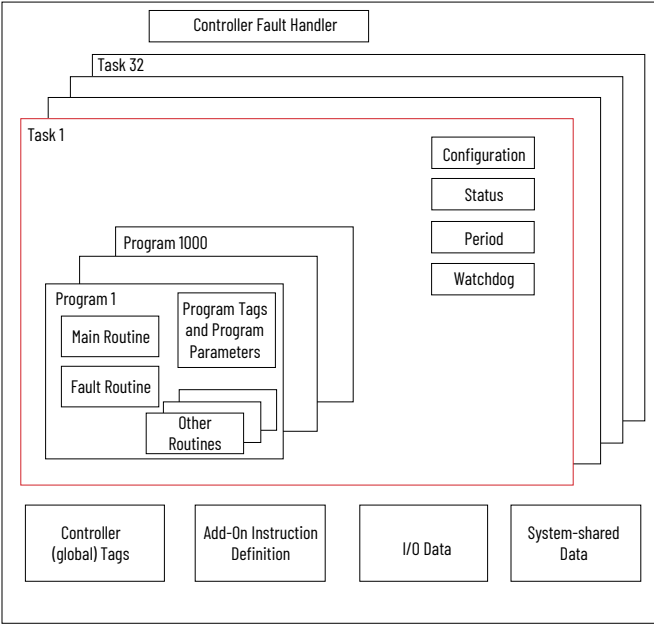
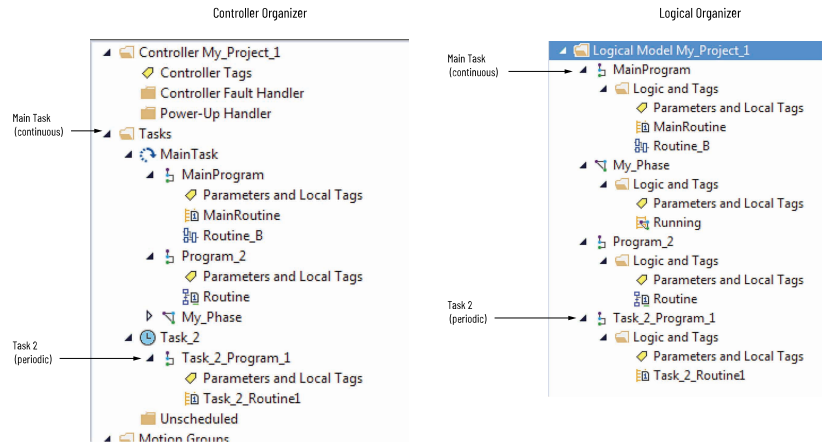
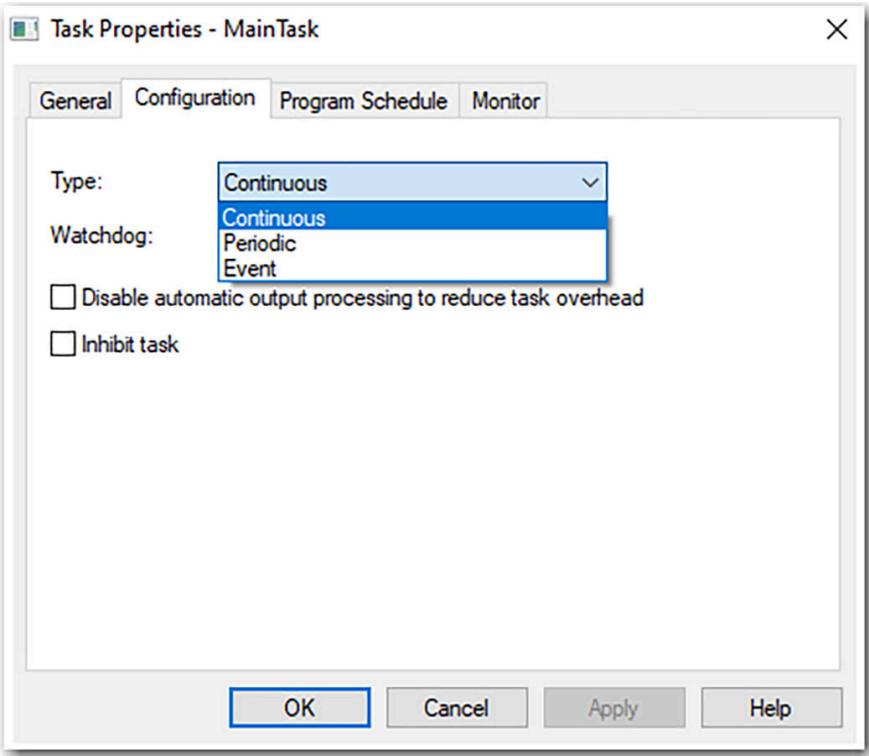


Figure 31. Tasks in the Controller Organizer and Logical Organizer



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

Figure 32. Configure the Task Type



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

Table 28. Task Types and Execution Frequency

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

Table 28. Task Types and Execution Frequency (continued)

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

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

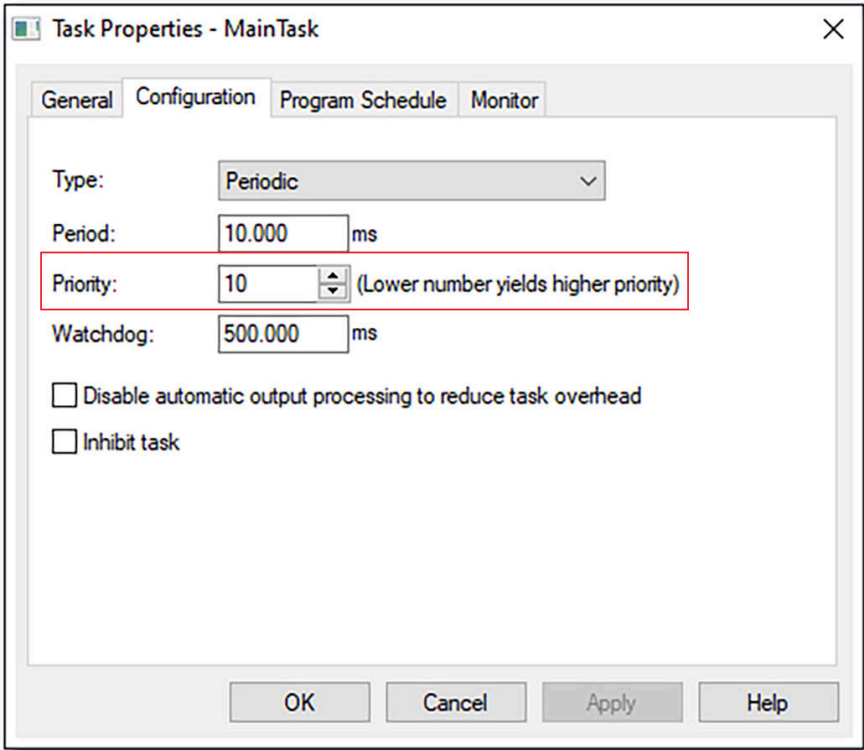
A task can have up to 1000 programs, each with its own executable routines and program-scoped tags. Once a task is triggered (activated), the programs that are assigned to the task execute in the order in which they are grouped. Programs can appear only once in the Controller Organizer and multiple tasks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

Task Priority

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

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

Figure 33. Configure the Task Priority



Programs

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

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

Each program contains the following:

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

Figure 34. Program Within a Control Application

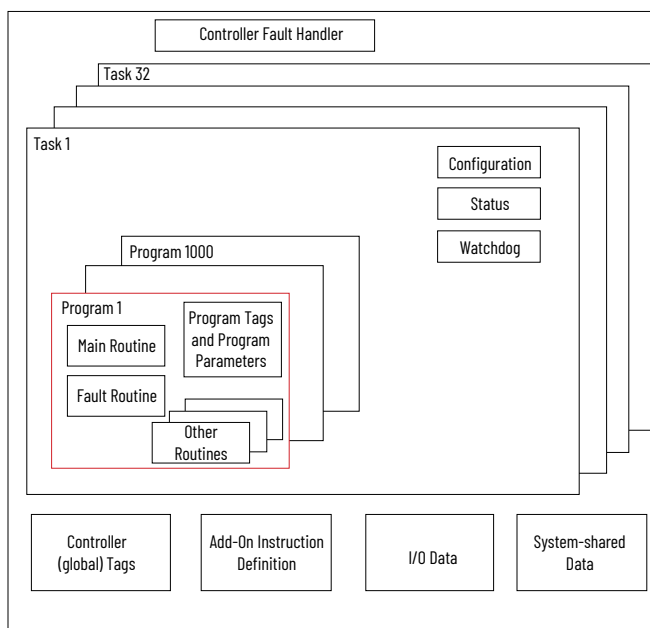
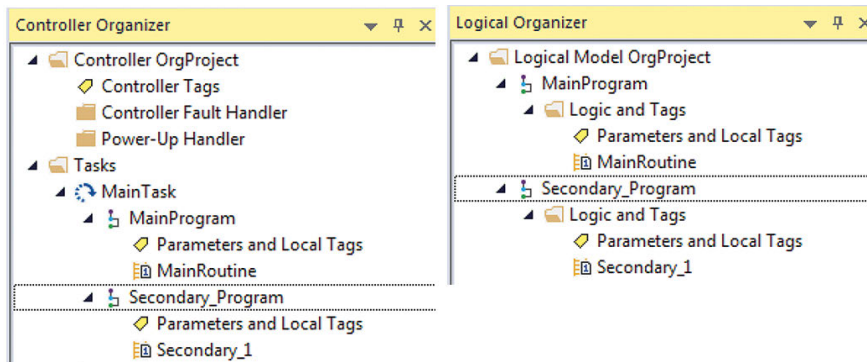


Figure 35. Programs the Controller Organizer and Logical Organizer



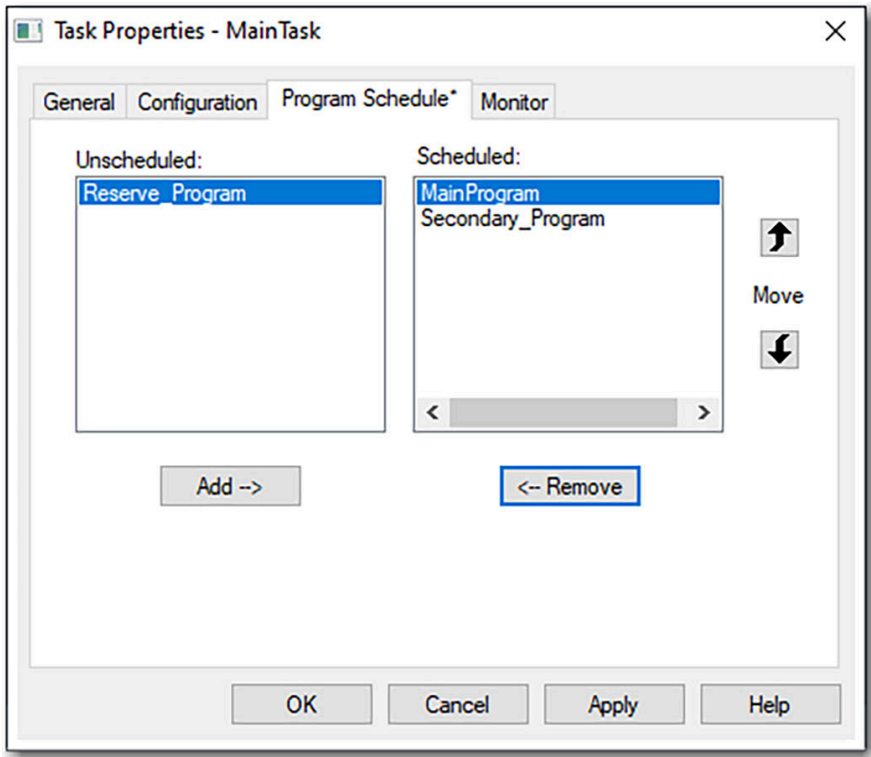
Scheduled and Unscheduled Programs

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

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

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

Figure 36. Schedule an Unscheduled Program



Routines

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

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

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

Figure 37. Routines in a Control Application

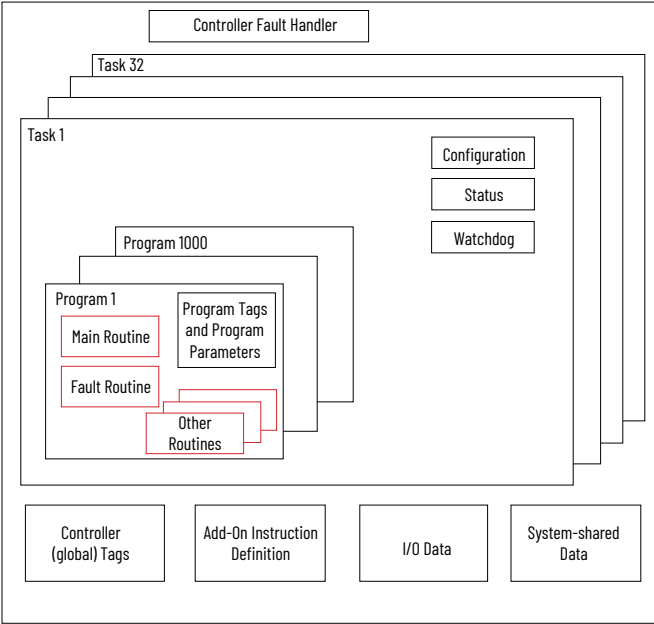
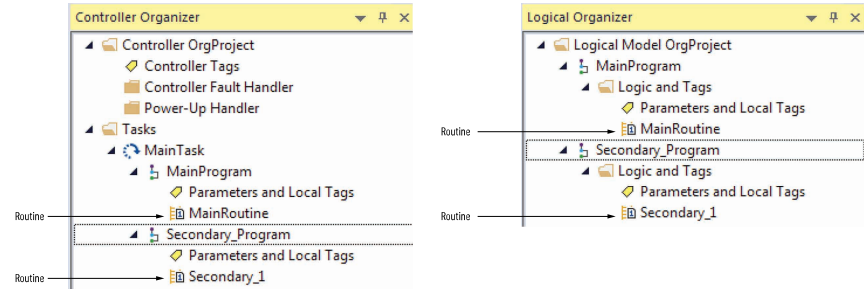


Figure 38. Routines in the Controller Organizer and Logical Organizer



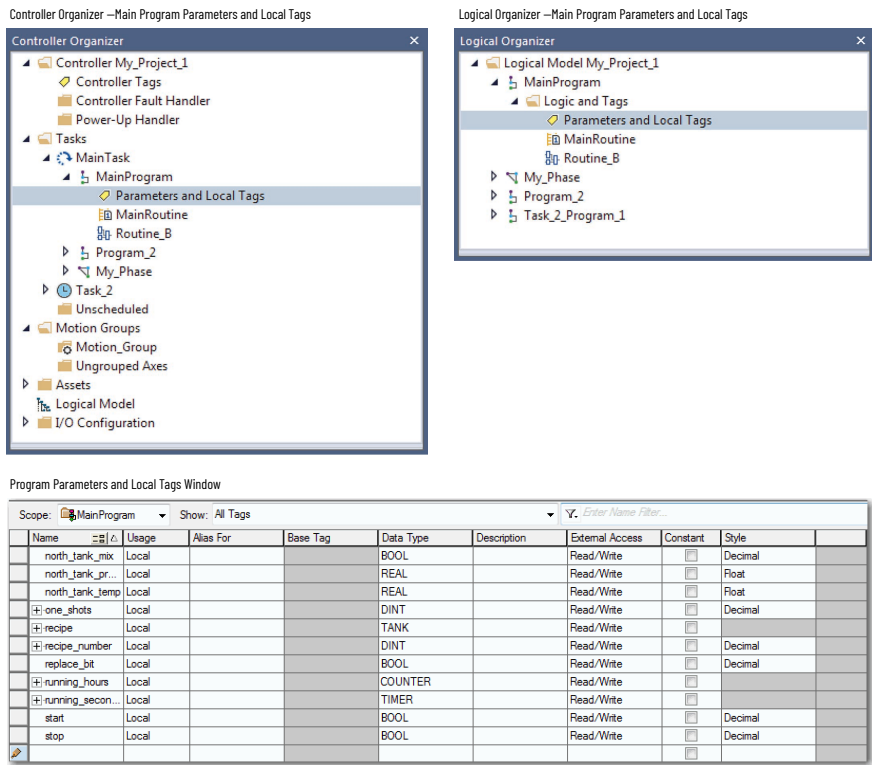
Parameters and Local Tags

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

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

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

Figure 39. Parameters and Local Tags



Program Parameters

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

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

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

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

Programming Languages

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

Table 29. Supported Programming Languages

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

Table 29. Supported Programming Languages (continued)

Language	Is best used in programs with
	Machine interlocking. Operations that service or maintenance personnel have to interpret to troubleshoot the machine or process. IMPORTANT: Ladder Diagram is the only programming language that can be used with the Safety Task on ControlLogix® 5590 controllers.
Function Block Diagram (FBD)	Continuous process and drive control. Loop control. Calculations in circuit flow.
Sequential Function Chart (SFC)	High-level management of multiple operations. Repetitive sequence of operations. Batch process. Motion control that uses structured text. State machine operations.
Structured Text (ST)	Complex mathematical operations. Specialized array or table loop processing. ASCII string handling or protocol processing.

For more information, see the Logix 5000 Controllers Common Procedures Programming Manual, publication [1756-PM001](#).

Add-On Instructions

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

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

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

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

Table 30. 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.

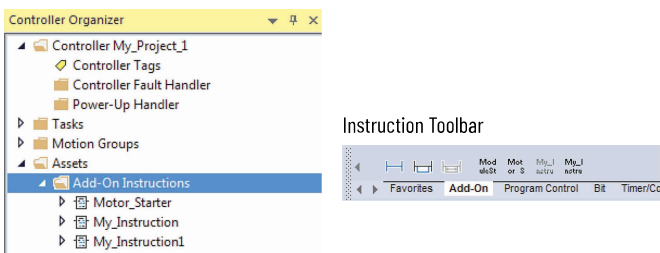
Table 30. Add-On Instruction Capabilities (continued)

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

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

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

Figure 40. Add-On Instructions Example



Extended Properties

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

Table 31. Extended Properties

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

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

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

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

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

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

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

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

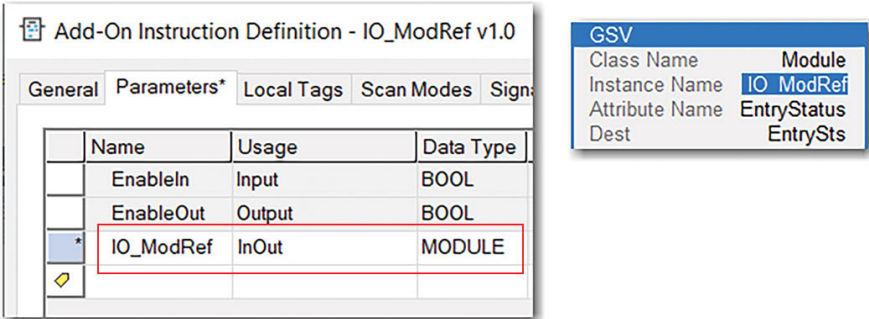
Module Object

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

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

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

Figure 41. Module Reference Parameter



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

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

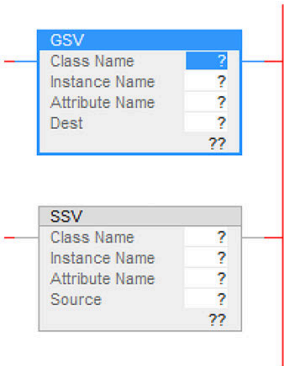
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Controller Status

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

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

Figure 42. GSV and SSV Instructions for Monitoring and Setting Attributes



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

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

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

I/O Connections

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

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

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

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

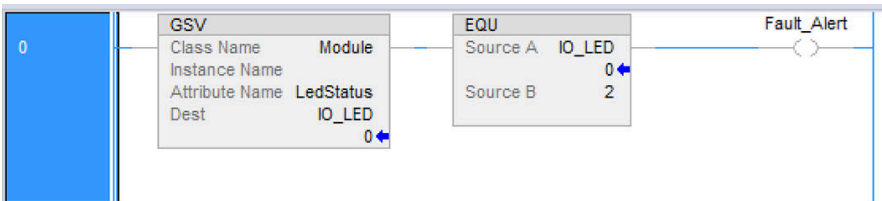
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#).

I/O Communication Timeout

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

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

Figure 43. GSV Used to Identify I/O Timeout



IMPORTANT: Safety Consideration

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

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

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

I/O Module Connection Faults

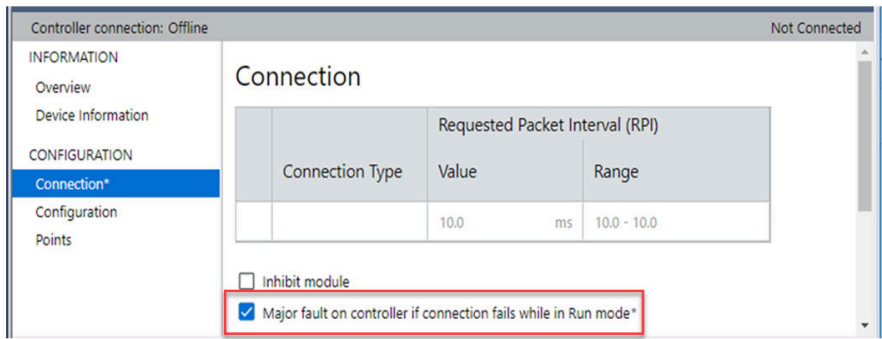
Depending on your application, you may want an I/O connection error to cause the Controller Fault Handler to execute. To do so, set the module property that causes a major fault to result from an I/O connection error. The major fault causes the execution of the Controller Fault Handler.



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

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

Figure 44. I/O Connection Fault Causes Major Fault



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

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

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

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

Sample Controller Projects

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

Figure 45. Sample Projects



Develop Motion Applications

The controllers support Integrated Motion on an EtherNet/IP™ network and digital drives interfaces that include connected drives. The controllers support any combination of CIP™, Virtual, and Consumed axes. You can add all axes to one Motion Group, and you can assign any combination of axes to different axis update schedules.

Table 32. Supported Axes and Drives

Controller	Total Number of Supported Axes	Support Drive Types
ControlLogix® 5590	512	- Integrated Motion on an EtherNet/IP™ network drives - EtherNet/IP™ connected drives - 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.



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

For more information, see these publications:

- Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication [MOTION-UM003](#).
- Integrated Motion on the EtherNet/IP Network Reference Manual, publication [MOTION-RM003](#).
- SERCOS and Analog Motion Configuration and Startup User Manual, publication [MOTION-UM001](#).

You can associate Integrated Motion axes to any appropriate drive, regardless of whether the communications path to the drive is via the embedded Ethernet port, or over the 1756 backplane via an Ethernet bridge, such as a 1756-EN2T.

The configuration process varies, depending on your application and drive selection. The following are general steps to configure a motion application.

1. Create a controller project.
2. Select the type of drive.
3. Create axis tags as needed.
4. Configure the drive.
5. Create axes as needed.

Program Motion Control

The controller provides a set of motion control instructions for your axes:

- The controller uses these instructions just like the rest of the Logix 5000® instructions.
- Each motion instruction works on one or more axes.

- You can program by using motion control instructions in these programming languages:
 - Ladder Diagram (LD)
 - Structured Text (ST)
 - Sequential Function Chart (SFC)
- Each motion instruction needs a motion control tag. The tag uses a **MOTION_INSTRUCTION** data type and stores the information status of the instruction.

For more information, see the Logix 5000 Controller Motion Instructions Reference Manual, publication [MOTION-RM002](#).



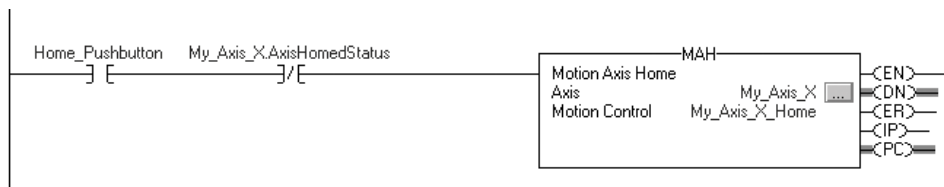
ATTENTION: Use each motion control tag in only one motion instruction. Unintended operation can result if you reuse the same motion control tag in other motion instructions, or if you write to any of the motion control tag elements.

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

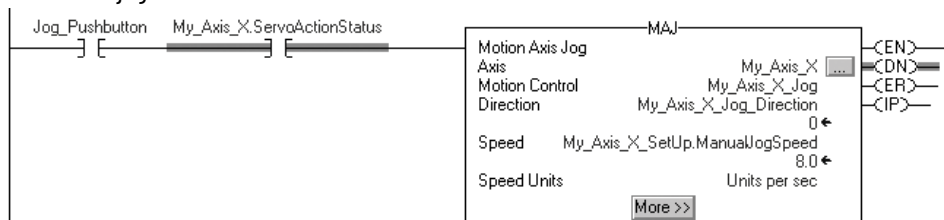
If Initialize_Pushbutton = on and the axis = off (My_Axis_X.ServoActionStatus = off) then the MSO instruction turns on the axis.



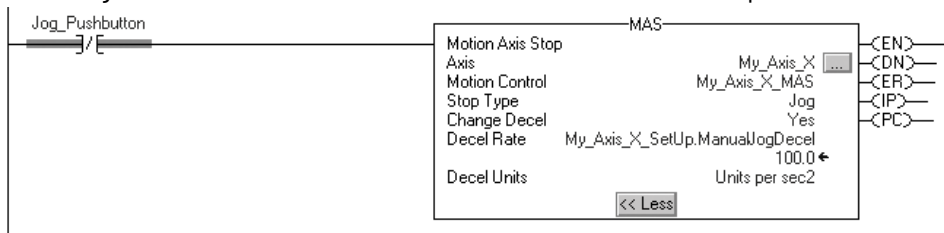
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off) then the MAH instruction homes the axis.



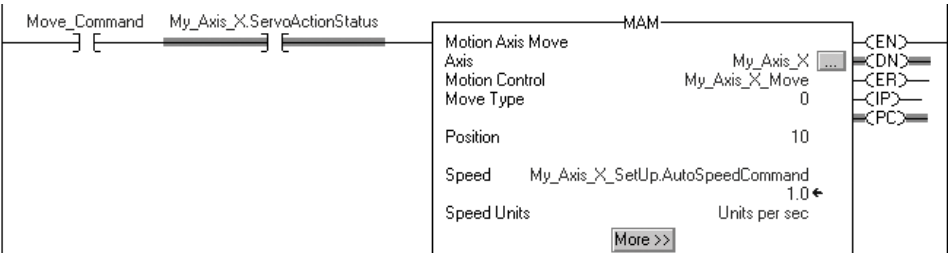
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAJ instruction jogs the axis forward at 8 units/second.



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

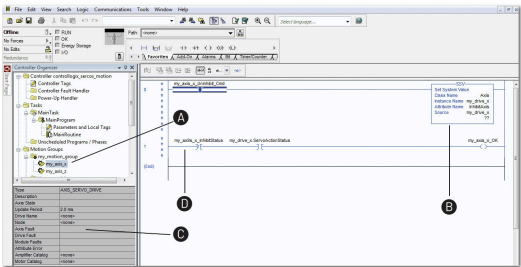


Obtain Axis Information

You can obtain axis information by using these methods:

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

Figure 46. Obtain Axis Information



Develop Secure Applications

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

Table 33. IEC 62443-4-2 SL 1-certified Controllers

Controller	Firmware Revision
ControlLogix® 5590 controllers	38 or later

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

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

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

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

Table 34. Security Additional Resources

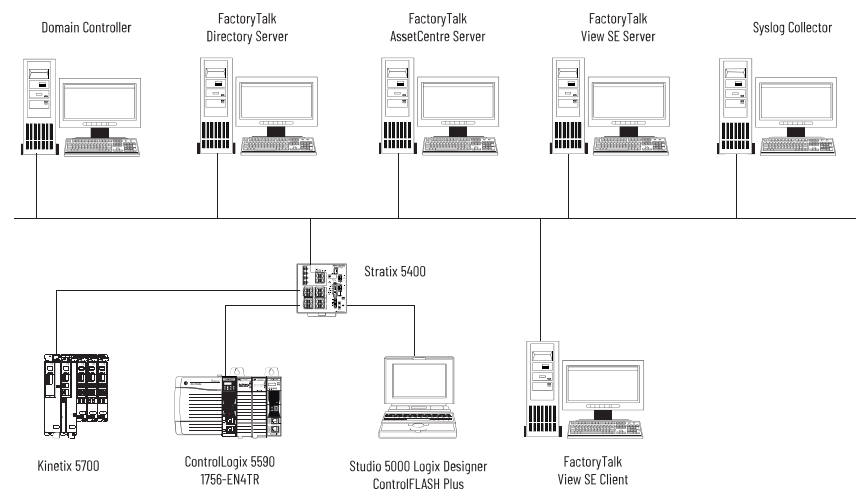
Resource	Description
Security Design Guide Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct vulnerability assessments, implement Rockwell Automation® products in a secure system, harden the control system, manage user access, and dispose of equipment.
Logix 5000 Controllers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

Controller Security Features

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

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

Figure 47. Secure Architecture Environment



Requirements for Identification and Authorization

Table 35. Requirements for Identification and Authorization

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® Security software Studio 5000 Logix Designer® application	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. - The Logix Designer application enforces the policy based on the access policies that are provided to it by FactoryTalk® Security for the software authenticated user. Once authenticated, the Logix Designer application acts as your interface to the controller. This applies to all protected CIP™ communications to the controller, whether from Ethernet, backplane, or USB. - The FactoryTalk Services Platform offers feature access control to manage user access to product features such as controller download, project import, project create, and firmware update. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
(Safety-enabled controllers only). Access control to generate and delete the safety signature	May be required based on system design, threat model, and risk assessment.	Configure FactoryTalk® Security to restrict access to generate and delete the safety signature. To configure FactoryTalk Security permissions, see the Configure System Security Features User Manual, SECURE-UM001 .
(Safety-enabled controllers only). Access control to safety-lock and safety-unlock actions	May be required based on system design, threat model, and risk assessment.	Configure FactoryTalk® Security to restrict access to safety-lock and safety-unlock actions. To configure FactoryTalk Security permissions, see the Configure System Security Features User Manual, SECURE-UM001 .

Requirements for Use Control

Table 36. Requirements for Use Control

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
Studio 5000 Logix Designer® application	May be required based on system design, threat model, and risk assessment.	Configure the controller project in the Logix Designer application to use these user access methods: - License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. - License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. - Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. - The Logix Designer application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag. For more information, see Logix 5000 Controllers Security Programming Manual, 1756-PM016.
FactoryTalk® Security software Studio 5000 Logix Designer® application	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. - The Logix Designer application enforces the policy based on the access policies that are provided to it by FactoryTalk® Security for the software authenticated user. Once authenticated, the Logix Designer application acts as your interface to the controller, including all protected CIP™ communication to the controller, whether from Ethernet, backplane, or USB. - The FactoryTalk® Services Platform offers feature access control to manage user access to product features, such as controller download, project import, project create, and firmware update. - In FactoryTalk® Security, define which users can change controller modes and download projects to the controller. - Security authority binding restricts the controller to a specific FactoryTalk® Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. For more information, see Configure System Security Features User Manual, SECURE-UM001.
Controller mode switch position	May be required based on system design, threat model, and risk assessment.	Place the mode switch in the RUN position to help prevent unauthorized remote configuration changes to the controller and restrict some communication services. IMPORTANT: Do not apply a new security policy while the controller is in RUN mode. RUN mode does not help prevent updates to the security policy, and a policy change has the potential to disrupt a running control system.
Disable the controller Ethernet ports	May be required based on system design, threat model, and risk assessment.	The Ethernet ports are enabled by default. Disable the Ethernet ports if required by the system design, threat model, or risk assessment. For more information, see Disable the Ethernet Port on the Port Configuration Tab on page 151 and Disable the Ethernet Port with an MSG Instruction on page 152.
Disable Simple Network Management Protocol (SNMP) on the controller	May be required based on system design, threat model, and risk assessment.	SNMP is disabled by default. If SNMP has been enabled, disable SNMP if required by the system design, threat model, or risk assessment. For more information, see Use a CIP Generic MSG to Disable SNMP on the Controller on page 104.

Table 36. Requirements for Use Control (continued)

Security Component	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 Disable CIP Security Ports via FactoryTalk Linx on page 154 and Disable CIP Security Ports via a CIP Generic MSG Instruction on page 155 .
Disable the controller USB port	May be required based on system design, threat model, and risk assessment.	The USB port on the controller is enabled by default. Disable the USB port if required by the system design, threat model, or risk assessment. For more information, see Disable the Controller USB Port on page 157 .
Disable the controller SD card	May be required based on system design, threat model, and risk assessment.	The SD card is enabled by default. Disable the SD card if required by the system design, threat model, or risk assessment. For more information, see Disable the Controller SD Card on page 159 .
Disable controller webpages	May be required based on system design, threat model, and risk assessment.	Controller webpages for diagnostics are read-only. With Studio 5000 Logix Designer® application version 33 or later, controller webpages are disabled by default. Disable the controller webpages if required by the system design, threat model, or risk assessment. For more information, see Disable Controller Web Pages on page 165 .

Requirements for System Integrity

Table 37. Requirements for System Integrity

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	The FactoryTalk® AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes based on FactoryTalk® Security settings. This server functionality assists with diagnostics and troubleshooting and reduces maintenance time for production assets. 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® software	Yes	Use ControlFLASH Plus® software to update controller firmware. Digitally signed firmware files have a .DMK (Device Management Kit) extension. ControlFLASH™ software authenticates the origin of a DMK file and validates the file before downloading in the device.
Studio 5000 Logix Designer® application	Yes	You can generate a signature on an Add-On Instruction. This signature seals (encrypts) the Add-On Instruction to help prevent modification.
Controller firmware update	Yes	To meet IEC-62443-4-2 SL 1 security requirements, you must use a certified version of the controller firmware. We recommend that you use the latest minor revision of your firmware. The controller is designed such that: - You cannot update firmware when the mode switch is in the RUN position. - You cannot go online with a controller that is in a firmware update process.

Table 37. Requirements for System Integrity (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		For more information, see Controller Firmware and Logix Designer Application Compatibility on page 32 .
CIP™ Bridging Control	May be required to maintain network segmentation.	CIP™ Bridging Control can be used to isolate secure and unsecure communication. For more information, see CIP Bridging Control on page 145 .
User-definable major controller faults	May be required based on system design, threat model, and risk assessment.	If your application requires a major fault in addition to those already monitored by the controller, define a predetermined state with a major fault so that outputs are off. For more information, see Configure User-definable Major Faults on page 144 .
(Safety-enabled controllers only). Safety signature	Yes for SIL 2 or SIL 3 configuration.	Safety-enabled controllers use a safety signature to verify the integrity of a safety application. The safety signature must be applied on a SIL 2/PLD or SIL 3/PLC safety-enabled controller to perform automated background integrity checks on the safety application. We recommend that you record and store the safety signature in a separate location to verify its integrity during audits or when tampering is suspected.

Requirements for Data Confidentiality

Table 38. Requirements for Data Confidentiality

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® Security software	Yes	Configure FactoryTalk® Security to define policies, user groups, and other permission sets. - The FactoryTalk® Services Platform offers feature access control to manage user access to product features such as controller download, project import, project create, and firmware update. - In FactoryTalk® Security, define which users can change controller modes and download projects to the controller. - Security authority binding restricts the controller to a specific FactoryTalk® Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
FactoryTalk® Policy Manager software	Yes	Use the FactoryTalk® Policy Manager software to define a secure data transport over an EtherNet/IP™ network to the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001 .
License-based source and execution protection	May be required based on system design, threat model, and risk assessment.	Configure licenses to manage access to controller source logic and execution of that logic. These licenses are not enabled by default. - License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. - License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. - License-based source protection cannot restrict access to safety logic and safety Add-On Instructions.

Table 38. Requirements for Data Confidentiality (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		For more information, see License-based Source and Execution Protection on page 145 .
Access to tag data	May be required based on system design, threat model, and risk assessment.	Configure the following attributes in the Logix Designer application to control access to tag data: - External Access attribute—Controls how external applications can access tags. - Constant attribute—Determines if controller logic can change a tag.
SD card encryption	May be required based on system design, threat model, and risk assessment.	If your system allows for microSD memory card use, the load process to the memory card encrypts and digitally signs the project by using the controller key. The memory card itself is not encrypted. When you save (load) firmware to the memory card, the process stores encrypted firmware and certificates on the memory card. 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 memory card. This can help prevent against potential loss of controller logs before FactoryTalk® AssetCentre can read them. For more information, see Use the Memory Card on page 87 .

Requirements for Restricted Data Flow

Table 39. Requirements for Restricted Data Flow

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

Requirements for Timely Response to Events

Table 40. Requirements for Timely Response to Events

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	Configure and use the following: - Audit log accessibility - Continuous monitoring For more information, see the following: - Configure System Security Features User Manual, SECURE-UM001. - System Security Design Guidelines Reference Manual, SECURE-RM001
Syslog collector	Yes, if not using FactoryTalk® AssetCentre for logging	The controller supports syslog event logging. Choose a syslog collector that supports the following: - RFC-5424 syslog protocol - Ability to receive messages from the controller

Table 40. Requirements for Timely Response to Events (continued)

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
		IMPORTANT: The controller sends events to a syslog collector through a front Ethernet port. The Ethernet port must be connected to the same network as the syslog collector. To set the IP address of the syslog collector, use FactoryTalk® Policy Manager software. For more information, see CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001. To view a list of syslog messages and their descriptions, see 1756-RD001.
Controller change detection	Yes	Enable the change detection feature to monitor program components to determine whether they change. The change detection feature is not enabled by default. For more information, see Change Detection on page 148.
Controller component tracking	May be required based on system design, threat model, and risk assessment	Enable component tracking to monitor configurable program components to determine whether they change. Component tracking is not enabled by default. For more information, see Component Tracking on page 149.
Disabled controller log auto-write	Yes	The controller log stores security-related events that can be accessed via FactoryTalk® AssetCentresoftware. To help prevent the potential loss of controller logs before FactoryTalk® AssetCentre can access them, follow these guidelines: - Do not use a Message to Self (MSG with a Path of THIS) to auto-write controller logs to the SD card. - Do not manually force a write of controller logs to the SD card. By default, the controller log auto-write is disabled. For more information, see Controller Logging on page 150.

Requirements for Resource Availability

Table 41. Requirements for Resource Availability

Security Component	Required to Meet IEC-62443-4-2 SL 1	Details
FactoryTalk® AssetCentre software	Yes	Configure and use the following: - Asset inventory - Control system backup - Disaster recovery For more information, see Configure System Security Features User Manual, SECURE-UM001.
UPS	Yes	Provide your own UPS with a separate battery unit and redundant power supplies. Size the UPS so that it correctly supports the system and provides enough power to shut down servers and workstations properly.

Configure User-definable Major Faults

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

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

To create a user-defined major fault, do the following.

1. Create a fault routine for the program.
2. Configure the program to use the fault routine.
3. Jump to the fault routine.

Create a Fault Routine

To create a fault routine, do the following.

1. In the Controller Organizer, right-click the program and click Add > New Routine.
2. On the New Routine dialog box, in the Name field, type a name for the fault routine.
3. In the Type field, use the default setting, Ladder Diagram.
4. In Program or Phase field, select the program or phase where the routine will reside.
5. In the Assignment field, select Fault.
6. (optional) Select the Open Routine checkbox, to open the ladder logic program immediately.
7. Click OK.

Configure the Program to Use the Fault Routine

To configure the program to use the fault routine, do the following.

1. In the Controller Organizer, right-click the program and click Properties.
2. On the Properties dialog box, click the Configuration tab.
3. In the Fault field, select the fault routine.
4. Click OK.

Jump to the Fault Routine

In the main routine of the program, enter the following rung, where:

- Fault_Routine_1 is the name of the fault routine for the program.
- 999 is the value for the fault code.



When Tag_1.0 = 1, execution jumps to name_of_fault_routine, a major fault occurs and the controller enters the faulted mode. Outputs go to the faulted state. The Controller Properties dialog box, Major Faults tab, displays the code 999.



CIP Bridging Control

CIP™ Bridging Control enables you to control the traffic flow between physical communication interfaces and backplanes.

Devices within an Industrial Control System (ICS) may involve multiple network interfaces. The use of Common Industrial Protocol (CIP™) on the backplanes and communication ports of Rockwell Automation devices can facilitate physical network segmentation. For EtherNet/IP™ interfaces, you can provide data bridging between two separate physical Ethernet networks by using CIP™.

The CIP Security™ communication modules and embedded EtherNet/IP™ interfaces can analyze and then allow or deny network traffic according to device-specific policies. You can use CIP™ Bridging to help prevent unintended data flows from occurring, especially data flows originating from unsecured parts of the system to secure parts of the system.

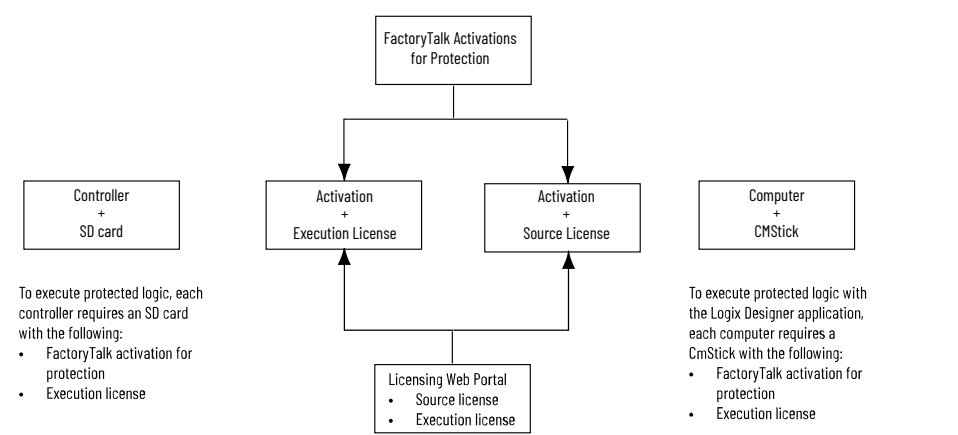
For more information, see the CIP Security with Rockwell Automation Products Application Technique, publication [SECURE-AT001](#).

License-based Source and Execution Protection

Source protection helps prevent logic components from being modified based on a license. Execution protection adds additional protection to controller logic. Execution protection makes sure that the right controller has access to execute the protected program. Use this with source protection to make sure that the right programmer has access to modify the logic.

Each device (controller or computer) requires an activation to access protection features. Each logic component or program requires a license to be accessed or executed.

Figure 48. Source and Execution Protection Example



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

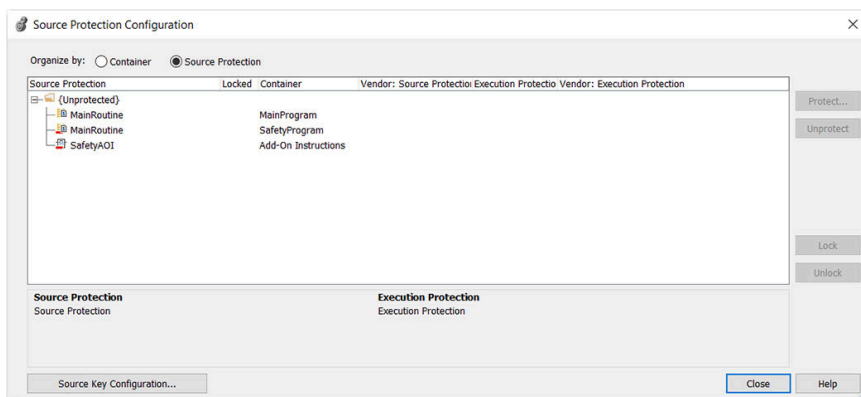
- A CmStick that contains a license with Use permission must be present locally on any USB port on the computer. Use permission cannot be obtained from a network license server. All other license privileges can be contained on the local CmStick, or provided by a license server on the network.
- A license that contains the Protect permission, either on a local CmStick or provided by a license server on the network. When components are locked, unauthorized users cannot view or edit the component, but authorized users can run the project without a CmStick.

IMPORTANT: Enabling license-based protection can have a significant impact on download times.

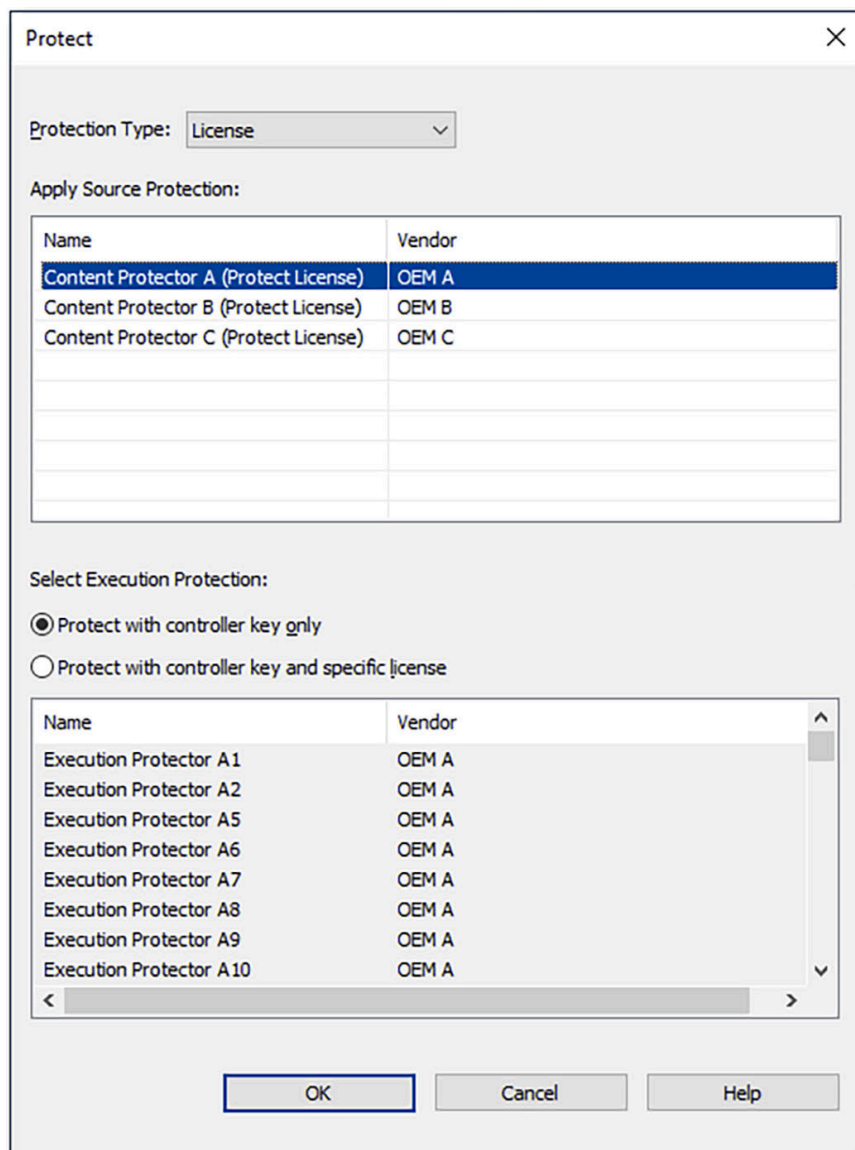
Enable License-based Protection

Complete the following.

1. Select Tools > Security > Configure Source Protection to open the Source Protection Configuration dialog box.



2. Insert the CmStick that contains the license that you want to use to help protect the component into the USB port on the computer. Licenses must contain the Protect permission to be used to protect components. If a license does not contain the Protect permission, it does not appear in the list of licenses.
3. In the Source Protection Configuration dialog box, select the component to be protected and click Protect.
4. In the Protect dialog box, select the license to apply.



5. Select the Execution Protection type:
 - Protect with controller key only. This option is selected by default. With this option selected, the component, when locked, runs only on a controller in the same family as the one specified for the project. For example, if you lock a License-based Protected component for a project on a ControlLogix® 5590 controller, the component can only be executed on another ControlLogix® 5590 controller.
 - Protect with controller key and specific license. When you select this option, the component runs only on a controller in the same family as the one specified for the project and that contains a CmCard with the execution license that you select. If you select Protect with controller key and specific license, select the execution license from the list of available licenses. After components are protected, they can also be locked. When you lock a component, it helps prevent users from viewing or editing the component, but allows authorized users to run it.

6. To return to the Source Protection Configuration dialog box, click OK.



To save changes to a component that is protected with License-Based Source Protection, a CmStick that contains the required license must be plugged into the computer that runs the Logix Designer application.

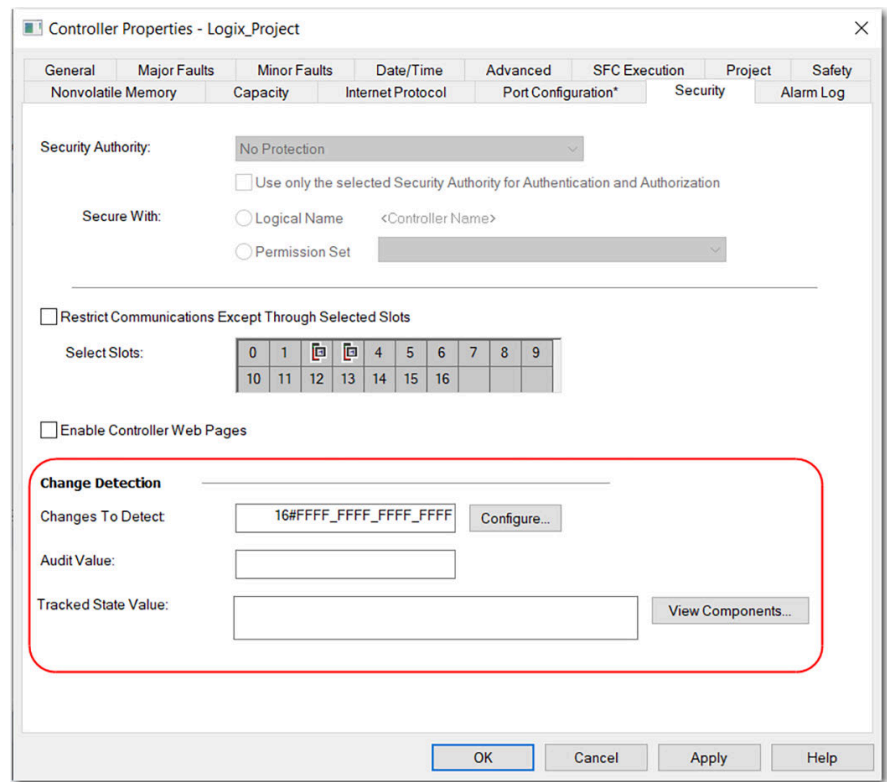
Make sure that you save your edits to the project or lock the protected components before removing the CmStick that contains the required license. If the license is not present, you could lose your edits to the project.

Change Detection

On the Security tab of the controller properties, the Change Detection feature tracks changes to a controller and generates an audit value when a monitored change occurs.

For more information about change detection, see the Logix 5000 Controller Information and Status Programming Manual, publication [1756-PM015](#).

Figure 49. Change Detection



Changes to Detect

Click Configure to open the Configure Changes to Detect dialog box. We recommend tracking the following changes for a standard controller. By default, all event types can cause the audit value to change, resulting in a default value of 0xFFFFFFFFFFFFFFF.

- Project stored to removable media
- Online edits modified controller program
- Transaction committed
- SFC forces enabled
- SFC forces disabled

- SFS forces removed
- SFC element force value changed
- I/O forces enabled
- I/O forces disabled
- I/O forces removed
- I/O forces modified
- Firmware update attempted
- Firmware update from removable media attempted
- Remote mode change
- Controller switch mode change
- A major fault occurred
- All major faults cleared
- All major faults cleared through controller switch
- Task properties modified
- Program properties modified
- Removable media removed
- Removable media inserted
- Constant Tag value changed
- Multiple constant Tag values changed
- Constant Tag attribute cleared
- Constant Tag attribute set
- Custom Log Entry Added
- Correlation affected
- Alarm Log values cleared
- Parameter Connection has been modified
- Port configuration has been changed

By default, all event types can cause the audit value to change, resulting in a default value of 0xFFFFFFFFFFFFFFFF.

Audit Value

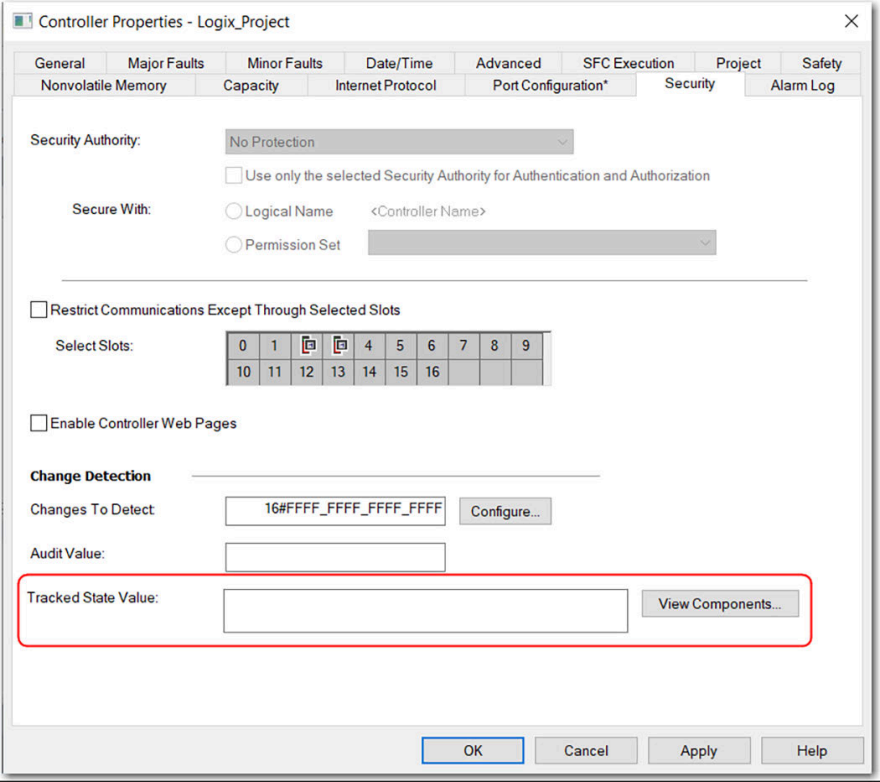
A unique value that is generated when a project is downloaded to the controller or loaded from a storage device. This value is updated when a change to an event occurs. Some events always cause an Audit Value change, while others are selectable in the Configure Changes to Detect dialog box. When the controller is offline, the Audit Value box is blank.

Component Tracking

On the Security tab of the Controller Properties dialog box, component tracking enables you to determine whether tracked routines, Add-On Instructions, I/O modules, and constant tags have been changed. The Studio 5000 Logix Designer® application creates a tracked state value to indicate the current state of all components.

For more information about component tracking, see the Logix 5000 Controller Information and Status Programming Manual, publication [1756-PM015](#).

Figure 50. Tracked State Value



Controller Logging

The controller log stores various security-related events that can be written to a memory card or accessed via FactoryTalk® AssetCentre or a third-party syslog collector. Some of these events are Logix Designer application request errors, control system events, backup/restore events, and configuration changes.

For more information on how to access the controller log, see the Logix 5000 Controller Information and Status Programming Manual, publication [1756-PM015](#).

For more robust logging and to help prevent rollover, use FactoryTalk® AssetCentre or a syslog collector.

Controller Ethernet Port

You can disable a controller Ethernet port with the Studio 5000 Logix Designer® application.

IMPORTANT: Remember the following:

- For controllers with two Ethernet ports, you can disable either of the Ethernet ports whether the controller uses Dual-IP mode or Linear/DLR mode.
- Once a port is disabled, you lose any connection that is established through the controller Ethernet port.
- You cannot disable Ethernet ports if the controller switch is in Run mode or if the FactoryTalk® Security settings deny this editing option.

Ethernet ports return to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset

- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - These examples clear the program from a controller:
 - Major nonrecoverable fault occurs.
 - Firmware update occurs.

You must reconfigure the settings to disable an Ethernet port after the port returns to its default settings.

There are two ways to disable an Ethernet port:

- [Disable an Ethernet Port on the Port Configuration Tab on page 151](#)
- [Disable an Ethernet Port with an MSG Instruction on page 152](#)

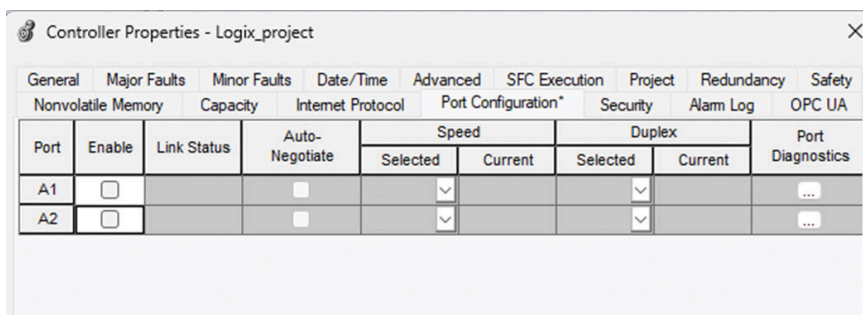
Disable an Ethernet Port on the Port Configuration Tab

You can disable an embedded Ethernet port on the controller. This method retains the setting in the project, so every time you download the project to the controller, the Ethernet port is disabled.

1. On the Online toolbar, click the Controller Properties button.



2. On the Controller Properties dialog box, click the Port Configuration tab.
3. On the Port Configuration tab, clear the Enable checkbox.



4. On the Port Configuration tab, click Apply.
 - If you are online when you make this change, then an Alert dialog box appears. On the dialog box, click Yes. The change takes effect immediately.
 - If you are offline, then the change takes effect when you download the program to the controller.
5. On the Port Configuration tab, click OK.

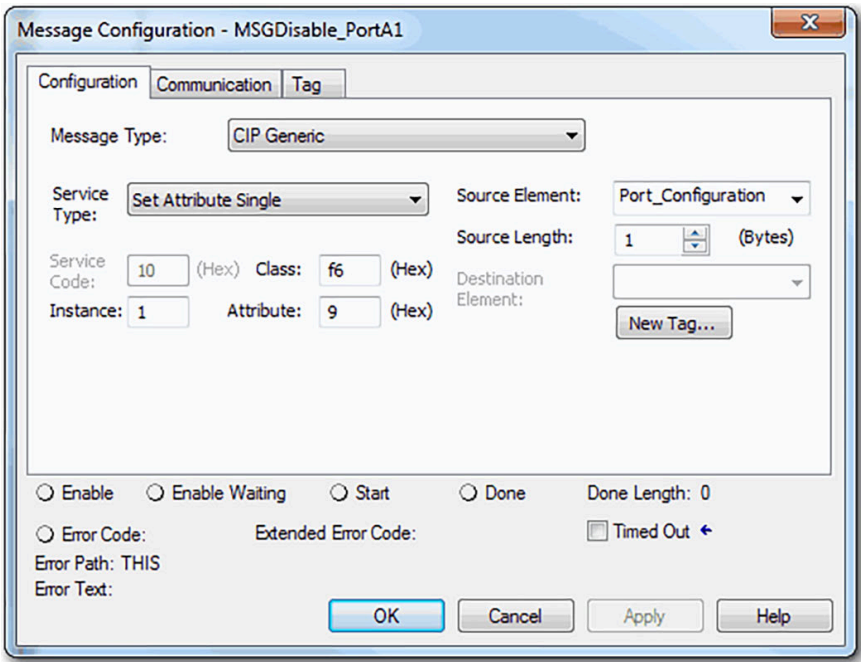
Disable an Ethernet Port with an MSG Instruction

You can use a CIP™ Generic MSG with a Path of THIS to execute this option. You cannot use this MSG instruction to disable an Ethernet port on another controller.

- 1. Add an MSG instruction to your program.
This message only has to execute once, it does not need to execute with every program scan.

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

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



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

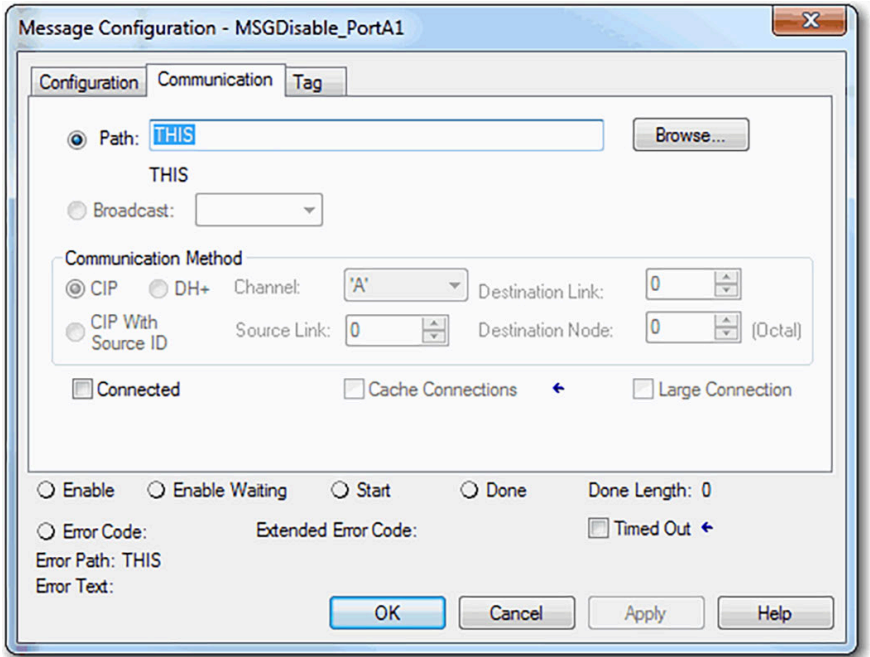
Table 42. Disable the Ethernet Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1 to disable the Ethernet port on controllers with a single Ethernet port, or disable Port A1 on controllers with two Ethernet ports. 2 to disable Port A2 on controllers with two Ethernet ports.
Class	f6

Field	Description
Attribute	9
Source Element	Controller tag of SINT data type. Source Element Tag Data: - 1 = Enable port - 2 = Disable Port In this example, the controller tag is name Port_Configuration.
Source Length	1

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

IMPORTANT: Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, verify that the Source Element tag value is 2.

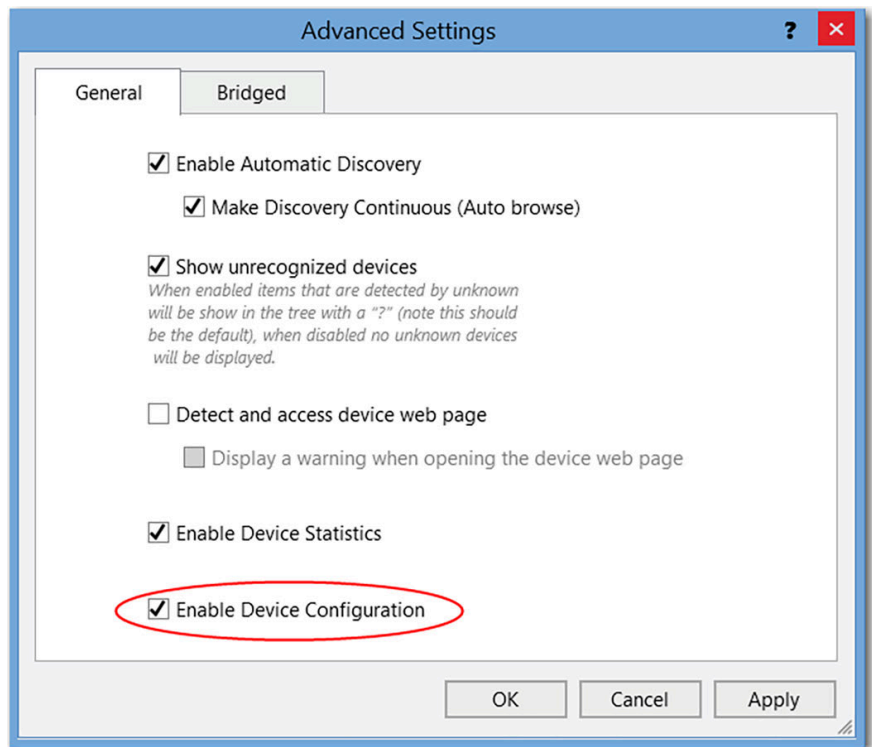
IMPORTANT: You can re-enable an Ethernet port after it is disabled.

To re-enable the port, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 1.

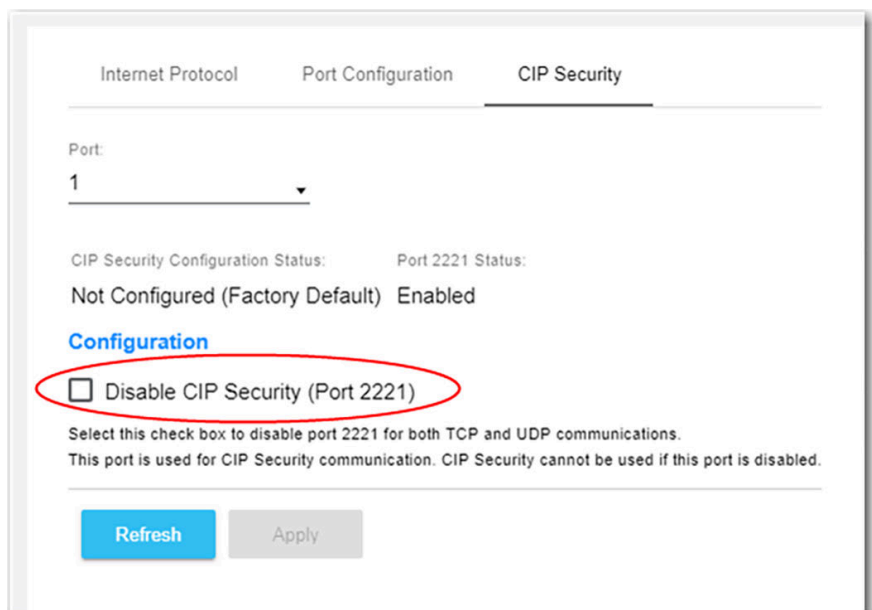
Disable CIP Security Ports via FactoryTalk Linx

To disable CIP Security™ ports via FactoryTalk® Linx, complete the following.

1. If the Device Configuration menu in FactoryTalk® Linx is not enabled, go to the Advanced Settings dialog box and check the Enable Device Configuration checkbox.



2. From the Device Configuration menu, click the CIP Security tab, and then check the Disable CIP Security (Port 2221) checkbox.



Disable CIP Security Ports via a CIP Generic MSG Instruction

To disable CIP Security™ ports via CIP™ Generic MSG instructions, complete the following.

IMPORTANT: This procedure disables CIP Security™ ports. To re-enable the ports, use the controller reset button to perform a Stage 2 reset, which returns the controller to a factory default state. For more information, see Stage 2 Reset on page .

You cannot use this MSG instruction to disable the CIP Security™ ports on another controller. The message only has to execute once rather than with every program scan.

1. Create a controller tag with the SINT[9] data type. In this example, the controller tag is named CIPSEC_DISABLE and must match the following image.

Name	Value	Style	Data Type
▲ CIPSEC_DISABLE	{...}	Hex	SINT[9]
▶ CIPSEC_DISABLE[0]	16#02	Hex	SINT
▶ CIPSEC_DISABLE[1]	16#ad	Hex	SINT
▶ CIPSEC_DISABLE[2]	16#08	Hex	SINT
▶ CIPSEC_DISABLE[3]	16#11	Hex	SINT
▶ CIPSEC_DISABLE[4]	16#00	Hex	SINT
▶ CIPSEC_DISABLE[5]	16#ad	Hex	SINT
▶ CIPSEC_DISABLE[6]	16#08	Hex	SINT
▶ CIPSEC_DISABLE[7]	16#06	Hex	SINT
▶ CIPSEC_DISABLE[8]	16#00	Hex	SINT

Before you enable the MSG instruction, consider the following:

- The element CIPSEC_DISABLE[4] is responsible for disabling UDP port 2221 and EtherNet/IP™ over DTLS, transport class 0/1.
- The element CIPSEC_DISABLE[8] is responsible for disabling TCP port 2221 and EtherNet/IP™ over TLS, UCMM, and transport class 3.
- To disable the controller CIP Security ports, the elements CIPSEC_DISABLE[4] and CIPSEC_DISABLE[8] in the SINT array for the Source Element CIPSEC_DISABLE must be 0.

2. Add an MSG instruction to your program.

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

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

Message Configuration - MSGDisable_CIP_Security

ConfigurationCommunicationTag

Message Type: CIP Generic

Service Type: Custom

Source Element: CIPSEC_DISABLE

Service Code: 4c (Hex) Class: f5 (Hex)

Source Length: 9 (Bytes)

Instance: 1 Attribute: 0 (Hex)

Destination Element:

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 43. Disable the CIP Security Port

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1
Class	f5
Attribute	0
Source Element	Controller tag of SINT[9] data type. This is the controller tag that you created previously.
Source Length	9

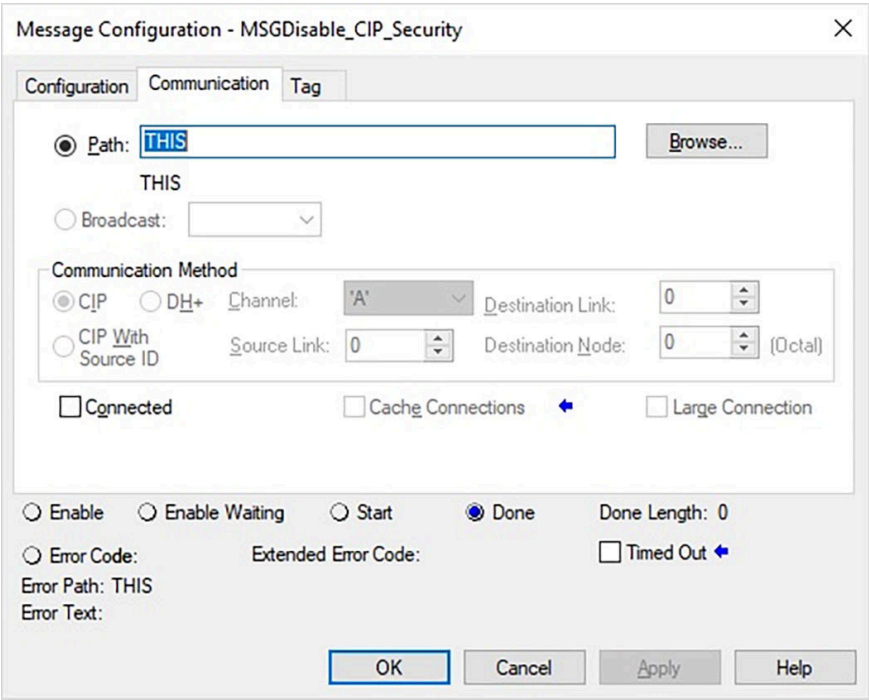
4. Configure the Communication tab to use a Path of THIS.

IMPORTANT: Messages to THIS must be unconnected messages.

156

1756-UM900B-EN-P - November 2025

Rockwell Automation, Inc.

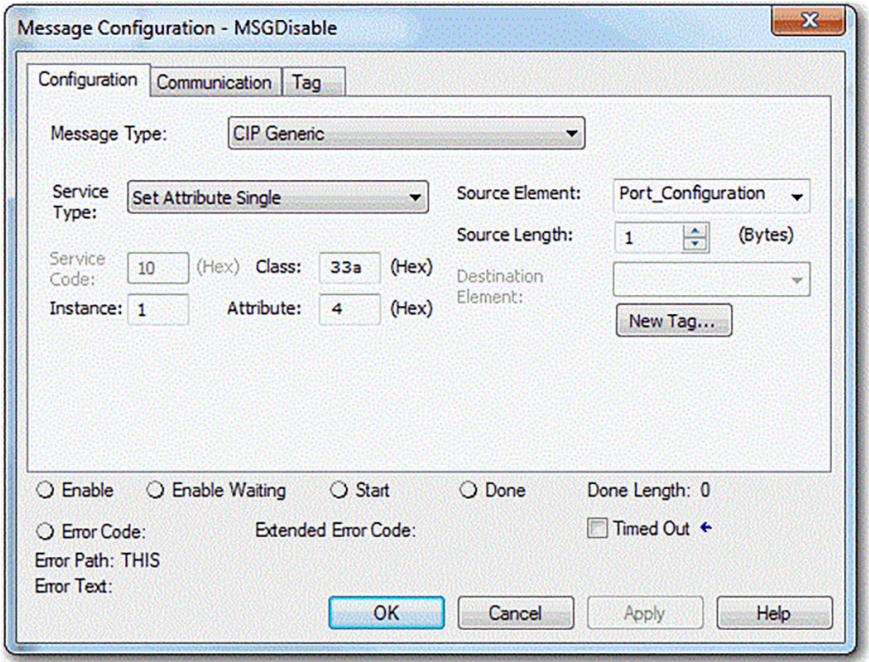


- 5. Cycle power on the controller for the configuration to take effect.

Disable the Controller USB Port

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

- 1. Add an MSG instruction to your program.
This message only has to execute once, it does not need to execute with every program scan.
- IMPORTANT:** You cannot add an MSG instruction to your program if the controller switch is in Run mode, or if the FactoryTalk® Security settings deny this editing option.
- 2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.



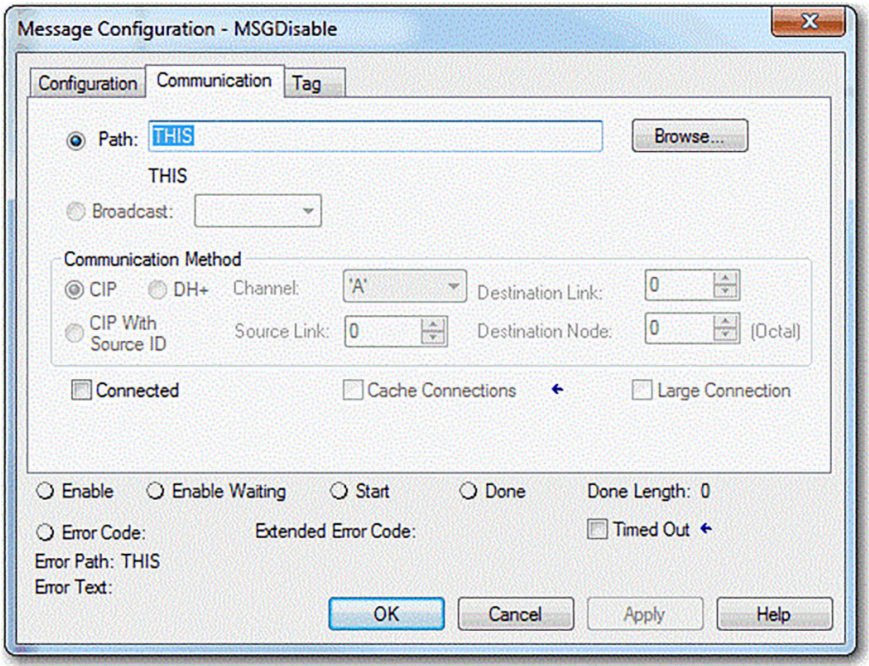
IMPORTANT: These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute up each time the controller powers up.

Table 44. Disable the USB Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	33a
Attribute	4
Source Element	Controller tag of SINT data type. In this example, the Source Element is named Port_Configuration.
Source Length	1

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

IMPORTANT: Messages to THIS must be unconnected messages.



Disable the Controller Memory Card

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

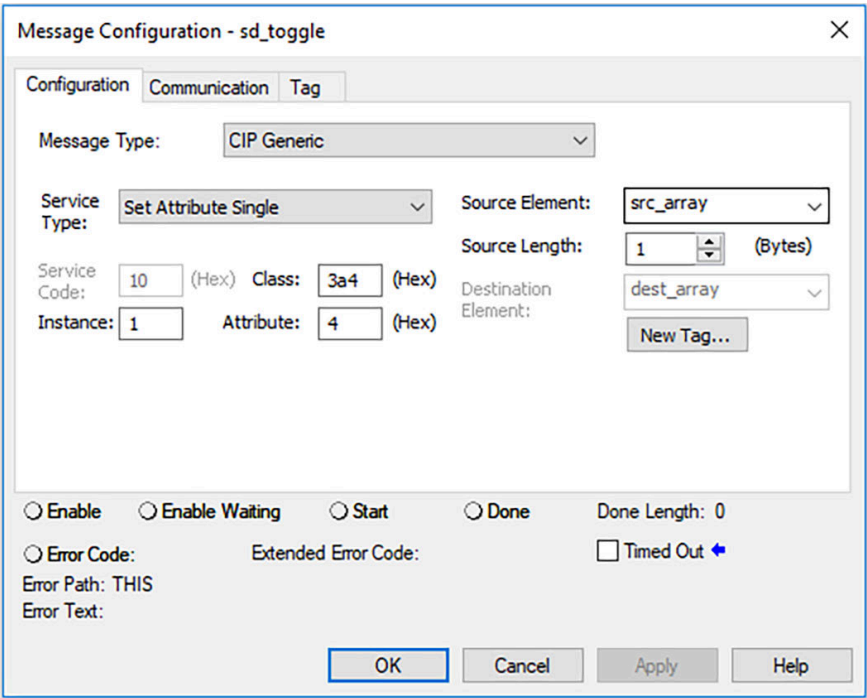
IMPORTANT: Remember the following:

- A memory card can only be disabled with a Message to Self.
- Once a memory card slot is disabled, you lose all ability to communicate to a memory card inserted into the slot. This includes any diagnostic information.

1. Add an MSG instruction to your program. This message only has to execute once, it does not need to execute with every program scan.

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

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



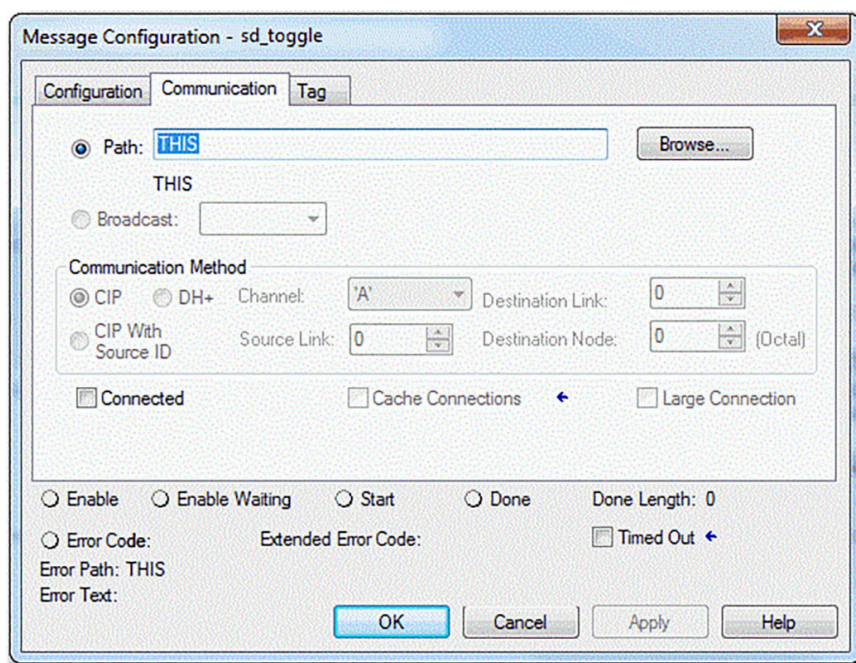
IMPORTANT: These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

Table 45. Disable the Memory Card

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a4
Attribute	4
Source Element	Controller tag of SINT Array. Source Element Tag Data: - 0 = Enable memory card - 1 = Disable memory card In this example, the Source Element is named src_array.
Source Length	1

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

IMPORTANT: Message to THIS must be unconnected messages.



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

IMPORTANT: You can re-enable the memory card after it's been disabled.

To re-enable the memory card, complete the steps that are described in this section. Before you enable the MSG instruction, be sure that the appropriate bit in the Source Element tag value is 0.

Controller 4-character Status Display

With the Studio 5000 Logix Designer® application, you can disable certain categories of messages on the four-character status display.

You use a CIP Generic MSG to execute each option.

IMPORTANT: You cannot disable these system messages, and they always display:

- Power-up messages, such as TEST, PASS, CHRG
- Catalog number message
- Firmware revision message
- Major / Critical failure messages

The 4-character status display returns to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset
- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - these examples can clear the program from a controller:
 - Major nonrecoverable fault occurs.
 - Firmware update occurs.

You must reconfigure the settings to disable the 4-character status display after it returns to its default settings.

Disable All Categories of Messages

You can disable a subset of the information that scrolls across the controller 4-character display. You can disable these subsets:

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

Complete these steps.

1. Add an MSG instruction to your program.
This message only has to execute once, it does not need to execute with every program scan.
2. Configure the Configuration tab on the Message Configuration dialog box as described in the table below.

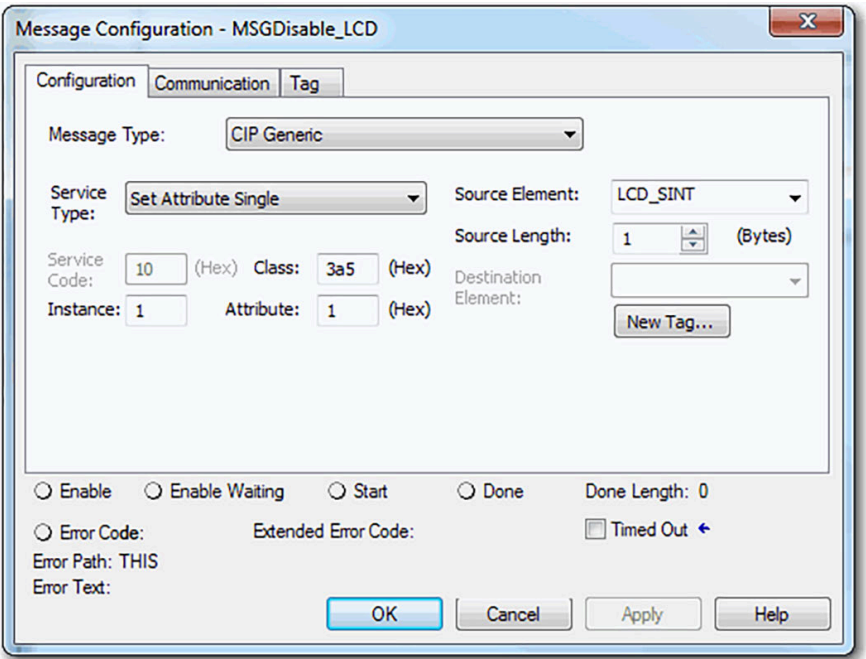


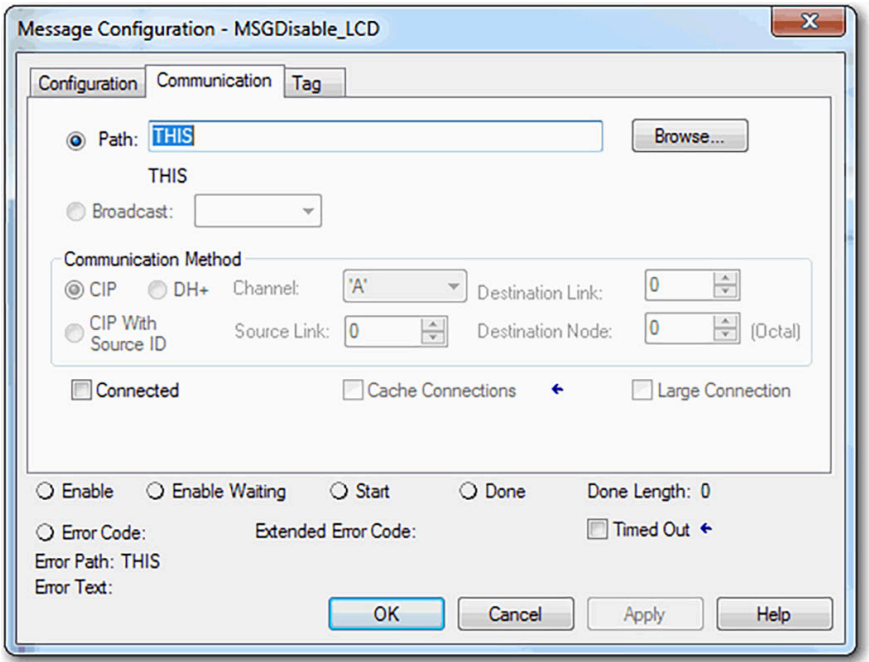
Table 46. Disable All Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1

Field	Description
Class	3a5
Attribute	1
Source Element	Controller tag of SINT data type. Source Element Tag Data: - 0 = Enable LCD Subset - 1 = Disable LCD Subset In this example, the controller tag is named LCD_SINT. To disable the subset of the information that scrolls across the controller 4-character display that are described in this section, the Source Element tag value must = 1.
Source Length	1

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

IMPORTANT: Messages to THIS must be unconnected messages.



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

IMPORTANT: You can re-enable the subsets of information on the 4-character display after they are disabled.

To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, be sure that the appropriate bit in the Source Element tag value is 0.

Disable Individual Categories of Messages

You can disable a subset of the information that scrolls across the controller 4-character display. You can disable these subsets:

- Project name and link status
- Port status and IP address

Complete these steps.

1. Add an MSG instruction to your program. This message only has to execute once, it does not need to execute with every program scan.

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

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

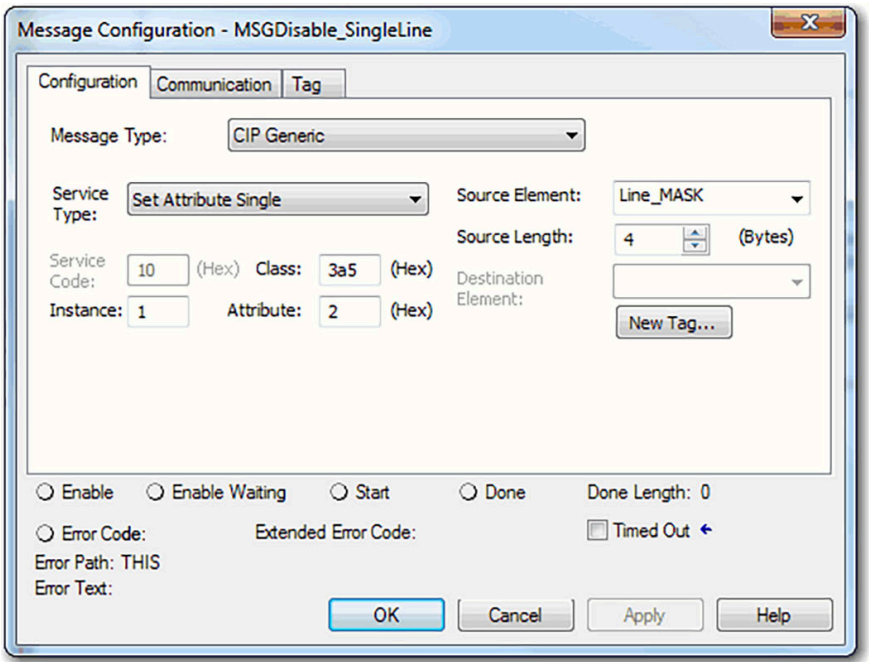


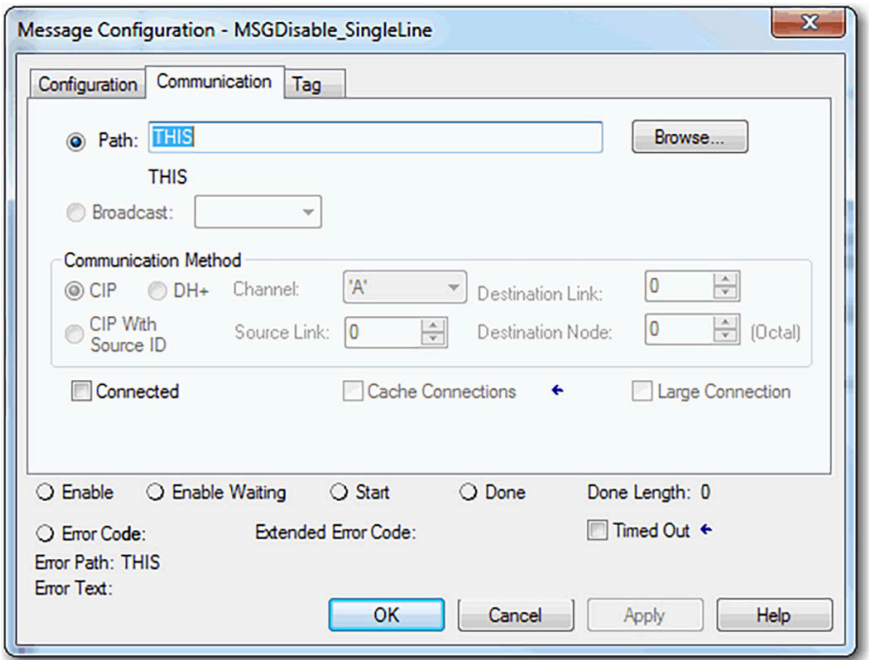
Table 47. Disable Individual Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a5
Attribute	2
Source Element	Controller tag of DINT data type.

Field	Description
	Source Element Tag Data: - Enable Project name and link status - Bit 0 of the Source Element = 0 - Enable Port status and IP address - Bit 1 of the Source Element = 0 - Disable Project name and link status - Bit 0 of the Source Element = 1 - Disable Port status and IP address - Bit 1 of the Source Element = 1 In this example, the controller tag is named Line_MASK.
Source Length	4

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

IMPORTANT: Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, make sure that the Source Element uses one of the following tag values that are based on what information that you want to disable:
- Project name and link status - Bit 0 of the Source Element = 1
 - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT: You can re-enable the subsets of information on the 4-character display after they are disabled.

To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, be sure that the appropriate bit in the Source Element tag value is 0.

Controller Webpage Default Settings

The controller webpages are disabled by default. You must reconfigure the settings to enable the controller webpages after it returns to its default settings.

Controller webpages return to the default setting in these situations:

- A stage 1 reset for all versions of the Studio 5000 Logix Designer® application.
- A stage 2 reset for all versions of the Studio 5000 Logix Designer® application.

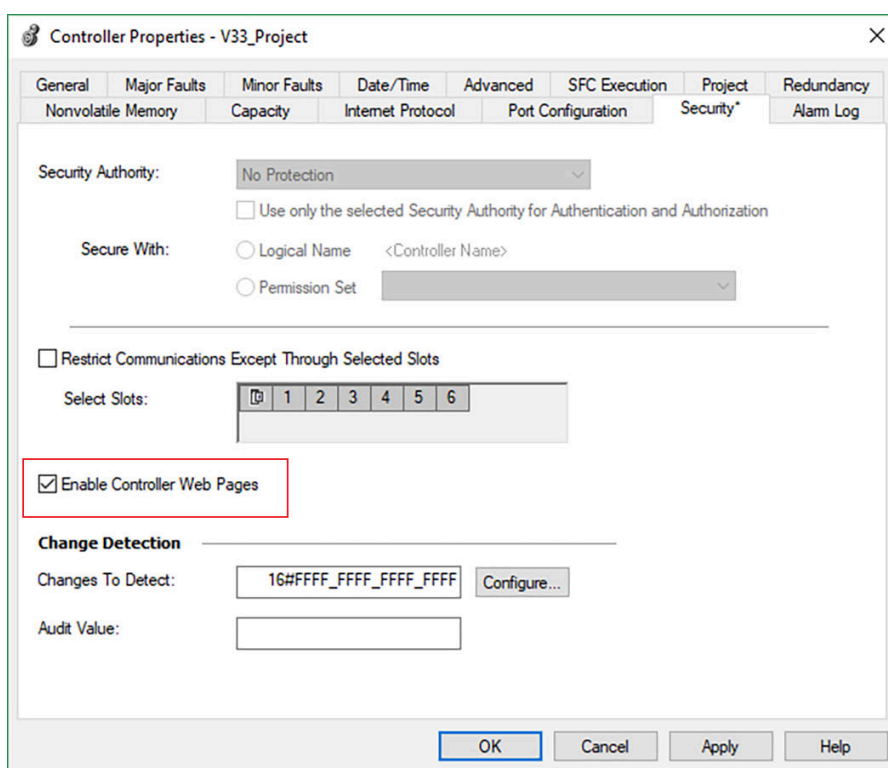
The setting of the controller webpages changes after the following occurs on the controller:

- New project is downloaded - in this case, the settings in the new project take effect.
- When the controller receives a configuration message, it takes the setting from the configuration message.

Disable Controller Webpages via Controller Properties

You can use one of the following methods to disable the controller webpages:

- If the controller web pages are enabled, disable them by clearing the Enable Controller Web Pages check box on the Security tab for the controller properties.



IMPORTANT: The status of the Enable Controller Web Pages checkbox is saved to and restored from the memory card when using the save/restore feature.

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

Manage Controller Webpages Via CIP Generic MSG Instructions

With the Studio 5000 Logix Designer® application, you use a CIP Generic MSG to disable or enable the controller webpages.

Disable the Controller Webpages Via a CIP Generic MSG Instruction

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 switch is in RUN mode, or if the FactoryTalk® Security settings deny this editing option.
2. Configure the Configuration table on the Message Configuration dialog box as described in the table below.

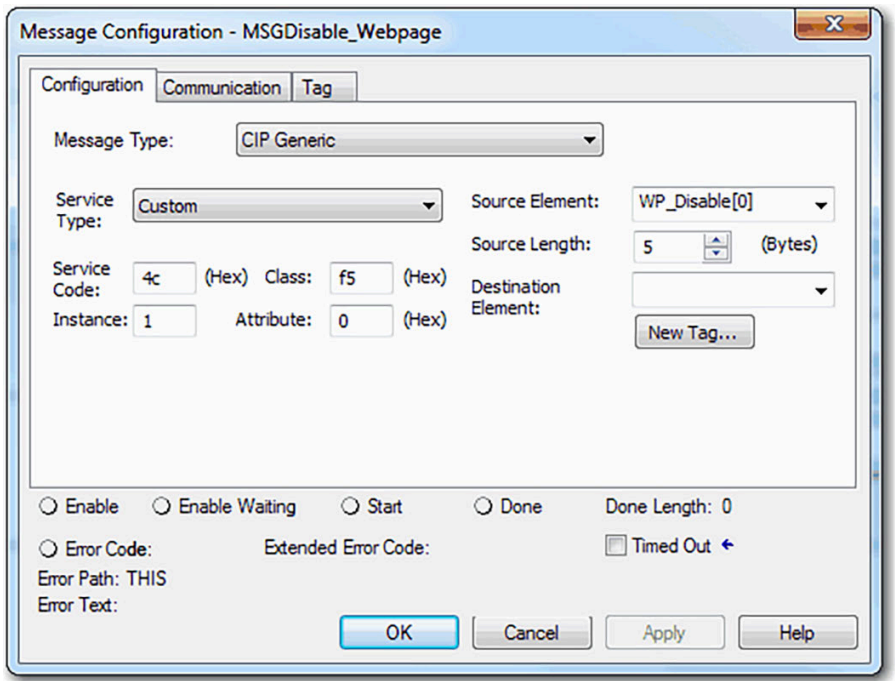


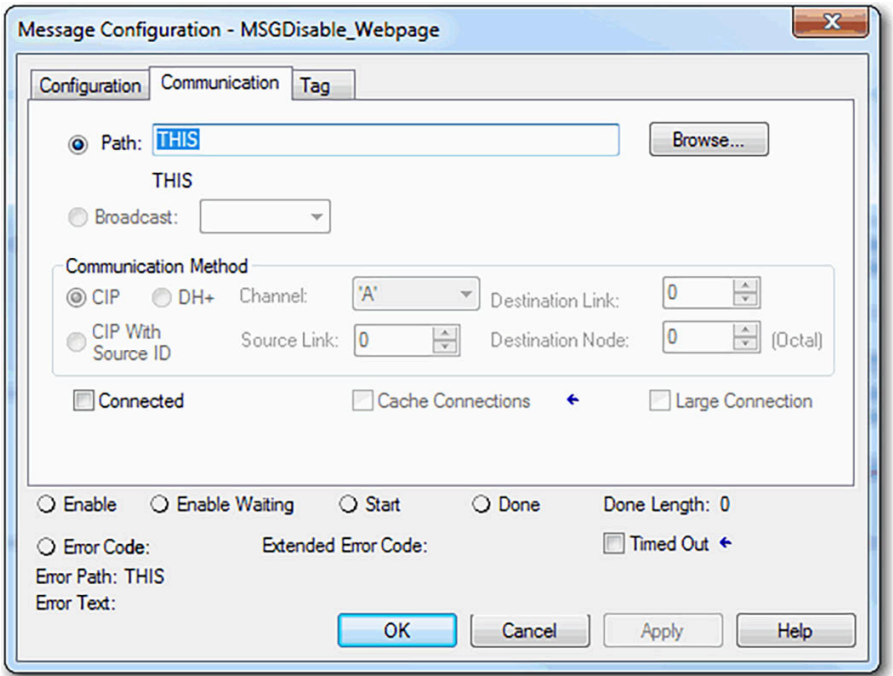
Table 48. Disable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode
Class	f5

Field	Description																								
Attribute	0																								
Source Element	Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Disable and must match the following graphic. <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> 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.	▾ 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																								

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

IMPORTANT: Messages to THIS must be unconnected messages.



Enable the Controller Webpages Via a CIP Generic MSG Instruction

- 1. Add an MSG instruction to your program.

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

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

Message Configuration - MSGEnable_Webpage

Configuration*

Communication

Tag

Message Type:

CIP Generic

Service Type:

Custom

Source Element:

WP_Enable

Service Code:

4c

(Hex)

Class:

f5

(Hex)

Source Length:

5

(Bytes)

Instance:

1

Attribute:

0

(Hex)

Destination Element:

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 49. Enable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode

Field	Description																								
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. <table><tr><td>▲ WP_Enable</td><td>{...}</td><td>Decimal</td><td>SINT[5]</td></tr><tr><td>▶ WP_Enable[0]</td><td>1</td><td>Decimal</td><td>SINT</td></tr><tr><td>▶ WP_Enable[1]</td><td>80</td><td>Decimal</td><td>SINT</td></tr><tr><td>▶ WP_Enable[2]</td><td>0</td><td>Decimal</td><td>SINT</td></tr><tr><td>▶ WP_Enable[3]</td><td>6</td><td>Decimal</td><td>SINT</td></tr><tr><td>▶ WP_Enable[4]</td><td>1</td><td>Decimal</td><td>SINT</td></tr></table> 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.	▲ 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
▲ 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																						
Source Length	5																								

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

IMPORTANT: Messages to THIS must be unconnected messages.

Message Configuration - MSGEnable_Webpage

Configuration* Communication Tag

☒ Path:

THIS

☐ Broadcast:

Communication Method

☒ CIP ☐ DH+ Channel: Destination Link:

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

☐ Connected ☐ Cache Connections ☐ Large Connection

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

☐ Error Code: Extended Error Code: ☐ Timed Out

Error Path: THIS

Error Text:

Privacy Aspects

If configured to do so, the controller can collect the following personal data for the purpose of logging user activity:

- User name (full name and domain name)
- Workstation name
- FactoryTalk® ID

No more personal data is collected than needed and no personal data is logged by default.

IMPORTANT: The general purpose programming capabilities of the controller allow you to program the controller to collect personal data through connection to other devices and systems for any purpose. You are responsible for protecting personal data collected as a result of your applications.

Data Protection

The following provides methods to protect personal data stored by the controller through restricted access:

- CIP Security™ — To implement CIP Security™, see the CIP Security with Rockwell Automation Products Application Technique, [SECURE-AT001](#).
- FactoryTalk® Security — To configure FactoryTalk® Security permissions, see the Configure System Security Features User Manual, [SECURE-UM001](#).

Data Removal

Personal data can be stored by the controller in these locations:

- Internal memory of the controller. The circular buffer of the controller only keeps a limited amount of data within the controller.
- External memory card, only if logging is configured to write to a text file on the card

IMPORTANT: Data that has been retrieved by external software is the responsibility of the respective software.

You can remove personal data by using these methods:

- Perform a factory reset on the controller to delete data from internal memory.
- Access the text file on the memory card and delete personal data.

IMPORTANT: The controller does not have secure reset functionality to make deleted data nonrecoverable. To address critical security concerns about data recovery, we recommend physically destroying a device when decommissioned.

Develop Safety Applications

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

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



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

Safety Applications

The safety concept assumes the following requirements:

- You are responsible to create, operate, and maintain the safety application.
- You are fully qualified, specially trained, and experienced in safety systems.
- You apply the logic correctly to detect programming errors through strict adherence to specifications, programming, and naming rules.
- You perform a critical analysis of the application and use all possible measures to detect a failure.
- You confirm all application downloads via a manual check of the safety signature.
- You perform a complete functional test of the entire system before the operational startup of a safety-related system. This test includes, but is not limited to, the following:
 - Validate that the overall functionality of the implemented safety functions, including I/O configuration via Add-On Profiles, beyond the limits of the individual devices (boundary testing).
 - Verify that the correct versions of software are used.

Table 50. Effect of Controller Modes on Safety Execution

Controller Mode	Controller Safety Execution
Program	• Safety input and output connections are established and maintained. Safety input tags are updated to reflect safety input values. • Safety mapped tags are updated to reflect the standard controller tag values. • Safety task logic is not being scanned.
Test	• Safety input and output connections are established and maintained. Safety input tags are updated to reflect safety input values. • Safety mapped tags are updated to reflect the standard controller tag values. • Safety task logic is being scanned.
Run	• Safety input and output connections are established and maintained: - Safety input tags are updated to reflect safety input values. - The controller sends 'run' safety output packets.

Table 50. Effect of Controller Modes on Safety Execution (continued)

Controller Mode	Controller Safety Execution
	• Safety mapped tags are updated to reflect the standard controller tag values. • Safety task logic is being scanned. • All safety task process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.

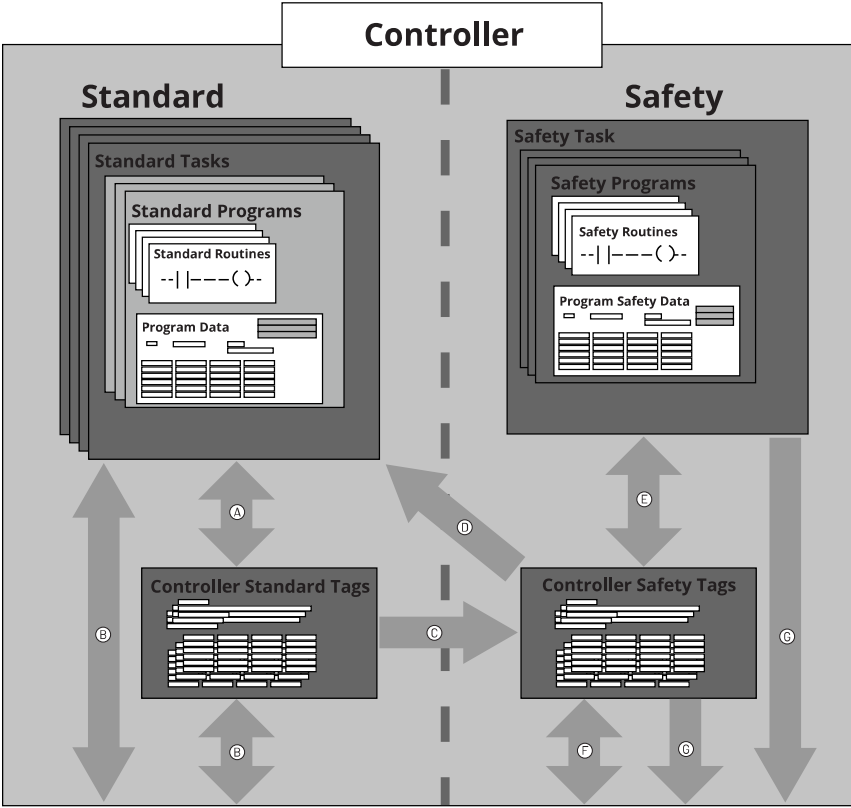
Table 51. Safety Application Status

Safety Task Status	Safety Rating ¹ (Up to and Including)	Controller Behavior
Unlocked no signature	Only for development purposes	• Safety I/O forces can be present. • Safety I/O forces can be modified. • Safety online editing is allowed. • Safety memory is isolated, but is unprotected (read/write). • Download allowed if a major firmware revision of the offline project matches the target controller.
Locked no signature	Only for development purposes	• Safety I/O forces are not allowed. Forces of safety I/O must be removed before locking is possible. • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Download is not allowed.
Unlocked with signature	SIL 2/SIL 3 (per controller)	• Safety I/O forces are not allowed. Forces of safety I/O must be removed before locking is possible. • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Safety signature is unprotected and anyone who has access to the controller can delete it. • Download allowed if a major firmware revision of the offline project matches the target controller.
Locked with signature	SIL 2/SIL 3 (per controller)	• Safety I/O forces are not allowed. • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Safety signature is protected. You must enter the unlock password to unlock the controller before you can delete the safety signature. • Download is allowed if the major and minor firmware revision and signature of the offline project match the target controller, the project is safety-locked, and the safety task status of the controller is OK. IMPORTANT: If the controller is safety-locked and the safety-unlock password is lost and a download is needed, you must perform a Stage 1 reset of the controller.

1. To achieve this level, you must adhere to the safety requirements defined in this safety reference documentation.

Controller Data Flow Capabilities

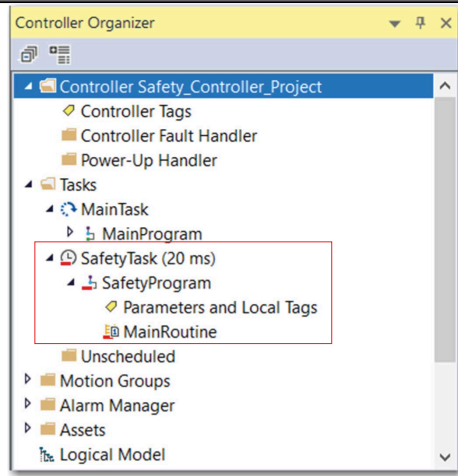
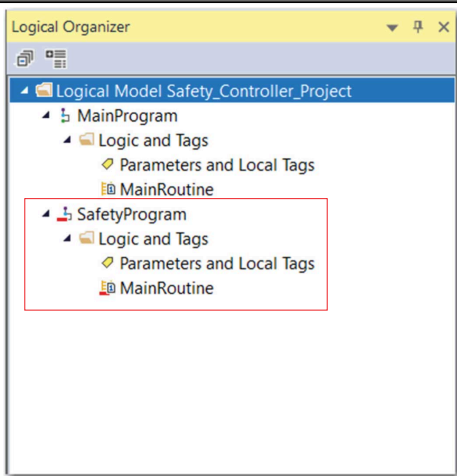
Figure 51. Controller Data-flow Capabilities



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

Safety Task

A safety application includes a safety task with a safety program and main routine.

Safety Task in Controller Organizer	Safety Program in Logical Organizer
	

A safety task has these characteristics:

- The safety task is a periodic timed task. A periodic task is triggered at repetitive intervals. When triggered, the period task and its programs are executed. Data and outputs that the programs in the task establish retain their values until the next execution of the task or until another task manipulates them. Periodic tasks always interrupt the continuous task.
- The safety task cannot be deleted.
- Within the safety task, you can use multiple safety programs that are composed of multiple safety routines.
- You cannot execute standard routines from within the safety task.
- There can be only one safety task for a controller.
- You must configure the period and the priority of the safety task. The safety task can be interrupted according to the same rules as standard tasks, such as interruptions by the motion task. The motion task is always a higher priority than any user task.

IMPORTANT: Large amounts of mapped safety tags or large amounts of safety produce/consume tag data can cause fluctuations in the safety task scan time of the controller.

IMPORTANT: If the controller is configured for SIL 2 and the next slot to the right is empty or populated by a non-safety module, execution of the safety task can be delayed during powerup by five seconds or more.

Safety Task Parameters

You can configure the following safety task parameters:

- Period—The safety task period is the time interval between successive executions of the safety task. The safety task period directly affects system reaction time. You cannot edit the safety task period online.
- Priority— Configure the safety task with a higher priority (lower number) to reduce fluctuations in execution time. A higher priority can allow a lower setting for the safety task watchdog, which improves the reaction time of the safety system.
- Watchdog—The safety task watchdog is the maximum time that is allowed from the start of the safety task to its completion. If a safety task watchdog timeout occurs, a nonrecoverable safety fault is generated in the controller.

To configure the safety task, right-click the safety task and choose Properties.

IMPORTANT: The values that you define for the safety task parameters must meet the requirements that are defined in the following table.

Figure 52. Safety Task Parameters

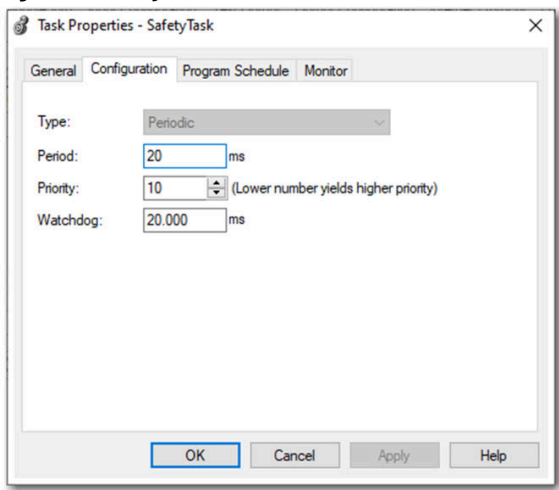


Table 52. Safety Task Requirements

Parameter	Requirement
Period	Be sure that the safety task has enough time to execute its logic before it restarts. Enter a value of 2...500 ms.
Priority	To get the most consistent safety task execution time and to minimize safety task watchdog faults, we recommend that you enter a value of 1 to make the safety task the highest priority user task.
Watchdog	Enter a value of 2...500 ms.

Safety Task Execution Details

The safety task executes like standard periodic tasks with these exceptions:

- Safety input tags and safety-consumed tags are updated only at the beginning of safety task execution. This process means that even though the I/O RPI can be faster than the safety task period, the data in the Safety Input tag only updates once at the beginning of each safety task execution. Safety input and consumed packets that arrive after the start of the safety task are buffered until the next execution of the safety task.
- Time is frozen at the start of safety task execution. As a result, timer-related instructions, such as TON and TOF, are not updated during a safety-task execution. They keep accurate time from one task execution to another, but the accumulated time is not changed during safety task execution.

IMPORTANT: This behavior differs from standard Logix task execution.

- For standard tags that are mapped to safety tags, the standard tag values are copied to the safety tags at the start of the safety task:
 - The standard tag is free to continue changing.
 - Programming logic can change the safety tag within the safety task, but the change is not reflected back to the standard tag.

IMPORTANT: The addition of more mapped tags can increase the scan time.

- Safety output tag values can be changed during the safety task scan by the safety programming logic. The final value is transmitted to safety modules at the end of the safety task scan. Likewise, safety produced values are transmitted to consuming safety controllers at the end of the safety task scan.

IMPORTANT: While safety-unlocked and without a safety signature, the controller helps prevent simultaneous write access to safety memory from the safety task and communication commands. As a result, the safety task can be held off until a communication update completes. The time that is required for the update varies by tag size. Insufficient time can result in safety connection and safety watchdog timeouts.

To compensate for the hold-off time due to a communication update, you must increase the safety watchdog time.

Depending on the edit, a watchdog timeout can occur if there is insufficient time to complete the safety task operation.

When the controller is safety-locked or a safety signature exists, the scenarios that are described in this note cannot occur.

Safety Programs

A safety program has the attributes of a standard program, except that it can be scheduled only in the safety task:

- A safety program can also define program-scoped safety tags.
- A safety program can be scheduled or unscheduled.
- A safety program can contain only safety components.
- All routines in a safety program are safety routines. One safety routine must be designated as the main routine, and another safety routine can be designated as the fault routine.
- A safety program cannot contain standard routines or standard tags.
- For program parameters, a safety parameter cannot be connected with or bound to a standard parameter or controller-scoped tag.

Safety Routines

Safety routines have the same attributes of standard routines, except for the following:

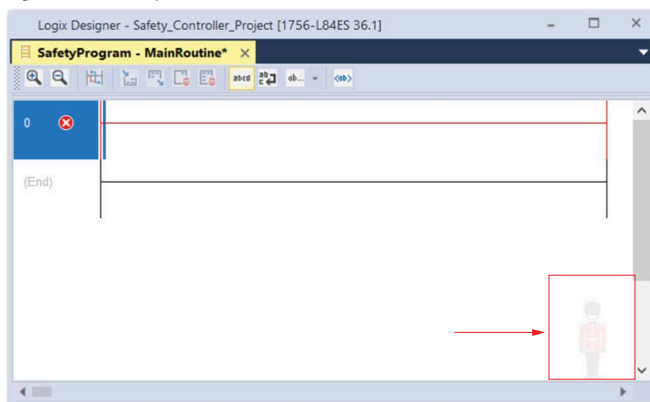
- Safety routines can exist only in safety programs.
- Safety routines cannot read or write standard tags.
- Safety routines can only be done in Ladder Logic.

One safety routine must be designated as the main routine in each safety program. Another safety routine can be designated as the fault routine for that safety program.

Only safety-certified instructions or Add-on Instructions composed from them are used in safety routines. For a list of instructions, see [Safety Instructions on page 282](#).

A watermark visually distinguishes a safety routine from a standard routine.

Figure 53. Safety Routine Watermark



Safety Tags

The controller supports the use of both standard and safety tags in the same project. However, the programming software operationally differentiates standard tags from safety tags.

Safety tags have the same attributes as standard tags with the addition of mechanisms that are certified to provide SIL 2/PLd and SIL 3/PLe data integrity.

When you create a tag, you assign the following properties:

- Name
- Description (optional)
- Tag type
- Data type
- Scope
- Class
- Style
- External Access
- If the tag value is a constant

The Studio 5000 Logix Designer® application helps prevent the direct creation of invalid tags in a safety program. If invalid tags are imported, they cannot be verified.

IMPORTANT: You cannot create a standard alias tag of a safety tag. Instead, standard tags can be mapped to safety tags using safety tag mapping. See [Standard Tags in Safety Routines on page 193](#).

The Logix Designer application can write to safety tags directly via the Tag Monitor when the controller is safety-unlocked, does not have a safety signature, and is operating without safety faults.

The controller does not allow writes to safety tag data from external human machine interface (HMI) devices or via message instructions from peer controllers. HMI devices can have read-only access to safety tags depending on the External Access setting.

Valid Data Types

The data type defines the type of data that the tag stores, such as bit or integer.

Data types can be combined to form structures. A structure provides a unique data type that matches a specific need. Within a structure, each individual data type is called a member. Like tags, members have a name and data type. You can create your own structures, such as arrays or user-defined data types.

Logix controllers contain predefined data types for use with specific instructions. Safety tags can be composed of the following:

- All primitive data types (for example, BOOL, SINT, INT, DINT, LINT, REAL)
- Predefined types used for safety application instructions
- User-defined data types or arrays that are composed of the two preceding types

Scope

The scope of a tag determines where you can access the tag data. When you create a tag, you define it as a controller tag (global data) or a program tag for a specific safety or standard program (local data).

Safety tags can be controller-scoped or safety program-scoped:

- Controller-scoped safety tags can be read by either standard or safety logic or external communication devices, but can be written by only safety logic or another GuardLogix controller.
- Program-scoped safety tags can be read by external communication devices, but only local safety routines within the safety program can write to them.

When you create program-scoped tags, the class is automatically specified, depending on whether you created the tag in a standard or a safety program. When you create controller-scoped tags, you must manually select the tag class.

When safety tags are controller-scoped, all programs have access to the safety data. Tags must be controller-scoped if they are used in the following ways:

- Multiple programs in the project
- In safety tag mapping
- To produce or consume data

Controller-scoped safety tags can be read, but not written to, by standard routines.

IMPORTANT: Safety input tags and safety consumed tags are readable by any standard routine, but the update rate is based on the execution of the safety task. These tags are updated at the beginning of the safety task execution, which differs from standard tag behavior.

Safety Signature Elements

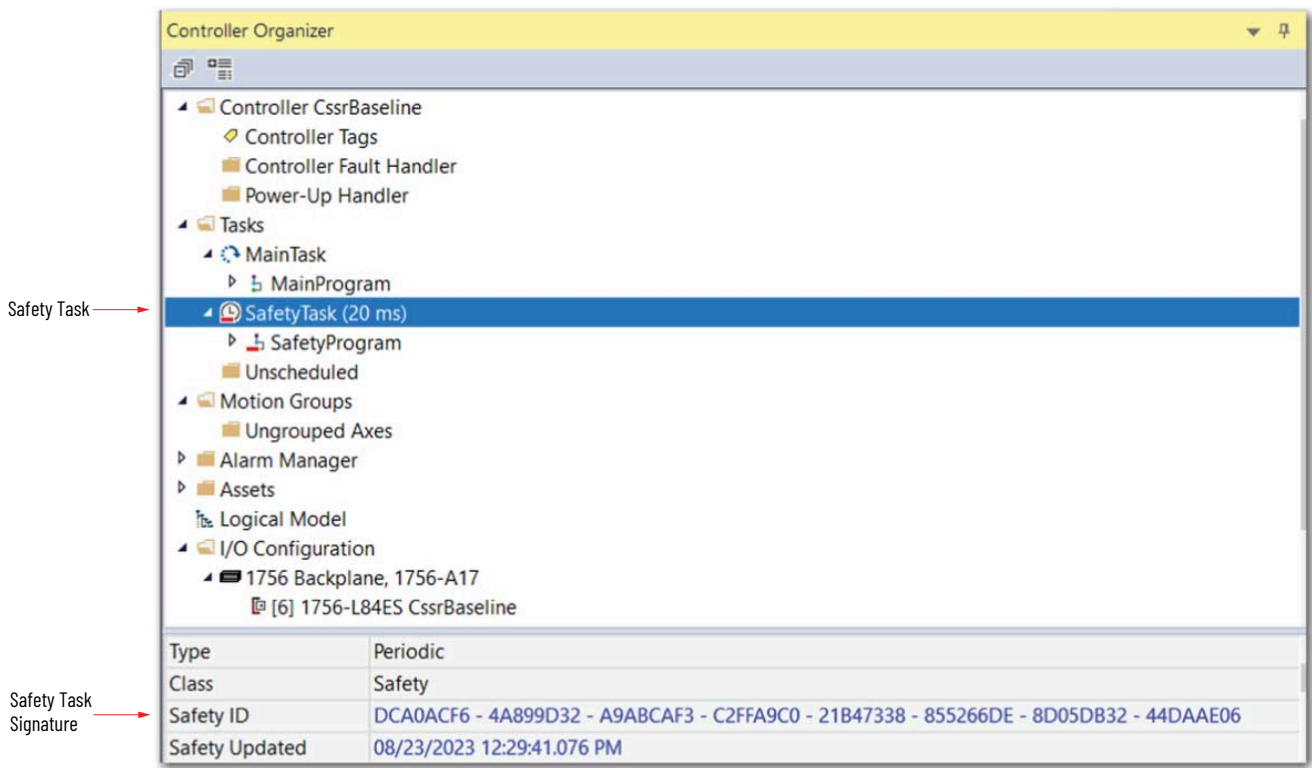
Safety signature elements include:

- Safety application
- Safety controller attributes
- Safety tags
- Tag mapping
- Safety task
- Safety programs
- Safety routines
- Safety add-on instructions
- Safety I/O device configuration

Each element has a safety signature. The signature changes when its associated element is modified and requires revalidation.

To view the safety signature for a safety tag, the safety task, or a safety program, select the element in the Controller Organizer. The safety signature ID and timestamp appear in the Quick View pane at the bottom of the Controller Organizer.

Figure 54. Safety Signature for Safety Task Element



Produced/Consumed Safety Tags

To transfer safety data between controllers, you use produced and consumed safety tags. Tags that are associated with safety I/O and produced or consumed safety data must be controller-scoped safety tags. For produced/consumed safety tags, you must create a user-

defined data type with the first member of the tag structure that is reserved for the status of the connection. This member is a predefined data type called CONNECTION_STATUS.

Table 53. Produced and Consumed Connections

Tag	Connection Description
Produced	Controllers can produce (send) safety tags to other controllers: • Controllers only support unicast produced tags. • Controllers do support producing a tag to up to 15 consumers if all consumers are configured to consume the tag unicast. • The producing controller uses one connection for each consumer. • The consuming controller must be at firmware revision 19 or later. Unicast was not added to safety produced/consumed tags until firmware revision 19.
Consumed	Controllers can consume (receive) safety tags from other controllers in these configurations: • If you have a ControlLogix® 5590 controller (the producer) in the I/O tree of another ControlLogix® 5590 controller (the consumer), then the consumer can only consume a tag from the producer if the tag is unicast. • If you have a GuardLogix® 5580 controller (the producer) in the I/O tree of another GuardLogix® 5580 controller (the consumer), then the consumer can only consume a tag from the producer if the tag is unicast. • If the producer controller is a GuardLogix® 5570 controller, then a consumer controller can consume multicast or unicast tags. • Each consumed tag consumes one connection.

Produced and consumed safety tags are subject to the following restrictions:

- Only controller-scoped safety tags can be shared.
- Produced and consumed safety tags are limited to 128 bytes.
- Produced/consumed tag pairs must be of the same user-defined data type.
- The first member of that user-defined data type must be the predefined CONNECTION_STATUS data type.
- The requested packet interval (RPI) of the consumed safety tag must match the safety task period of the producing GuardLogix® controller.

To configure produced and consumed safety tags to share data between peer safety controllers, you must properly configure the peer safety controllers, produce a safety tag, and consume a safety tag. See [Configure the SNN for a Peer Safety Controller Connection](#).

Configure the SNN for a Peer Controller Connection

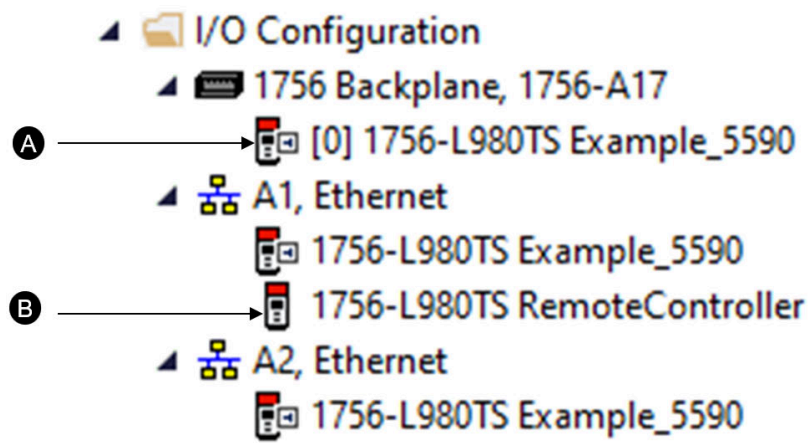
The peer controller is subject to the same configuration requirements as the local controller. The peer controller must also have a safety network number (SNN). The safety application that is downloaded into the peer controller configures SNN values for each CIP Safety™ port on the controller.

Table 54. SNN and Controller Placement

Peer Controller Location	SNN
Placed in the local chassis	The user application on the peer controller generates an SNN value for the local backplane port of the controller.
Placed in another chassis	The controller must have a unique SNN.

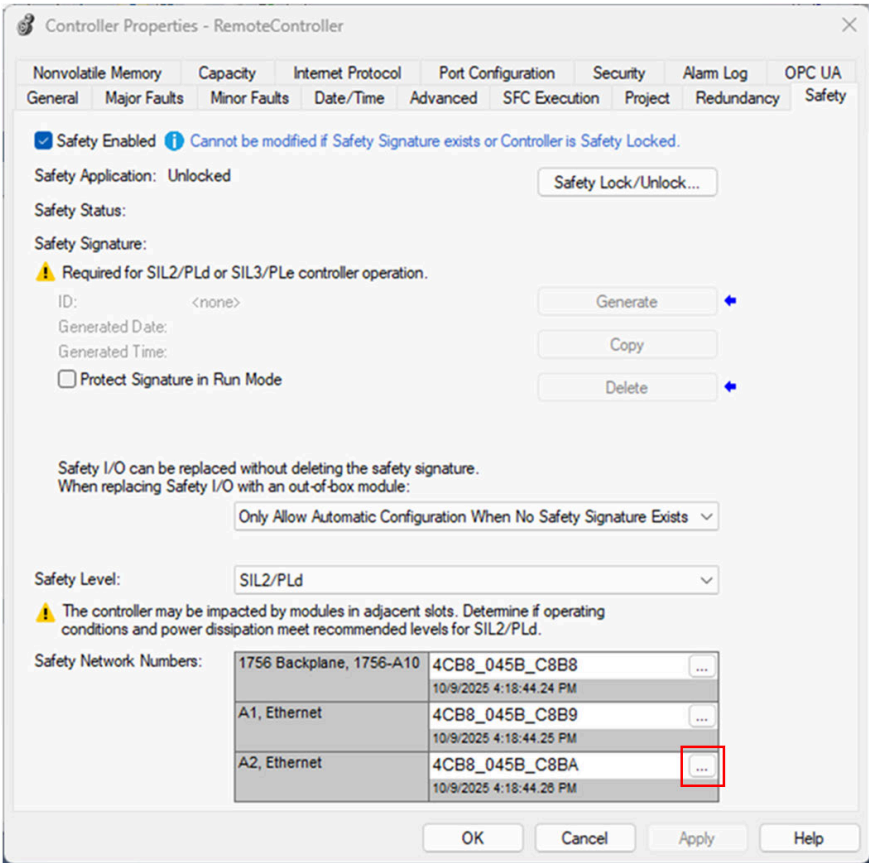
Setting the correct SNNs of the controller usually results in the producer controller being assigned the correct SNN. If the automatically assigned SNN of the producer controller does not match the SNN that the controller uses, you can follow these steps to copy and paste the SNN.

1. Add the producer controller to the consumer controller's I/O tree.

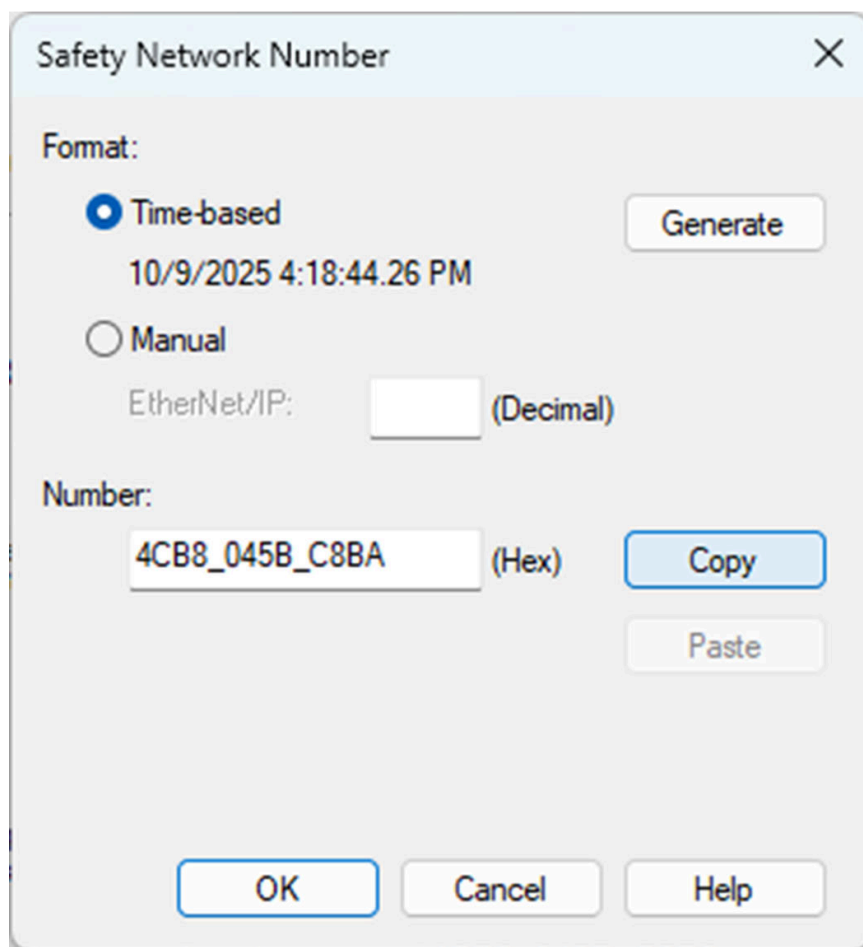


Item	Description
A	Consumer controller
B	Producer controller

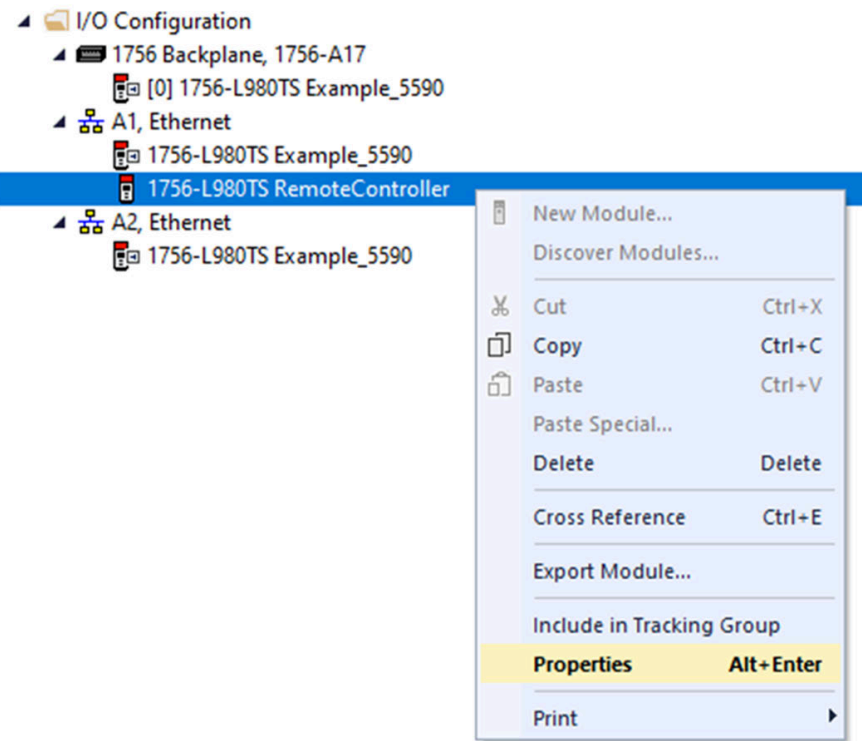
2. In the producer controller's project, right-click the producer controller and select Controller Properties.
3. On the Safety tab, select Browse (...) next to the port that communicates with the consumer controller.



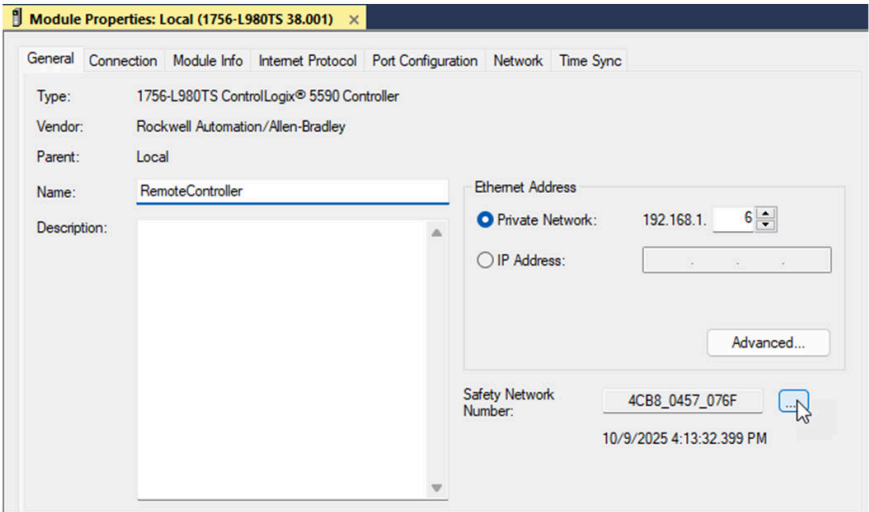
4. On the Safety Network Number dialog box, copy the producer controller’s SNN.



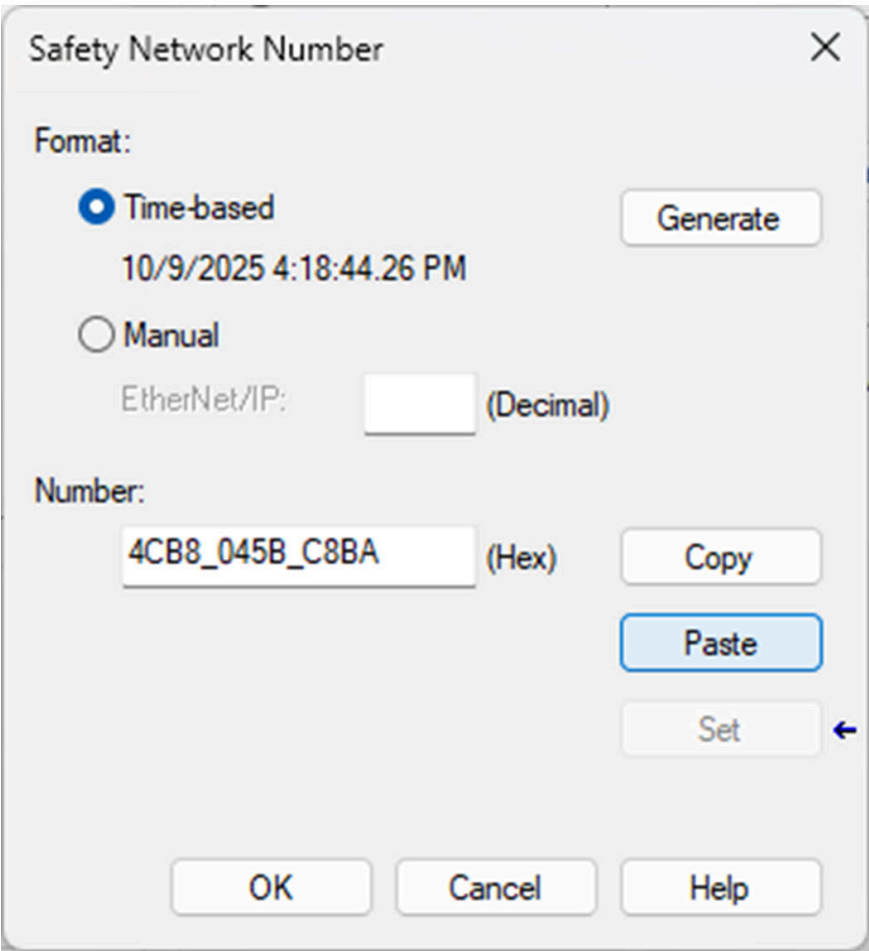
5. In the I/O tree of the consumer controller's project, right-click the module that represents the producing controller, and select Module Properties.



- 6. On the General tab of the Module Properties dialog box, select Browse (...) to open the Safety Network Number dialog box.

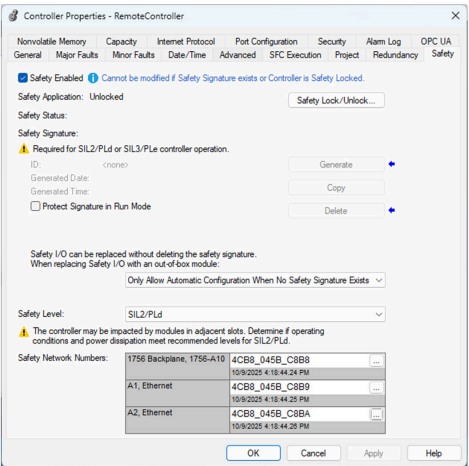


- 7. On the Safety Network Number dialog box, paste the producer controller's SNN into the SNN field and click OK.

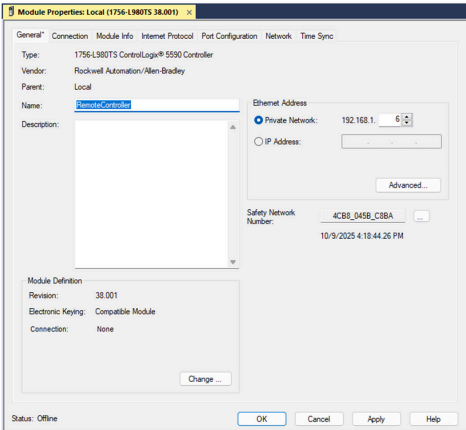


The safety network numbers in the producer and consumer projects now match.

Producer Controller Properties Dialog Box in Producer Project



Module Properties Dialog Box in Consumer Project



Produce a Safety Tag

Complete these steps to produce a safety tag.

1. In the project of the producing controller, create a user-defined data type that defines the structure of the data to be produced.
Make sure that the first data member is of the CONNECTION_STATUS data type.
2. Right-click Controller Tags and select New Tag.
3. On the New Tag dialog box, set the type as Produced, the class as Safety, and the data type to the user-defined data type that you created.

New Tag [X]

Name: Create ▼

Description:

Usage:

Type: Connection...

Alias For:

Data Type: ...

Parameter Connection:

Scope:

Class:

External Access:

OPC UA Access:

Style:

☐ Constant

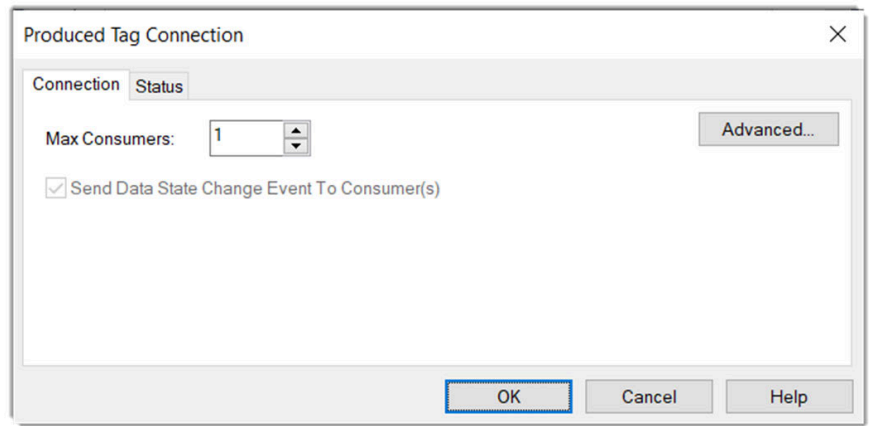
☐ Sequencing

☐ Open Configuration

☐ Open Parameter Connections

Cancel Help

4. Click Connection and enter the max limit on the number of consumers (1...15).



5. Click OK.
6. Click Create.

Consume Safety Tag Data

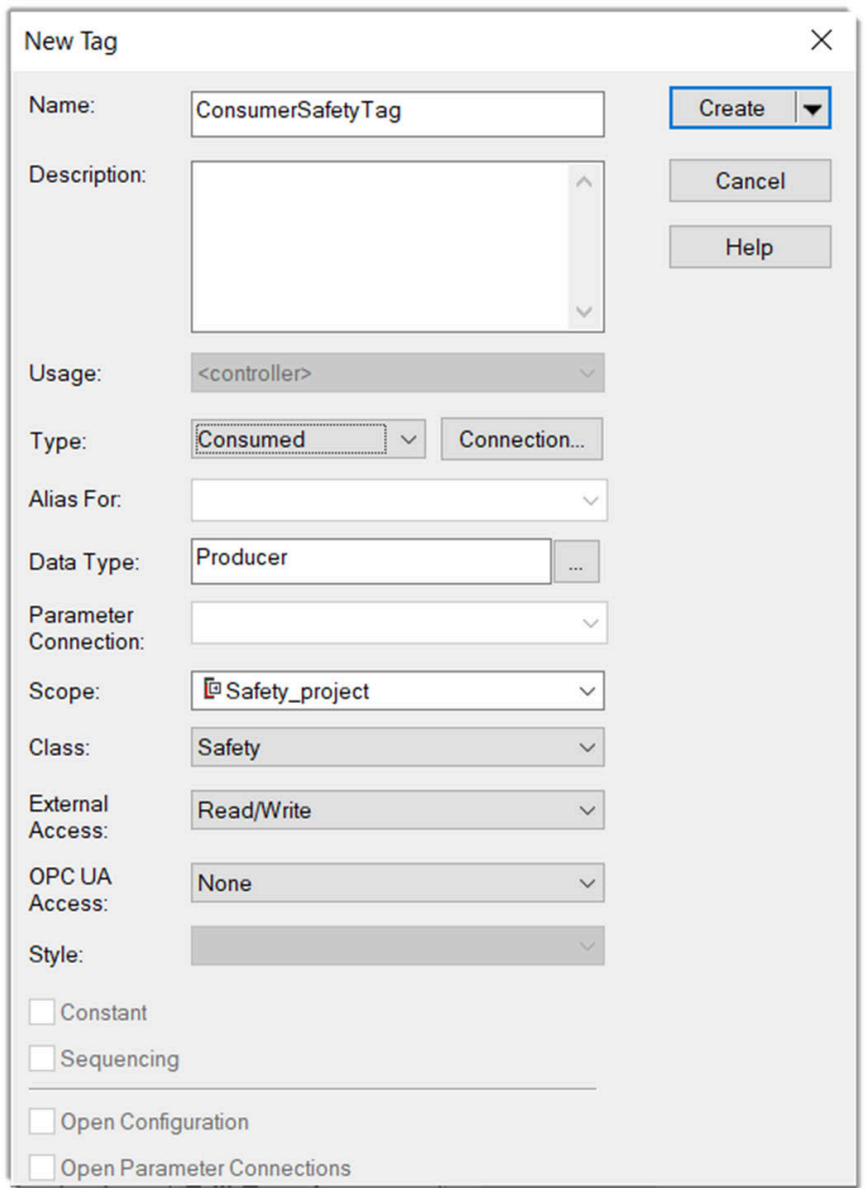
Follow these steps to consume data produced by another controller.

1. In the project of the consumer controller, create a user-defined data type identical to the one created in the project of the producer controller.
The names of the user-defined data types must match.



The user-defined data type can be copied from the producer project and pasted into the consumer project.

2. Right-click Controller Tags and select New Tag.
3. On the New Tag dialog box, set the type as Consumed, the class as Safety, and the data type to the user-defined data type that you created.

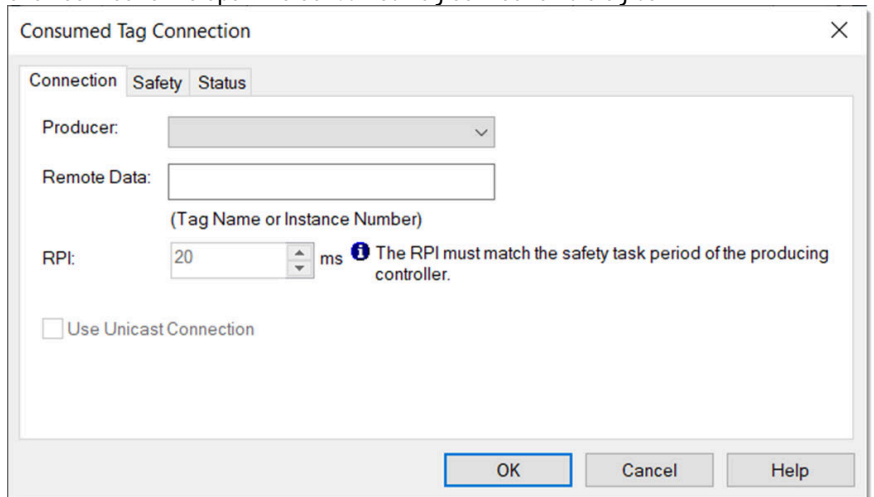


The 'New Tag' dialog box is used to configure a new tag. It contains the following fields and options:

- Name:** ConsumerSafetyTag
- Description:** (Empty text area)
- Usage:** <controller>
- Type:** Consumed (with a 'Connection...' button)
- Alias For:** (Empty dropdown)
- Data Type:** Producer
- Parameter Connection:** (Empty dropdown)
- Scope:** Safety_project
- Class:** Safety
- External Access:** Read/Write
- OPC UA Access:** None
- Style:** (Empty dropdown)
- ☐ Constant
- ☐ Sequencing
- ☐ Open Configuration
- ☐ Open Parameter Connections

Buttons: Create, Cancel, Help

4. Click Connection to open the Consumed Tag Connection dialog box.



The 'Consumed Tag Connection' dialog box is used to configure the connection for a consumed tag. It contains the following fields and options:

- Connection:** Safety (selected)
- Producer:** (Empty dropdown)
- Remote Data:** (Empty text field)
- RPI:** 20 ms
- Use Unicast Connection:** ☐

Buttons: OK, Cancel, Help

5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.

7. Click the Safety tab.
8. In the Requested Packet Interval (RPI) field, enter the RPI for the connection in 1 ms increments. The default is 20 ms.
 - The RPI specifies the period when data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.
 - The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, you can achieve an acceptable Connection Reaction Time Limit by adjusting the safety task period of the producing controller which adjusts the RPI.
 - The Max Network Delay is the maximum observed transport delay from the time that the data was produced until the time the data was received. When online, click Reset Max to reset the Max Network Delay.
9. If the Connection Reaction time limit is acceptable, click OK.
If a safety consumed tag has the error code: "16#0111 Requested Packet Interval (RPI) out of range," check that the consumed tag RPI matches the producer's safety task period.
10. If your application has more complex requirements, click Advanced on the Safety tab to access the Advanced Connection Reaction Time Limit parameters.
 - The Timeout Multiplier determines the number of RPIs to wait for a packet before declaring a connection timeout.
 - The Network Delay Multiplier defines the message transport time that is enforced by the CIP Safety protocol. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and back to the producer.

You can use the Network Delay Multiplier to increase or decrease the Connection Reaction Time Limit.



ATTENTION: If you decrease the timeout multiplier or network delay multiplier below the defaults, this could cause nuisance safety connection losses. Wireless networks can require you to increase the values above the default.

Advanced Connection Reaction Time Limit Configuration

Requested Packet Interval (RPI):	20	ms (1 - 500)
Timeout Multiplier:	2	(1 - 4)
Network Delay Multiplier:	200	% of RPI (10 - 600%)
Connection Reaction Time Limit	80.0	ms

OK Cancel Help

Standard Tags in Safety Routines (Tag Mapping)

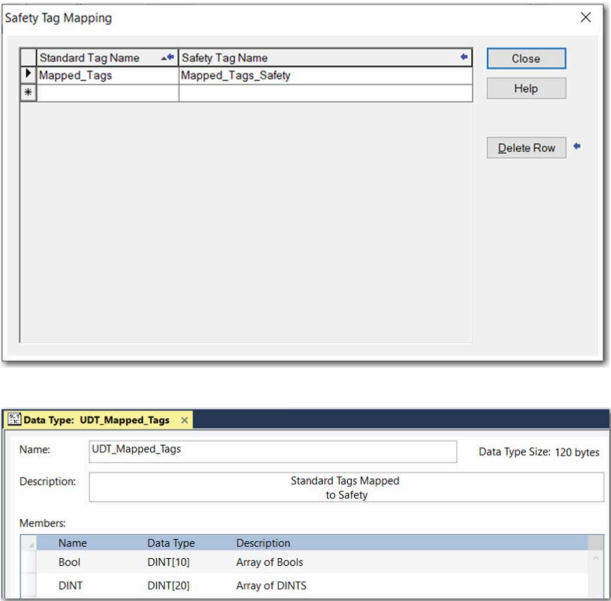
A safety routine cannot directly access standard tags. To allow standard tag data to be used within safety routines and synchronize standard and safety actions, safety controllers provide a safety tag-mapping feature that copies standard tag values into safety task memory.

Mapped tags are copied from the standard tags to their corresponding safety tags at the beginning of the safety task. The copying process can increase the safety task scan time.

 Standard task routines can directly read safety tags.

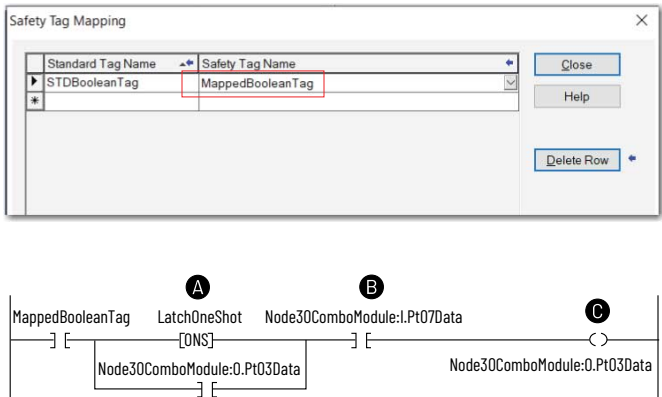
Because a download is required to change tag mapping, mapping a structure of information provides programming standardization and flexibility during commissioning.

Figure 55. Mapped Tag Structure Example



The following example shows how to qualify standard data with safety data.

Figure 56. Qualify Standard Data with Safety Data



Item	Description
A	Latch circuit to help prevent automatic restart if the standard input (MappedTag) is failed in a 'stuck at 1' state.

Item	Description
B	Safety input qualifier for mapped tag
C	Safety output

Restrictions

Safety tag mapping has these restrictions:

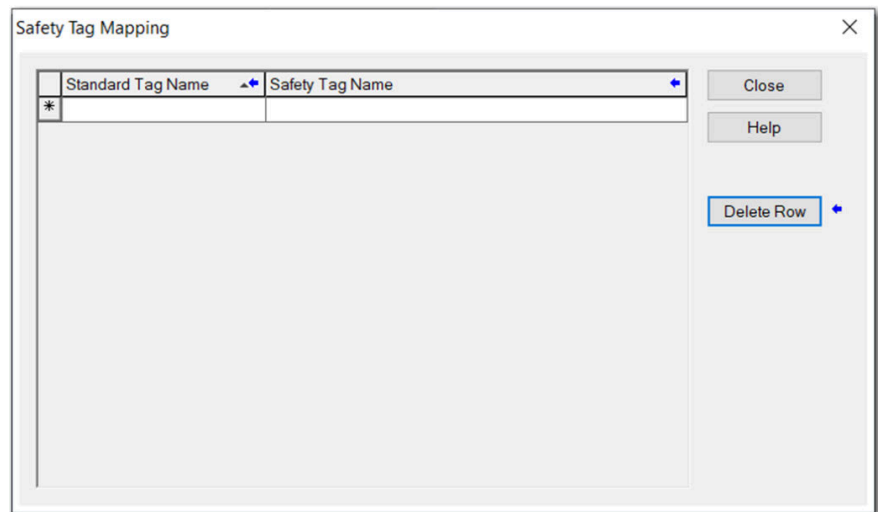
- The safety tag and standard tag pair must be controller-scoped.
- The data types of the safety and standard tag pair must match.
- Alias tags are not allowed.
- Mapping must take place at the whole tag level. For example, myTimer.pre is not allowed if myTimer is a TIMER tag.
- A mapping pair is one standard tag that is mapped to one safety tag.
- You cannot map a standard tag to a safety tag that has been designated as a constant.
- Tag mapping cannot be modified when any of the following are true:
 - The project is safety-locked.
 - A safety signature exists.
 - The controller switch is in RUN position.
 - A nonrecoverable safety fault exists.
 - An invalid partnership exists between the primary controller and safety partner.



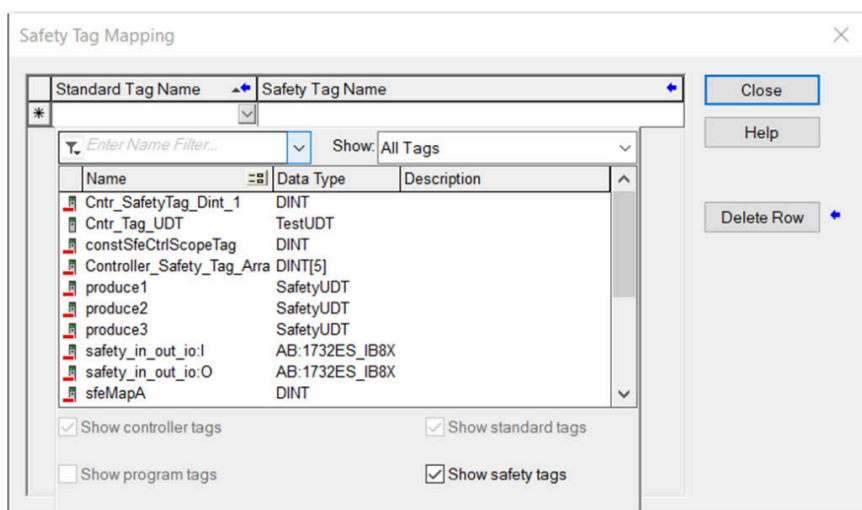
ATTENTION: If you use standard data in a safety routine, you must verify that the data is used in an appropriate manner. Standard data in a safety tag is not safety data. Do not directly control a SIL 2 or SIL 3 safety function by using standard data.

Create Tag Mapping Pairs

1. From the Logic menu, select Map Safety Tags.



2. In the Standard Tag Name or Safety Tag Name column, enter or select an existing tag:
 - To show only controller-scoped standard tags, click the arrow in the Standard Tag Name column.
 - To show only controller-scoped safety tags, click the arrow in the Safety Tag Name column.



3. In the Standard Tag Name or Safety Tag Name column, add a new tag:
 - a. Right-click in the empty cell.
 - b. Select New Tag.
 - c. Enter the tag name into the field.
4. Right-click the field and select New tagname, where tagname is the text you entered in the field.

Custom Tag Initialization During Prescan

Only safety tags that are configured as constant value tags are captured as part of the safety signature.

IMPORTANT: When you use non-constant safety tag values for a safety critical operation, you must initialize the non-constant safety tags before Run mode.

Give special consideration to instructions that use pseudo-operands, such as the following:

- .PRE value for TON, TOF, RTO, CTD, and CTU
- .LEN value for FAL and FSC

Unless modified by the application, pseudo-operands are initialized only once when the application is downloaded. For details, see the 'Pseudo-operand Initialization' online Help topic. Before the controller is in Run mode, you must initialize the .PRE and .LEN values for the preceding instruction tags and other non-constant safety tags that are used in a safety critical operation. Initialize these values by using one of these methods:

- A first scan subroutine
- An Add-On Instruction prescan routine

For more information about how to perform a custom tag initialization during prescan, see the Logix 5000 Controllers Design Considerations Reference Manual, publication [1756-RM094](#).

You can use the SaveSnapshot routine to copy non-constant safety tag values to the safetyPrescanInitUDT backup, which consists of safety tag types, such as CTU preset, FAL length, TON preset, DINT array, REAL, and BOOL. For example, once the application is downloaded and configured, toggle the saveSnapshot tag to call the SaveSnapshot routine to initialize safetyPrescanInitAOI. Upon subsequent transitions to RUN mode, the prescan routine of safetyPrescanInitAOI reinitializes the non-constant safety tag values from the safetyPrescanInitUDT backup.

Figure 57. Main Routine

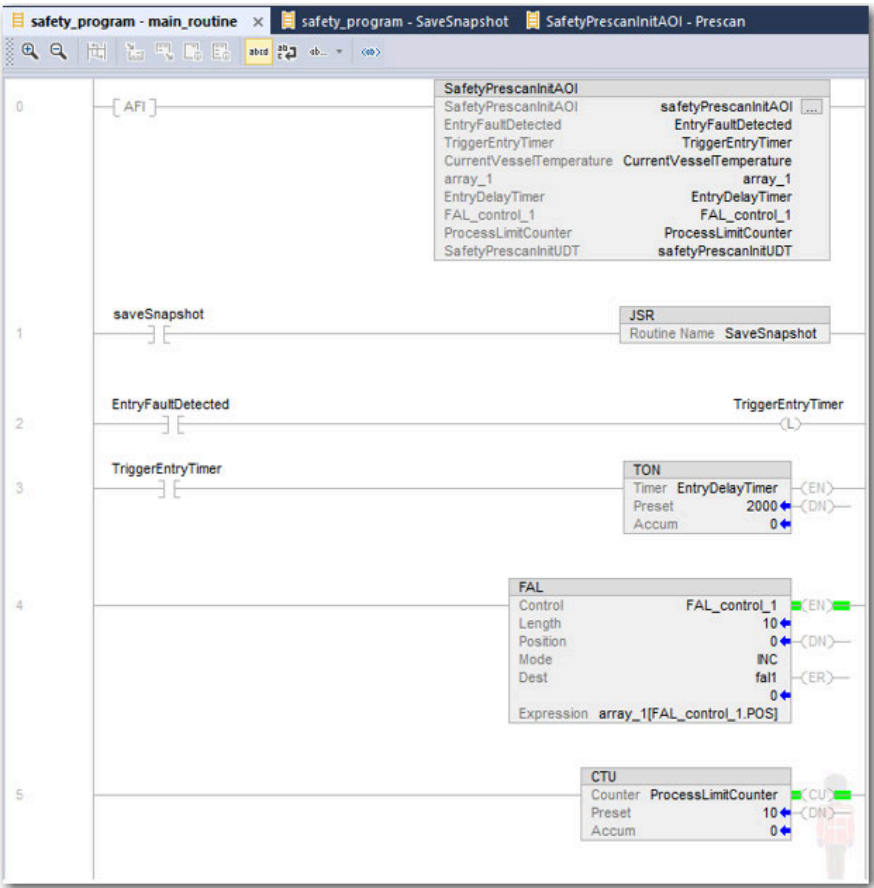


Figure 58. SaveSnapshot Routine

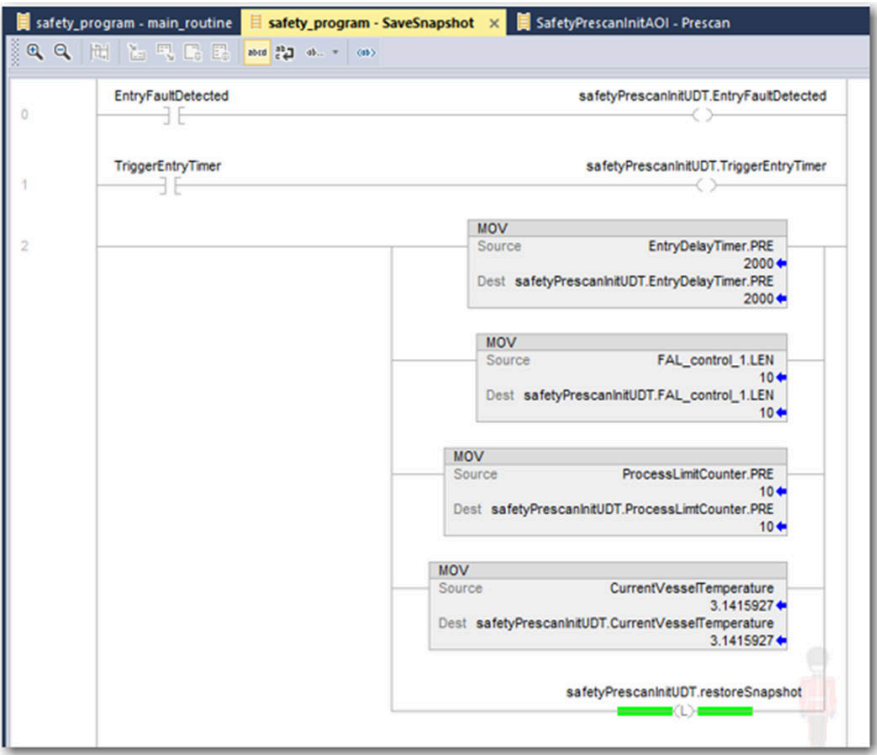
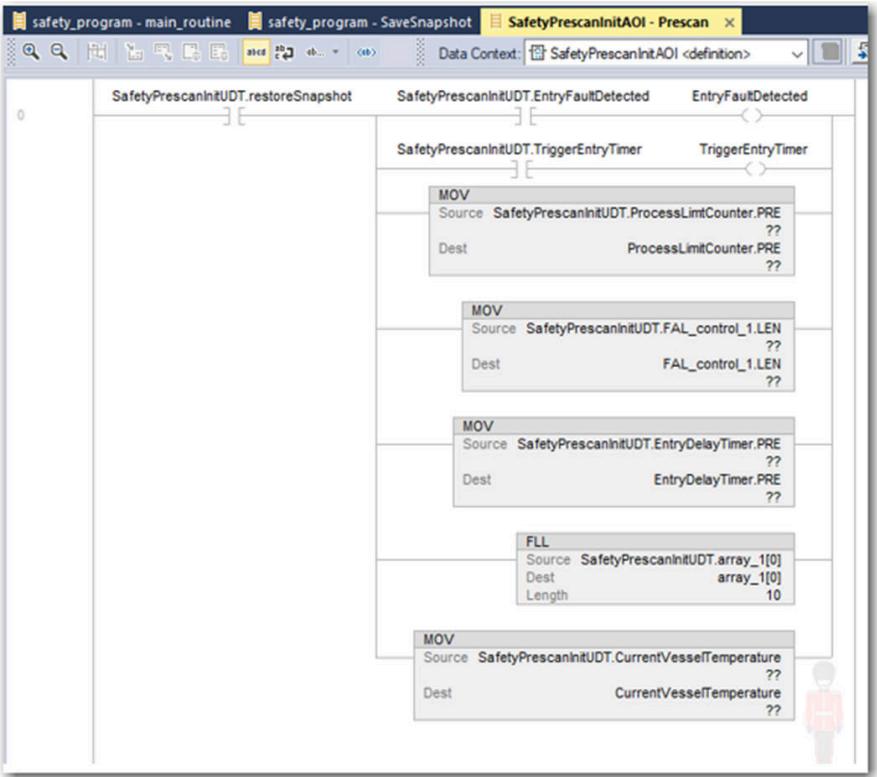


Figure 59. Add-On Instruction Prescan Initialization Routine



Safety Add-On Instructions

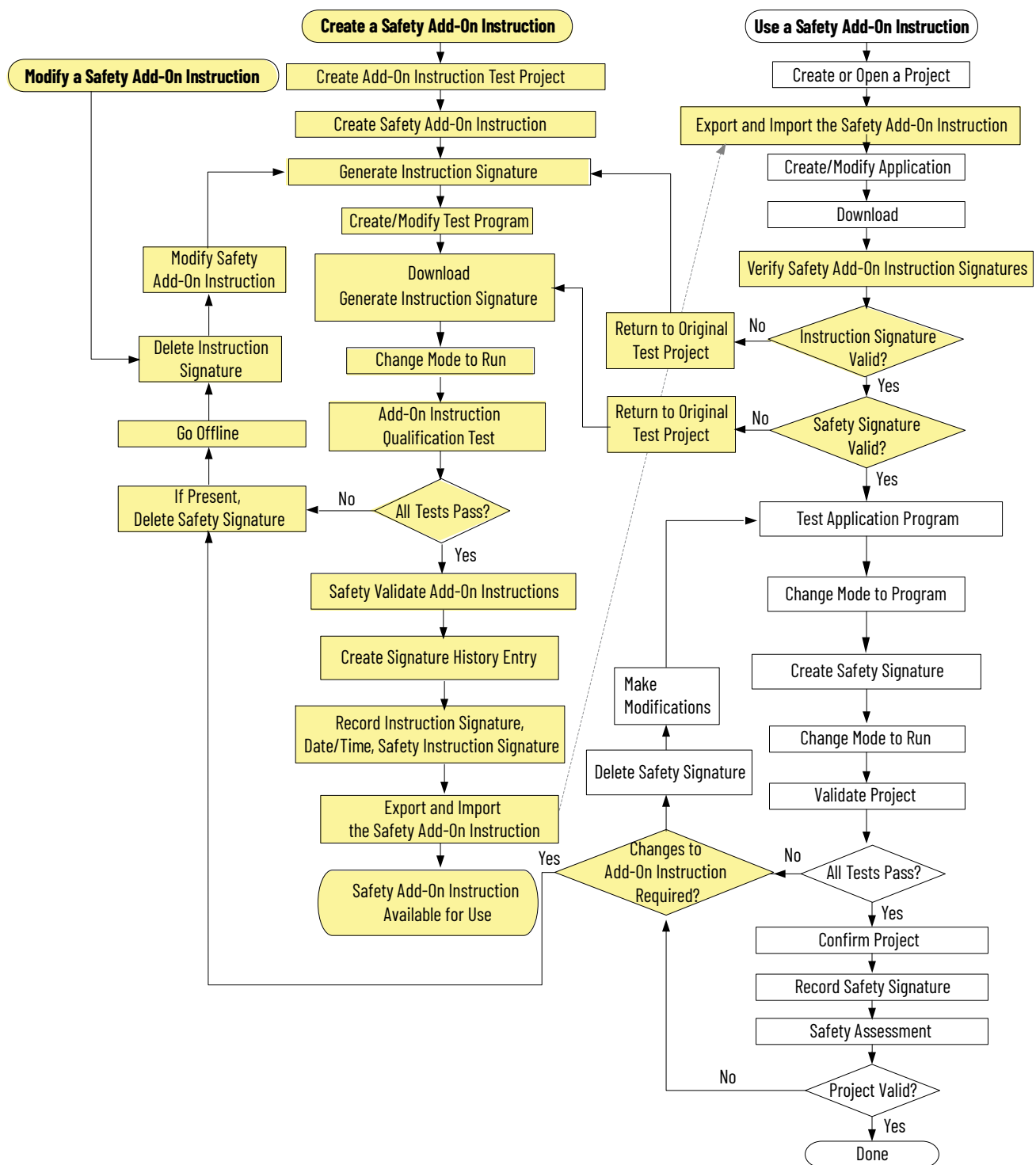
You can create safety Add-On Instructions to be used in safety applications. Safety Add-On Instructions enable you to put commonly used safety logic into one instruction, which makes it modular and easier to reuse. An Add-On Instruction is composed of parameters, local tags, logic routine, and optional scan-mode routines.

Safety Add-On Instructions feature a safety instruction signature for use in safety-related applications up to and including SIL 3-rated applications. The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction. The signature is used to verify the integrity of the safety Add-On Instruction during downloads to the controller.

IMPORTANT: You must initialize safety critical Add-On Instruction tag values in the Add-On Instruction prescan logic.

The following figure shows the steps that are required to create a safety Add-On Instruction and then use that instruction in a safety application program. The shaded items are steps unique to Add-On Instructions.

Figure 60. Safety Add-On Instruction Workflow



Create an Add-On Instruction Test Project

You must create a unique test project to create and test the safety Add-On Instruction. This project must be a separate and dedicated project to minimize any unexpected influences. Follow the guidelines for projects that are described in [Create the Project on page 205](#).

Create a Safety Add-On Instruction

For guidance in how to create Add-On Instructions, see the Logix 5000 Controllers Add-On Instruction Programming Manual, publication [1756-PM010](#).

Generate the Instruction Signature

The instruction signature consists of an ID number and time stamp that identifies the contents of the Add-On Instruction at a given point in time. The source of the date and time is from the local clock on the computer generating the signature.

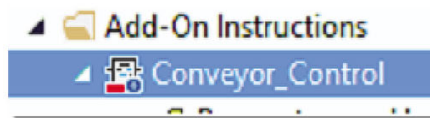
The instruction signature enables you to quickly determine if the instruction has been modified. Each Add-On Instruction can have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and can sometimes be required for regulated industries. Use it when your application calls for a higher level of integrity.

Once generated, the instruction signature seals the Add-On Instruction, which helps prevent it from being edited while the signature is in place. This restriction includes rung comments, tag descriptions, and any instruction documentation that was created. When the instruction is sealed, you can perform only these actions:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

When you generate an instruction signature, the Studio 5000 Logix Designer® application displays the instruction definition with the seal icon.

Figure 61. Add-On Instruction Icon



IMPORTANT: If you protect your Add-On Instruction with the source protection feature in the Studio 5000 Logix Designer® application, enable source protection before you generate the instruction signature.

When you generate a safety signature for a controller project, the Quick View Pane and Safety Signature Report show a safety signature element for Add-On Instructions even if the instruction signature is not generated. For more information about safety signature elements, see [Safety Signature on page 217](#).

When a sealed safety Add-On Instruction is downloaded for the first time, a safety instruction signature is automatically generated.

IMPORTANT: Checking or clearing the Report Overflow Faults checkbox in the controller properties changes the safety instruction signature ID for safety Add-On Instructions that include math instructions.

Safety Add-On Instruction Qualification Tests

Safety Add-On Instruction tests must be performed in a separate, dedicated application to verify that unintended influences are minimized. You must follow a well-designed test plan and

perform a unit test of the safety Add-On Instruction that exercises all possible execution paths through the logic, including the valid and invalid ranges of all input parameters.

An independent, third-party review of the safety Add-On Instruction can be required before the instruction is approved for use. An independent, third-party validation may be required for functional safety certification.

Create Signature History Entry

The signature history provides a record for future reference. A signature history entry consists of the instruction signature, the name of the user, the time stamp value, and a user-defined description. Up to six history entries can be stored. You must be offline to create a signature history entry.



The Signature Listing report in the Studio 5000 Logix Designer® application prints the instruction signature, the time stamp, and the safety instruction signature. To print the report, right-click Add-On Instruction in the Controller Organizer and choose Print > Signature Listing.

Export and Import the Safety Add-On Instruction

When you export a safety Add-On Instruction, choose the option to include all referenced Add-On Instructions and user-defined data types in the same export file. By including referenced Add-On Instructions, you make it easier to preserve the signatures. When importing Add-On Instructions, consider these guidelines:

- You cannot import a safety Add-On Instruction into a standard controller project.
- You cannot import a safety Add-On Instruction into a safety controller project that has been safety-locked or one that has a safety signature.
- You cannot import a safety Add-On Instruction while online.
- If you import an Add-On Instruction with an instruction signature into a project where referenced Add-On Instructions or user-defined data types are not available, you may need to remove the signature.

For more information, see the Import/Export Project Components Programming Manual, publication [1756-PM019](#).

Qualification and Verification

After you download the application project that contains the imported safety Add-On Instruction, you must compare the instruction signature value, the date and time stamp, and the safety instruction signature values with the original values you recorded before you exported the safety Add-On Instruction. If they match, the safety Add-On Instruction is valid and you can continue with the validation of your application.

Next, test the application program. This step consists of any combination of Run and Program mode, online or offline program edits, upload and download, and informal testing that is required to get an application to run properly.

To validate the project, perform an engineering test of the application, including the safety system. For more information about requirements, see [Validate the Project on page 207](#).

An independent, third-party review of the safety system can be required before the system is approved for operation. An independent, third-party validation may be required for functional safety certification.

Safety Programming Considerations

Complete these programming tasks for safety applications:

- Define the location, ownership, and configuration of I/O devices and controllers.
- Create, test, and debug program logic. Only ladder diagram is supported in the safety task.

IMPORTANT: When the controller is in Run or Program mode and you have not validated the application program, you are responsible for maintaining safe conditions.

Programming Restrictions

The Logix Designer application limits the availability of some menu items and features, such as cut, paste, delete, and replace, to protect safety components from being modified whenever any of these are true:

- The controller is safety-locked
- A safety signature exists
- Safety faults are present
- Safety status is in any of these states when online:
 - Partner missing
 - Partner unavailable
 - Hardware incompatible
 - Firmware incompatible

IMPORTANT: The maximum and last scan times of the safety task and safety programs can be reset when online.

If even one of these conditions applies, you cannot do the following:

- Create or modify safety objects, including safety programs, safety routines, safety tags, safety Add-On Instructions, and safety I/O devices
- Apply forces to safety tags
- Create safety tag mappings
- Modify or delete tag mappings
- Modify or delete user-defined data types that are used by safety tags
- Modify the controller name, description, chassis type, slot, and safety network number
- Create, modify, or delete a safety connection

When the controller is safety-locked, you cannot modify or delete the safety signature.

Application Development and Testing

We recommend that a user who is trained and experienced in safety applications develop the application program for the intended SIL 2 or SIL 3 system. The developer must follow good design practices:

- Use functional specifications, including flowcharts, timing diagrams, and sequence charts.
- Perform a review of safety task logic.
- Perform application validation.

As you develop your safety application, consider the following.

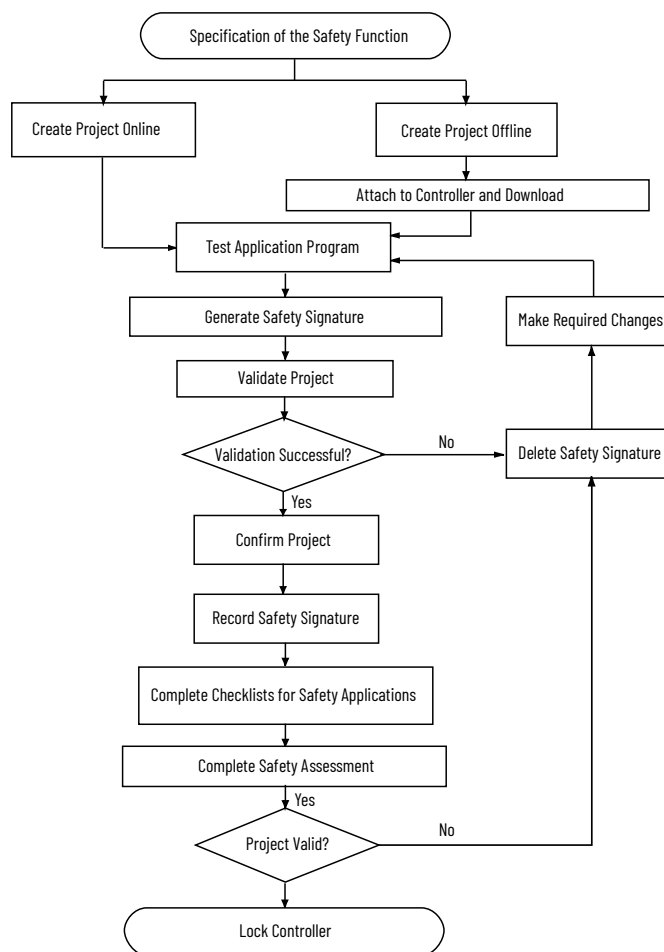
IMPORTANT:

- The programming application has been certified to clause 7.4.4 of IEC 61508-3 Edition 2 and can be used during the coding lifecycle of controller-based applications and also as an aide in the module test, integration test, and validation test lifecycle phases. As a result, no additional justification for its use during those lifecycle phases is required. If, however, other tools are used, either on their own or with the application, additional justification for those other tools are required. It is your responsibility to verify that other offline tools that are used during all lifecycle phases are selected as a coherent part of the software development activities.
 - It is your responsibility to conduct an assessment to determine the level of reliance that is placed on the programming application and the potential failure mechanisms that can affect the executable software when the application is used in a manner other than what is specified in the product documentation.
 - You must verify that all programming and configuration information that is entered into the programming application, and downloaded to the controller, meets the requirements for your application. See [Confirm the Project on page 208](#).
 - As required by the safety integrity level, the software or design representation must match the characteristics of the application.
 - As required by the safety integrity level, the software or design representation must be compatible with the features that are supported in the programming application and controllers. It is your responsibility to verify that the desired software and design representation are supported in the application and controllers. For example, if the design is represented in a flowchart format, it is your responsibility to convert that design to a ladder diagram.
 - Use of third-party, or internally developed, tools to generate logic automatically to import into the programming application for compilation and download to a controller requires assessment of its suitability at the point in the development cycle where it is selected.
-

Commissioning Lifecycle

The flowchart shows the steps that are required for commissioning a safety system.

IMPORTANT: To achieve IEC-62443-4-2 SL 1 security certification, you must enable CIP Security™ before you download a safety application to the controller.

Figure 62. Commission a Safety System

Specification of the Safety Function

You must create a specification for your safety function. Use this specification to verify that program logic correctly and fully addresses the functional and safety control requirements of your application. In some applications, the specification can be presented in various formats. However, the specification must be a detailed description that includes the following (if applicable):

- Sequence of operations
- Flow and timing diagrams
- Sequence charts
- Program description
- Program printout
- Written descriptions of the steps with step conditions and actuators to be controlled, which includes the following:
 - Input definitions
 - Output definitions
 - I/O wiring diagrams and references
 - Theory of operation
- Matrix or table of stepped conditions and the actuators to be controlled, including the sequence and timing diagrams
- Definition of marginal conditions, for example, operating modes and emergency stop

The I/O portion of the specification must contain the analysis of field circuits:

- Sensors (digital or analog)
 - Signal in standard operation (dormant current principle for digital sensors, sensors OFF means no signal)
 - Determination of redundancies that are required for SIL levels
 - Discrepancy monitoring and visualization, including your diagnostic logic
- Actuators
 - Position and activation in standard operation (normally ON)
 - Safe reaction/positioning when switching OFF or power failure
 - Discrepancy monitoring and visualization, including your diagnostic logic

Create the Project

The logic and instructions that are used in programming the application must be the following:

- Easy to understand
- Easy to trace
- Easy to change
- Easy to test

Review and test all logic. Keep safety-related logic and standard logic separate.

Use these labels to identify the application program clearly:

- Name
- Date
- Revision
- Any other useful identification

Test the Application Program

This step consists of any combination of Run and Program modes, online or offline edits, upload and download, and informal testing that is required to get an application to run properly in preparation for the Project Validation test.

Generate the Safety Signature

The safety signature is composed of a safety signature ID and a time stamp. The safety signature ID applies to the entire safety portion of the controller and uniquely identifies each project, including its logic, constant data, and configuration.



ATTENTION: The safety signature is required for the controller to operate at a SIL 2 or SIL 3 rating. Controller operation without a safety signature is only suitable during development.

Before you generate the safety signature, make sure the following requirements are met:

- Your programming tests are complete, but verification testing has not begun.
- The programming software is online with the controller.
- With firmware revision 38 or later, the controller can be in Remote Run, Program/Remote Program, or Remote Test mode. If your controller supports firmware revision 37 or earlier, the controller must be in Program/Remote Program mode.



ATTENTION: When the controller is in Program mode, outputs are commanded to their Program mode state.

- The controller is safety-unlocked.
- The controller has no safety forces or pending online safety edits.
- If a constant safety tag value was changed online, the project must be saved with an upload of the online tag values.
- The safety task status is OK.

IMPORTANT: When the safety application has been validated, there can be scenarios that require a redownload even though the safety application has not changed. For example, you make changes to the standard application, but not the safety application.

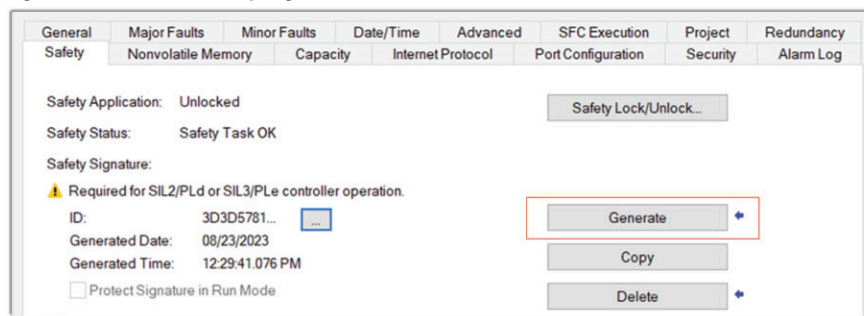
To verify that the correct safety application is downloaded, manually record the safety signature after initial creation and check the safety signature after every download to make sure that it matches the original sign.

You can generate the safety signature in three ways:

- From the Safety tab of the Controller Properties dialog box, click Generate, as shown in the figure below.
- From the Tools menu, select Safety > Generate Signature.
- From the Safety Status menu, select Generate Signature.

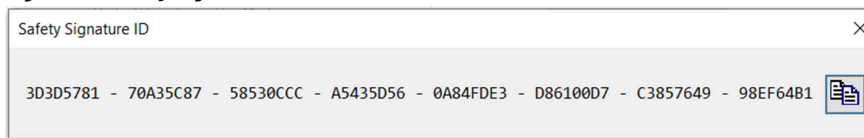
The programming application automatically uploads the safety signature after it is generated.

Figure 63. Generate Safety Signature



To view and copy the entire 64-character signature ID, click the Ellipse button next to the ID to open the Safety Signature ID dialog box.

Figure 64. Safety Signature ID



Safety signature creation and deletion are logged in the controller log. For more information on accessing the controller log, refer to Logix 5000 Controllers Information and Status Programming Manual, publication [1756-PM015](#).

When a safety signature exists, the following actions are not permitted in the safety portion of the application:

- Online/offline programming or editing, including safety Add-On Instructions
- Force safety I/O
- Change the inhibit state of safety I/O or producer controllers from module properties
- Safety data manipulation, except by safety routine logic
- Download a new safety application

With Logix SIS, you can update the firmware when a safety signature exists by using the Redundancy System Update (RSU) process.

Copy the Safety Signature

You can use the Copy button to create a record of the safety signature for use in safety project documentation, comparison, and validation. When you click Copy, the safety signature ID, date, and time components are saved to the Windows® clipboard.

Delete the Safety Signature

If safety-related changes are required to an application that has a safety signature, the safety signature must be deleted.



ATTENTION: When you delete the safety signature, all safety functions are impacted and require additional safety measures while the safety signature is removed.

After you delete the safety signature, you must retest and revalidate your system at some level to meet SIL 2/PLd or SIL 3/PLe.

To delete the safety signature, click Delete. The safety signature cannot be deleted when the following is true:

- The controller is safety-locked.
- The controller is in Run mode with the switch set to RUN.
- The controller is in Run or Remote Run mode with Protect Signature in Run Mode enabled.

Validate the Project

To check your application program for adherence to the specification, you must generate a suitable set of test cases that cover the application. The set of test cases must be documented and retained as the test specification. To determine what to validate for your specific application, refer to IEC 61508 or your industry-specific safety standard.

You must include a set of tests to prove the validity of your application logic. These are tests within the defined value ranges, at the limits, or in invalid value ranges. The necessary number of test cases depends on safety application.

Active validation with field devices must also be included, as it is the only way to verify that the sensors and actuators in the system are wired correctly. Verify the operation of programmed functions by manipulating sensors and actuators manually.

You must also include tests to verify the reaction to wiring faults and network communication faults.

Project validation includes tests of fault routines, and input and output channels, to be sure that the safety system operates properly.

To perform a project validation test on the controller, you must perform a full test of your application. You must activate each sensor and actuator that is involved in every safety function. Be sure to test all shutdown functions, because these functions may not be exercised during normal operation.

Also, know that a project validation test is valid only for the specific application tested. If the safety application is moved to another installation, you must perform startup and project validation on the safety application in the context of the new sensors, actuators, wiring, networks, and control system physical equipment.

Revalidation Considerations

The IEC 61508 functional safety standard requires an impact analysis before you upgrade or modify components in a certified, functional safety system. Reference the standard to make sure that you fulfill all requirements as they relate to your application. Consider the following high-level information for impact analysis of safety controller software, hardware, and firmware modification:

- All major and minor firmware releases for safety controller systems are certified for use in safety applications. As part of the certification process, Rockwell Automation tests the safety-related firmware functions, such as the CIP Safety™ communication subsystems, which are 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 modifications.
 - Review the firmware release notes for changes in safety-related functionality.
 - Review the hardware and firmware compatibility in the Product Compatibility and Download Center (PCDC) to identify potential compatibility conflicts.
 - Plan, analyze, and document the impact of any modification, enhancement, or adaptation of your validated safety system.
 - As part of the upgrade process, remove and regenerate the safety signature.
- Based on the results of the safety impact analysis, choose the appropriate level of hardware and software revalidation. Use the Safety Signature report to determine which safety elements have been modified and require revalidation. If your validation plan does not require revalidation of unchanged elements, your certification effort can be reduced.

Confirm the Project

You must review the project and compare the uploaded safety I/O and controller configurations, safety data, and safety task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

If your application program contains a safety Add-On Instruction that has been sealed with an instruction signature, you must also compare the instruction signature, date/time, and safety instruction signature to the values you recorded when you sealed the Add-On Instruction.

The following steps illustrate one method for confirming the project.

1. While online with the controller, save the project.
2. Answer Yes to the Upload Tag Values prompt.
3. With the Studio 5000 Logix Designer® application offline, save the project with a new name, such as Offlineprojectname.acd, where 'projectname' is the name of your project.
This file is the new tested primary project file.
4. Close the project.
5. Move the original project archive file out of its current directory.
You can delete this file or store it in an archival location.
This step is required because if the Studio 5000 Logix Designer® application finds the projectname.acd in this directory, it correlates it with the controller project and does not perform an upload.
6. Upload the project from the controller.
7. Save the uploaded project as Onlineprojectname.acd, where 'projectname' is the name of your project.
8. Answer Yes to the Upload Tag Values prompt.

9. Use the Studio 5000 Logix Designer® Program Compare utility to perform these comparisons:
 - a. Compare all properties of the controller and CIP Safety™ I/O devices.
 - b. Compare all properties of the safety task, safety programs, and safety routines.
 - c. Compare all logic in the safety routines.
10. Verify that all controller and I/O configuration fulfills the requirements of your application specification.

Complete Checklists for Safety Applications

Complete the checklists located in the Checklists for Safety Applications Appendix.

Safety Assessment

An independent, third-party safety assessment can be required before the system is approved for operation. An independent, third-party certification can be required for IEC 61508 SIL 2 or SIL 3 levels.

Lock the Controller



ATTENTION: Safety-locking alone does not satisfy SIL 2/PLd or SIL 3/PLe requirements.

The default state of the controller is safety-unlocked. We recommend that you safety-lock the controller to help protect safety control components from modification and help prevent the safety signature from being deleted accidentally. However, safety-locking the controller is not a requirement for SIL 2 or SIL 3.

The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety tags, safety Add-On Instructions, safety I/O, and safety signature.

No aspect of safety can be modified while the controller is in the safety-locked state. When the controller is safety-locked, the following actions are not permitted in the safety task:

- Update the firmware without using the Redundancy System Update (RSU) process
- Online or offline programming or editing
- Forcing safety I/O
- Data manipulation of safety components except through routine logic or another controller
- Creating or editing safety Add-On Instructions
- Generating or deleting the safety signature

IMPORTANT: If a safety signature exists and the controller is safety-locked, only projects with a matching safety signature can be downloaded to the controller.

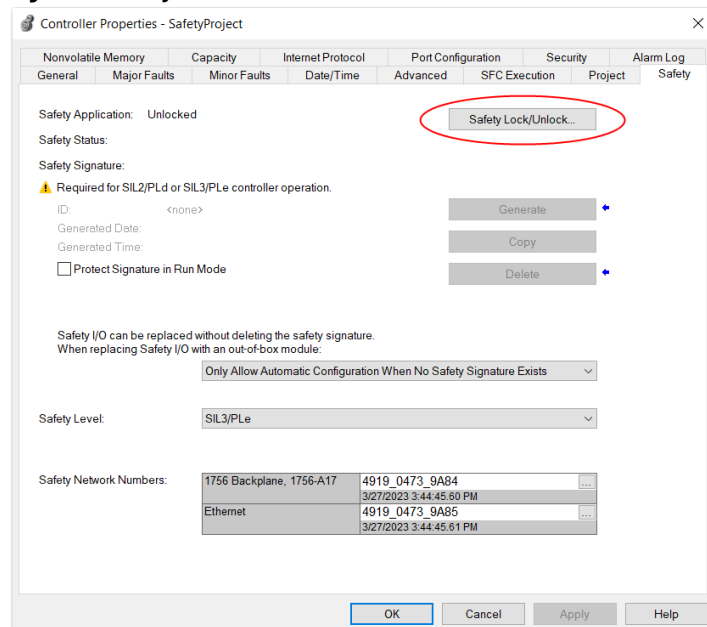
You can place the safety application in a safety-locked state regardless of whether you are online, offline, or you have the original program source. However, no safety forces or pending safety edits can be present. Safety-locked or -unlocked status cannot be modified when the keyswitch is in the RUN position.

Safety-lock and safety-unlock actions are logged in the controller log. For more information on accessing the controller log, see the Logix 5000 Controllers Information and Status Programming Manual, publication [1756-PM015](#).

You can change the safety-lock status in three ways:

- From the Safety tab of the Controller Properties dialog box.
- In the Studio 5000 Logix Designer® application, select Tools > Safety > Safety Lock/Unlock.
- From the Safety Status drop-down menu, select Safety Lock/Unlock.

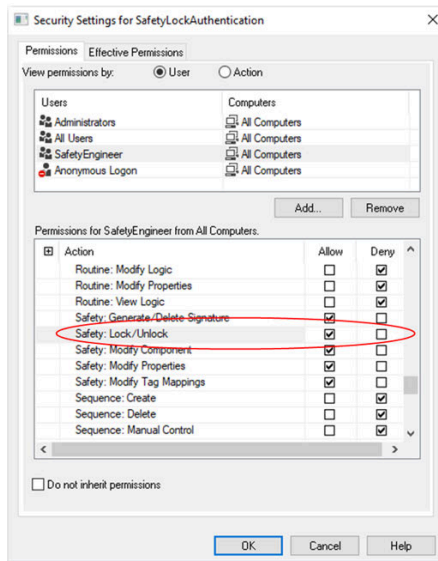
Figure 65. Safety Lock/Unlock Button



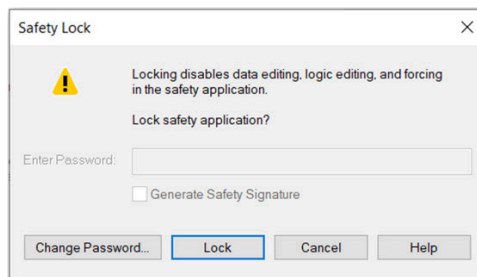
Restrict Access to Safety-lock and Safety-unlock Functionality

To provide additional layers of protection, you can use two methods to restrict access to safety-lock and safety-unlock functionality:

- **FactoryTalk Security**—To comply with IEC-62443-4-2 SL 1 security certification, you must use FactoryTalk Security to configure restricted access to safety-lock and safety-unlock actions. For information about setting these permissions, see the Configure System Security Features User Manual, publication [SECURE-UM001](#).



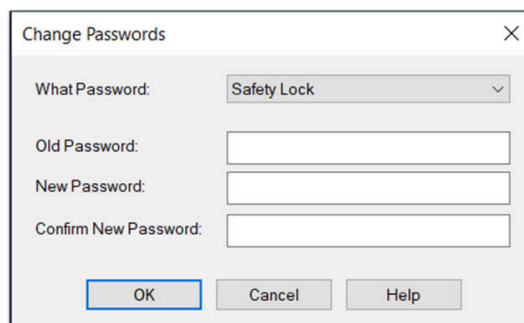
- Safety passwords—You can set separate passwords that are required to safety-lock or safety-unlock the controller. Passwords are optional and not required for IEC-62443-4-2 SL 1 security certification.



IMPORTANT: For added security, enable CIP Security on the controller before you set password protection. For non-redundant controllers, we recommend that you enable CIP Security on the front Ethernet port of the controller. For more information about CIP Security, see CIP Security with Rockwell Automation Products, publication [SECURE-AT001](#).

To set password protection for safety-lock or safety-unlock actions, follow these steps.

1. On the Logix Designer menu bar, click Tools > Safety > Change Passwords.
2. In the What Password field, select Safety Lock or Safety Unlock.



3. Enter the old password, if one exists.
4. Enter and confirm the new password.
5. Click OK.



Passwords can be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols can be used: ' ~ ! @ # \$ % ^ & * () _ + , - = { } [] \ : ; ? / . To clear an existing password, enter a new password of zero length.

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.

Download/Upload a Safety Application Program

Upon download, application testing is required unless a safety signature exists.

IMPORTANT: To verify that the correct safety application is downloaded or restored from a memory card, you must manually check that the safety signature matches the original signature in your safety documentation.

Downloads to a safety-locked controller are allowed only if the safety signature and the firmware revision of the offline project all match what is contained in the target controller and the safety task status of the controller is OK.

IMPORTANT: If the safety signature does not match and the controller is safety-locked, you must unlock the controller to download. In this case, downloading to the controller deletes the safety signature. As a result, you must revalidate the application.

IMPORTANT: To avoid project download failure, do not change the communication adapter name of a chassis containing safety I/O while the safety application has a safety signature.

If the controller contains a safety signature, the safety signature is uploaded in an online save of the project. The option to upload tag values includes both standard and safety tag values.

Store and Load a Project from a Memory Card

Safety controllers support firmware updates and user program storage and retrieval with a memory card. In a GuardLogix® system, only the primary controller uses a memory card.

When you store a safety project on a memory card, we recommend that you select Remote Program as the Load mode. The Load mode specifies the mode that the controller enters after a project load. Before system operation, operator intervention is required to start the controller.

You can initiate a load from a memory card only under these conditions:

- If the controller type specified by the project that is stored on the memory card matches your controller type.
- If the major and minor revisions of the project on the memory card match the major and minor revisions of your controller.

IMPORTANT: A revision mismatch helps prevent only user-initiated loads. Controller-initiated loads overwrite the firmware on the controller with the contents of the memory card.

- If your controller is not in Run mode.

Loading a project to a safety-locked controller is allowed only when the safety signature of the project that is stored on the memory card matches the project on the controller. If the signatures do not match or the controller is safety-locked without a safety signature, you must first unlock the controller before attempting to update the controller via a memory card.

IMPORTANT: If you unlock the controller and initiate a load from the memory card, the safety-lock status, passwords, and safety signature are then set to the values contained on the memory card once the load is complete.

Force Data

All data that is contained in an I/O, produced, or consumed safety tag, including CONNECTION_STATUS, can be forced while the project is safety-unlocked and no safety signature exists. However, forces must be removed, not just disabled, on all safety tags before the safety project can be safety-locked or a safety signature can be generated. You cannot force safety tags while the project is safety-locked or when a safety signature exists.

 You can install and remove forces on standard tags regardless of the safety-locked or safety-unlocked state.

Inhibit a Device

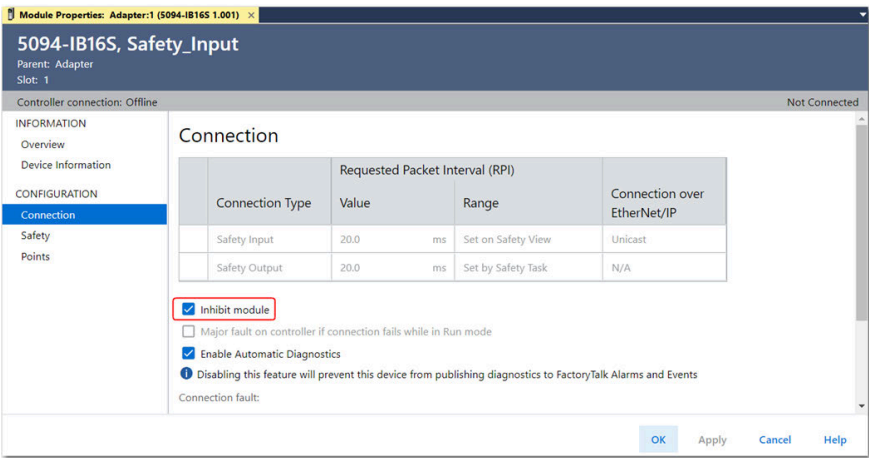
You cannot inhibit or uninhibit safety I/O devices or producer controllers from the module properties dialog under these conditions:

- The application program is safety-locked
- A safety signature exists

To inhibit a device, follow these steps.

1. Select the device and then select Properties.
2. In the navigation pane, select Connection.
3. On the Connection view, select Inhibit Module and click Apply.

The device is inhibited when the Inhibit Module checkbox is selected. If a communication device is inhibited, all downstream devices are also inhibited.



Regardless of safety signature or safety-locked status some I/O products allow the ability to programmatically inhibit and uninhibit with SSV from the standard task:

- Class Name: Module
- Attribute Name: Mode
- Source: Inhibit = 4; Uninhibit = 0

Edit a Safety Application

The following rules apply to changing your safety application program:

- Only authorized, specially trained personnel should make program edits. These personnel must use all supervisory methods available, for example, using the controller switch and software password protections.
- When authorized, specially trained personnel make program edits, they assume the safety responsibility while the changes are in progress. These personnel must also maintain safe application operation.
- When you edit online, you must use an alternate protection mechanism to maintain the safety of the system.
- You must sufficiently document all program edits, which include the following:
 - Authorization
 - Impact analysis
 - Execution
 - Test information
 - Revision information
- If online edits exist only in the standard routines, those edits are not required to be validated before returning to normal operation.
- You must make sure that changes to the standard routine, regarding timing and tag mapping, are acceptable to your safety application.
- You can edit the logic portion of your program while offline or online, as described in the following sections.

Offline Edits

When you make offline edits to only standard program elements and the safety signature matches following a download, you can resume operation.

When you make offline edits to the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before you resume operation.

Online Edits



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

Online edits in standard routines are unaffected by the safety-locked or safety-unlocked state.

The following requirements apply to online edits of safety logic:

- The controller must be safety-unlocked and unsigned. If the controller is locked with safety edits, you must unlock the controller to assemble or cancel the edits. You assemble edits to make online edits change the controller program.

You cancel edits to reject and delete any unassembled online edits.

- For safety routines, the controller cannot be locked when there is a pending edit, but it can be locked when there is a test edit.

A pending edit is a change to a routine that has been made in the Studio 5000 Logix Designer® application, but has not yet been communicated to the controller by accepting the edit.

A test edit is an online edit that has been accepted and causes the controller to execute the new, edited version of logic. The original, unedited version of logic is still in controller memory, but is not executed.

IMPORTANT: Certain parameters are only evaluated when the instruction is first evaluated. You must transition the controller to Program mode and back to Run mode before the changes take effect. For affected operands, see the Logix 5000® Controller Safety Application Instruction Set Reference Manual, publication [1756-RM095](#).

You cannot edit standard or safety Add-On Instructions when the controller is online.

When you make online edits to the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before you resume operation.

Limit online edits to minor program modifications, such as setpoint changes or minor logic additions, deletions, and modifications.

The safety-lock and safety signature features of the controller affect online edits. For more information, see [Lock the Controller on page 209](#) and [Generate the Safety Signature on page 205](#).

Modification Impact Test

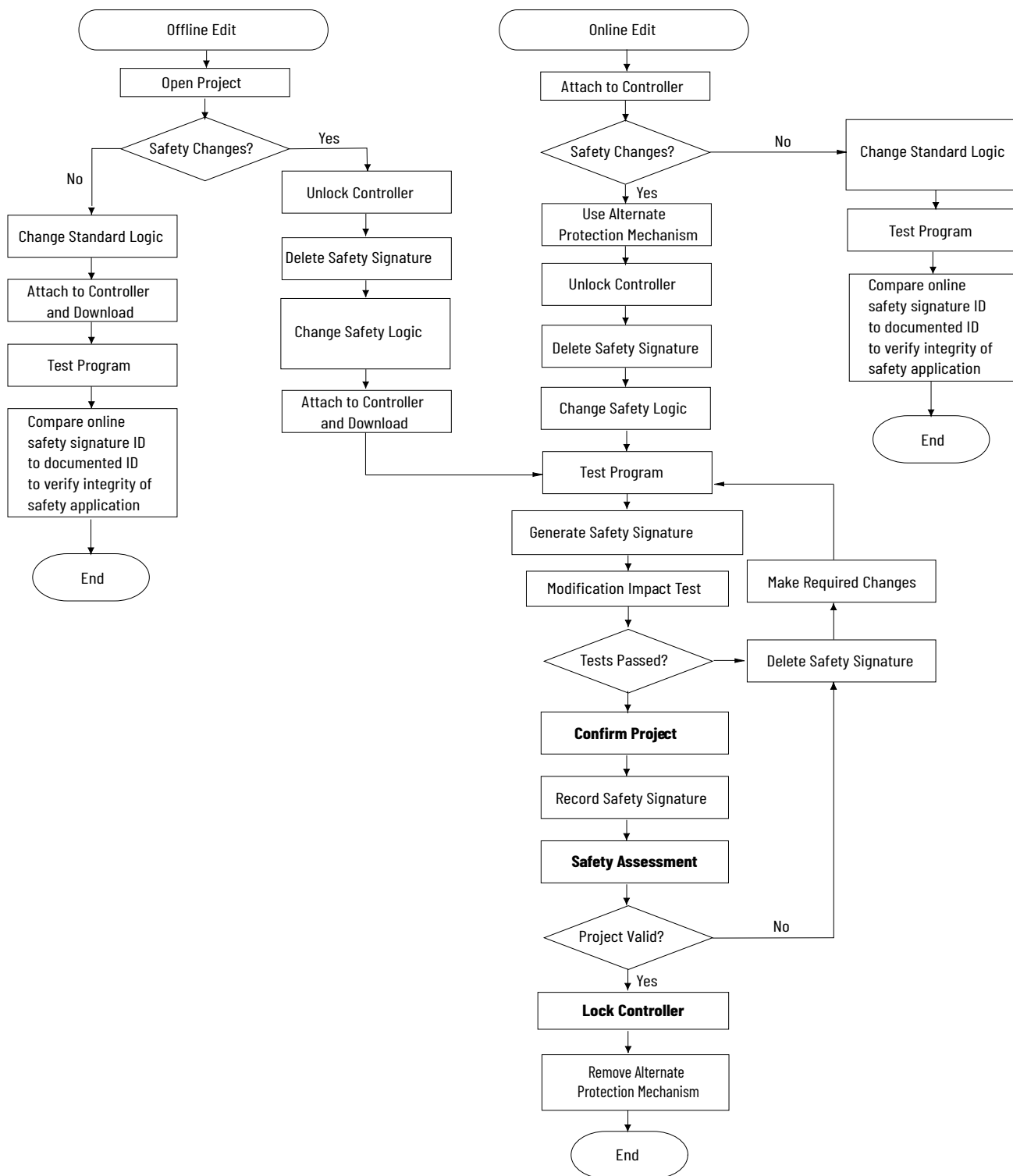
Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system. All appropriate phases of the software safety lifecycle must be conducted as indicated by the impact analysis. If your validation plan requires cold start or warm start testing of the modification, this can be achieved by transitioning from Program mode to Run mode. Special attention should be paid to the impact of the modification on safety task initialization as described in [Custom Tag Initialization During Prescan on page 195](#).

At a minimum, you must perform these actions:

- Perform functional tests of all impacted software.
- Document all modifications to your software specifications.
- Document all test results.

For detailed information, see IEC 61508-3, Section 7.8 Software Modification.

Figure 66. Online and Offline Edit Process



Functional Safety Reference

When the controller is safety-enabled, the 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 system is made up of a primary controller and a safety partner that function together in a 1oo2 architecture.

You must read, understand, and fulfill safety requirements as described in this manual before you operate a SIL 2/PLd or SIL 3/PLe safety system.

Safety Signature

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

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

Figure 67. Safety Signature

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

Safety Signature Hierarchy

- The following image shows an example of the safety signature hierarchy:
- A signature with ID and time stamp exists for each element in the hierarchy.
 - Expand the safety signature at the top to view its underlying elements.
 - Expand a parent element to view its underlying child elements.

Figure 68. Safety Signature Hierarchy

Signature for	Updated	ID
▼ Controller CsrBaseline	08/23/2023 12:29:41.076 PM	3D3D5781 - 7BA35C87 - 58530CCC - A5435D56 - 0A84FDE3 - D8610007 - C3857649 - 98EF6481
▼ Safety Application	08/23/2023 12:29:41.076 PM	17F02989 - 6AE041D3 - D558C16C - 575D2B3D - 4358E3AD - A0DF6511 - E8832578 - 42F48735
Safety Controller Attributes	08/23/2023 12:29:41.076 PM	1216A880 - 1064C1F9 - F95A694D - 0BA963E6 - 8A6F3449 - F80EF09C - 59A65413 - 518C8E92
Safety Tag Mapping	08/23/2023 12:29:41.076 PM	51FA4700 - 3BC628C5 - 1CAF8C1D - 3D1E9416 - 64948655 - 50B5B478 - EF722809 - 3FA6A60E
Controller Tags	08/23/2023 12:29:41.076 PM	EAEB684E - 5DAF9376 - 170E9A35 - E96CE77E - 14384E84 - 3953EC81 - B58CD097 - 7EC6E1A6
▼ SafetyTask	08/23/2023 12:29:41.076 PM	DCABACF6 - 4A899D32 - A9ABCFA3 - C2FFA9C0 - 21847338 - B55260DE - 8D05D832 - 44DAAE06
▼ SafetyProgram	08/23/2023 12:29:41.076 PM	7A75D175 - 47FE2CF8 - CDABA451 - 551F00F9 - 188CD8FD - 2C666009 - 48B941C8 - FD7D25D7
Parameters and Local Tags	08/23/2023 12:29:41.076 PM	95A78CF1 - BE256AAA - 2A137EAF - 2DA881F5 - 4AD3CD76 - 7D925805 - 535AF839 - 6EADE89F
MainRoutine	08/23/2023 12:29:41.076 PM	DE68C78 - EB49CFB2 - 09C587FE - 131A24C2 - 3FASCS5C - 7919903C - 98361F72 - D854532A
▼ Add-On Instructions	08/23/2023 12:29:41.076 PM	9893902D - 2CE3AEEC - CF0BC539 - 88EEC018 - A540B2ED - D08E32E5 - A1558F01 - A163F2EF
▼ SafetyAOI	08/23/2023 12:29:41.076 PM	6015A73B - 62945DEF - C05EABC6 - 0A472070 - 600B80A9 - 2318B3D - D648F33 - 70E85328
Parameters and Local Tags	08/23/2023 12:29:41.076 PM	6085D642 - 81C776DE - FF41376F - 2C9E7C02 - 64E04807 - B465C14C - AB9582F6 - C71557DB
Logic	08/23/2023 12:29:41.076 PM	57F8070 - C5E027AF - B86801E6 - 8757758F - ECC3229F - 25DC9E25 - 6D66C8FF - ED97C0E9
▼ I/O Configuration	08/23/2023 12:29:41.076 PM	EC1ED9A4 - 79EDC014 - 6578FDE6 - 7E140556 - D01FCFB - 4AACFFC5 - 3D158C24 - F80F5697
Local	08/23/2023 12:29:41.076 PM	D2EF28AF - 4EACDE78 - 2D8D4A3F - F558404C - 5F3AA792 - BF3D6388 - 88E1AE91 - E3FD038A
▼ safety_in_out_io	08/23/2023 12:29:41.076 PM	F530E119 - 0283E5C4 - B3BA2B05 - C6360F57 - CE93CFFC - 0190C05C - E8E2C1FA - 19D7C6DD
▼ Connection	08/23/2023 12:29:41.076 PM	E1057A2B - 51E6F5A1 - F7CF3357 - 5F21EE21 - AA7F46A6 - 0B169C08 - 908B10E8 - 722D0A1E
Input	08/23/2023 12:29:41.076 PM	9D2A6881 - 480D286F - 5F1BE74A - 78998437 - 71CAFA42 - 080DEA74 - C6785853 - 5CCDDC15
Output	08/23/2023 12:29:41.076 PM	1597E871 - EBF3C3D8 - 5EFA53C7 - FA428554 - 52BF2FF1 - AFB494A6 - 497E7898 - 05C51223

Item	Description
A	Safety signature
B	Safety signature elements

Aggregate Signatures

Safety elements that include a collection of tags and parameters have aggregate signatures. An aggregate signature represents the validity of all tags and parameters within the element.

The following elements have aggregate signatures:

- Controller-scoped safety tags
- Safety program parameters and tags
- Safety Add-On Instructions
- Safety mapped tags
- Safety I/O connections

If one of the preceding elements has a collection with no members, such as no controller-scoped safety tags, the aggregate signature value appears as 64 zeros.

View Safety Signature Elements

There are multiple places where you can view safety signature elements:

- Quick View pane
- Safety Signature report
- Compare Tool

Quick View Pane

When you select a safety element in the Controller Organizer, such as a safety program, its signature appears in the Quick View pane. Before the safety signature is generated, the Safety ID and Safety Updated fields in the Quick View pane display <none>.



To display all 64 characters of the safety signature ID, hover over the ID in the Quick View pane. From the tooltip, you can copy the signature ID.

Before Safety Signature Generation

Controller Organizer

Controller P15_000190_PLC

Controller Tags

Controller Fault Handler

Power-Up Handler

Tasks

T00_Main (80 ms)

T01_Safety (50 ms)

S_Machine

S_xxxxx_Cabinets_xxxxx

S_DE1

S_DG1

S_E1

Parameters and Local Tags

SR00_Main

SR02_PLC_I_O_R060

SR12_PS1_DE1

SR12_PS2_GMS

SR12_PS3_TE1

SR12_PS4_TE2

SR21_DoorInterlock

SR22_SmokeDetection

S_GMS

S_GR0

S_GR1

S_GR2

S_GR3

S_H1

S_H2

S_RE1

S_RR1

Class	Safety
Safety ID	<none>
Safety Updated	<none>
Description	
Status	Scheduled
Number of Routines	8
Main Routine	SR00_Main
Fault Routine	
Max Scan	
Last Scan	
Parent	
Scheduled In	T01_Safety

After Safety Signature Generation

Controller Organizer

T01_Safety (50 ms)

S_Machine

S_xxxxx_Cabinets_xxxxx

S_DE1

S_DG1

S_E1

Parameters and Local Tags

SR00_Main

SR02_PLC_I_O_R060

SR12_PS1_DE1

SR12_PS2_GMS

SR12_PS3_TE1

SR12_PS4_TE2

SR21_DoorInterlock

SR22_SmokeDetection

S_GMS

S_GR0

S_GR1

S_GR2

S_GR3

S_H1

S_H2

S_RE1

S_RR1

S_RR1_1

S_RR1_2

S_RE2

S_RR2

S_RR2_1

S_RR2_2

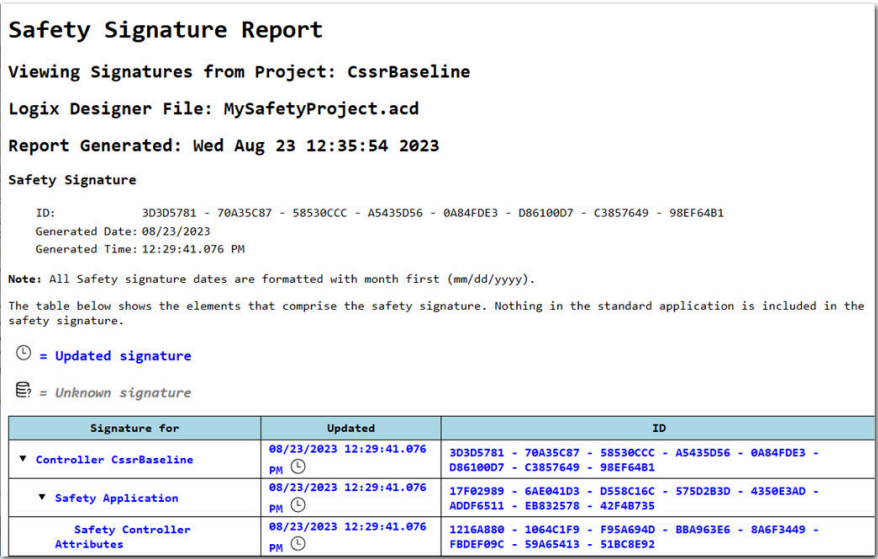
Class	Safety
Safety ID	A9E417A8 - 469D75A7 - 953EC9BF - D...
Safety Updated	08/31/2023 10:47:39.893 AM
Description	
Status	Scheduled
Number of Routines	8
Main Routine	SR00_Main
Fault Routine	
Max Scan	62 us
Last Scan	51 us
Parent	
Scheduled In	T01_Safety

Safety Signature Report

The Safety Signature Report includes all safety signature elements for the controller project. To view the report in the Logix Designer application, select Tools > Safety > Generate Signature Report. The report opens in a web browser and shows the following:

- The safety signature appears in the report header
- The safety signature elements appear in the report table.
- The state of the signature for an element is indicated by its color, tooltip, and icon.

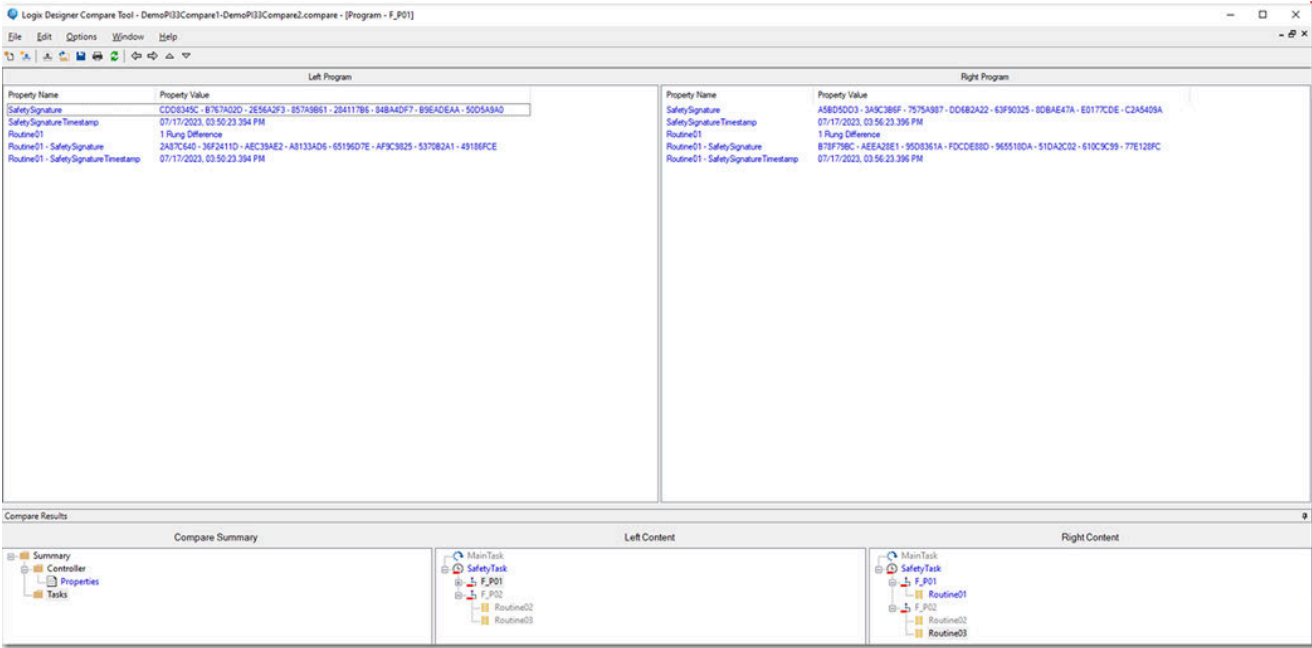
Figure 69. Safety Signature Report



Logix Designer Compare Tool

The Logix Designer Compare Tool can compare safety signature elements in two controller projects. The following image compares two safety routine elements.

Figure 70. Logix Designer Compare Tool



Safety Signature States

A signature can have three states as indicated by its color: blue, black, or gray.

Blue Signature

A signature appears blue in these scenarios:

- After the first generation of the safety signature
- After any subsequent generation of the safety signature to indicate a change to a safety element or one of its child elements

In the following example, the Safety Signature report shows blue signatures as a result of the following workflow:

1. Generate a safety signature for the first time.
2. Create a safety tag in the S_DE1 program.
3. Generate the safety signature a subsequent time.
4. Generate the Safety Signature report.

The creation of the safety tag in step 2 results in blue signatures for these elements:

- Parameters and Local Tags child element
- S_DE1, T01_Safety, and Safety Application parent elements

Figure 71. Blue Parent and Child Signatures

Signature for	Updated	ID
▼ Controller_P15_000190_PLC	08/31/2023 10:56:56.448 AM	92EEF81B3 - 605EEF2A - 973E5DF7 - D248C4E6 - 0B440298 - 25E8D80F - B05528F4 - E62AC3D8
▼ Safety Application	08/31/2023 10:56:56.448 AM	2339E8E5 - DFFA0683 - 085E82D1 - 08D824E5 - 8FD99865 - 798E3559 - 9E79172C - 1FC51B33
Safety Controller Attributes	08/31/2023 10:47:39.893 AM	CE50C9B5 - 40ABA086 - C20BF434 - 8445AD5F - D6954D80 - E414236A - 56EF0365 - 4A148457
Safety Tag Mapping	08/31/2023 10:47:39.893 AM	7624105E - 14DC1627 - 70480CD0 - D149CB70 - CAF8ACF8 - F60FF95F - C3758865 - 607E245F
Controller Tags	08/31/2023 10:47:39.893 AM	94523844 - 802F6054 - 3E48F8BC - 2CD96795 - 84C96808 - 2E54924E - 558F470D - 8956086D
▼ T01_Safety	08/31/2023 10:56:56.448 AM	F95E9CFA - 7FE9096F - A61FC452 - C10379E0 - 934F55B5 - D514FD5E - 33F87770 - BF788833
▼ S_DE1	08/31/2023 10:56:56.448 AM	84185D04 - 64F14011 - C29C8CF0 - 29C8A465 - 0F6C2163 - D31F8E93 - 72F81A0A - FD05E2B3
Parameters and Local Tags	08/31/2023 10:56:56.448 AM	01BCF740 - EEBE9E4A - 6AC84F8F - 732A005F - 57676C70 - EAAE008C - 0F417086 - 82C44D72
SR00_IfaIn	08/31/2023 10:47:39.893 AM	07887482 - 58D02C57 - CCE231D5 - 9A8A344D - 17E49D47 - AC0A1DE3 - 6FD68F96 - 052E95F8
SR02_PLC_I_O_R070	08/31/2023 10:47:39.893 AM	D48F3380 - 1350D53E - 7700A2F0 - 71346E41 - 8D046478 - 9A828ECB - 8C31F0E6 - 71044374
SR11_P51_DrivesSpoolChamber	08/31/2023 10:47:39.893 AM	7588CB8A - D89A0E17 - 8DFF8133 - 63AF8B7C - 18FC8168 - 800AA734 - 99E9A629 - B12DE867
SR11_P52_DrivesCrossChamber	08/31/2023 10:47:39.893 AM	F71AF1F8 - 8515EF3A - CCF8E898 - 9AA938FC - 47750943 - 89D560F4 - 4720012D - 87B85D14
SR11_P53_DrivesPivotingPlatform	08/31/2023 10:47:39.893 AM	90DE48FE - 2E89FC2C - 46D03105 - 949951F5 - F2807F45 - 6325CC6C - 8148D602 - A32783C2
SR11_P54_DrivesReactor1	08/31/2023 10:47:39.893 AM	27027869 - 79F283CA - 07AEF4CF - 049A137E - 8A473F77 - E29A011C - D7980676 - 80E09793
SR11_P55_DrivesReactor2	08/31/2023 10:47:39.893 AM	0891D7B3 - 7988D678 - F765E89D - E488C187 - A98D4750 - E0C769F2 - 8E1437FA - 877EFDAC
SR11_P56_DrivesReactor3	08/31/2023 10:47:39.893 AM	8A6C1C8E - 51D7FCE2 - 2E801ABA - 11908CCA - F35CE654 - 827F8D12 - 48D2194E - 312D02A6
SR20_CompressedAir	08/31/2023 10:47:39.893 AM	08919E67 - 69492280 - 102D9561 - 60168987 - 08F1ED48 - 94448331 - E80A484A - 680847D
SR21_DoorInterlock	08/31/2023 10:47:39.893 AM	C590CC40 - E6C5AA6A - 8DFF8074E - C242D493 - 110FAF12 - 283E1A08 - 84172E08 - 08885DEF
SR22_SmokeDetection	08/31/2023 10:47:39.893 AM	17E1B3FF - 78480838 - 88A84206 - D6189781 - 330877CC - D1C2360C - 7EC0A1D4 - AAC576E8
▼ S_D01	08/31/2023 10:47:39.893 AM	CD18AA25 - B22B1202 - A9A1B1CC - 0EA1B119 - FDF7D1F8 - 70797419 - 47597019 - AADEF6D3

Black Signature

A signature appears black after any subsequent generation of the signature when no change occurred to the safety element or any of its child elements.

Gray Signature

A gray signature is an unknown signature. An unknown signature occurs when the Logix Designer application cannot verify that the signature ID matches the associated value. Unknown signatures cannot be used for certification and must be updated.

A signature appears gray when you perform any of the following workflows:

- Delete the safety signature
- Create a controller project from an imported project with an existing safety signature
- Copy a safety signature element with an existing signature

Archive Safety Signature Reports for Audit

You can compare an original Safety Signature report to an updated Safety Signature report to show which elements changed and which elements did not change for auditing purposes. If your

validation plan does not require revalidation of unchanged elements, your certification effort can be reduced, such as in these scenarios:

- You want to migrate a validated safety application to a future release without revalidating the entire application.
- You want to add or update some elements of a validated safety application without revalidating the unchanged elements.
- You want to copy some validated elements to another project without revalidating the copied elements.

Safety Signature reports are archived as .htm files in the following default directory:

C:\Users\Public\Documents\Rockwell Automation\Studio 5000\Logix Designer\Safety Signature Reports

Signature Authentication

If a signature for an element cannot be authenticated, the following occurs:

- A warning appears in the Errors pane below the Controller Organizer.
- No signature is shown for the element in the Quick View pane.

For example, if you copy a main routine, but the routine was changed before the copy, warnings appear to indicate that the signature could not be authenticated. No signature appears for the copied routine in the Quick View pane.

Figure 72. Signature Authentication Failed—Warning

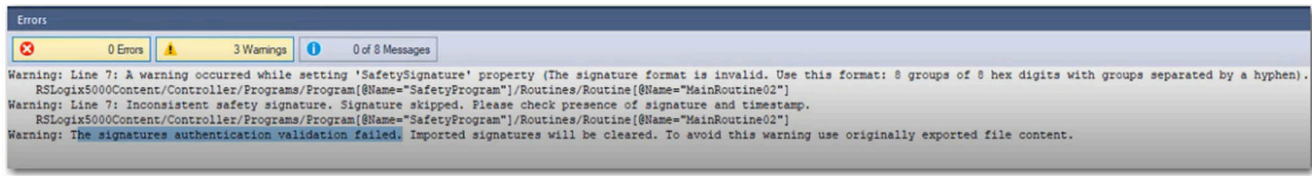
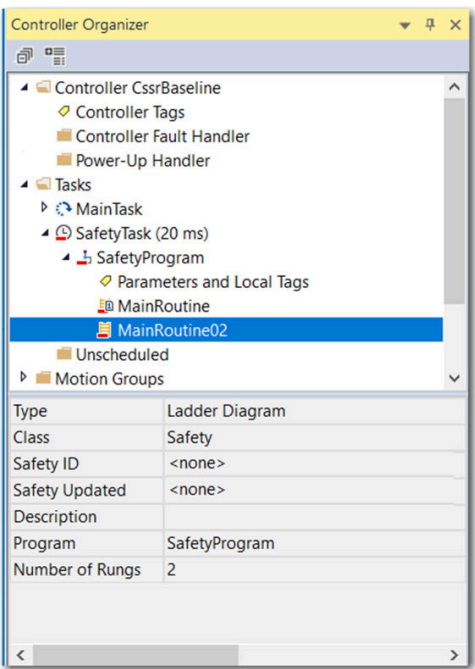


Figure 73. Signature Authentication Failed—No Signature



Settings that Do Not Affect the Safety Signature

In the Logix Designer application, version 36 or later, you can make the following changes to a safety project with no effect on the safety signature:

- Change the controller slot number, if applicable.
- Modify controller IP settings.
- Change the EtherNet/IP™ mode on a controller that support multiple modes.
To change the EtherNet/IP™ mode, you must first delete the safety signature. After changing the mode, you can regenerate the safety signature with the same value.

Programmatic Changes to the Safety Application Signature

If there are no changes to your safety application, then the safety application signature and all of its underlying elements remain constant across software and firmware releases with the following possible exceptions:

- You update the controller with a firmware revision that contains a change to the offline compiler or internal signature algorithm. These changes can trigger a change to the safety signature. These types of changes are infrequent.
- You use the copy/paste or import function in a way that causes an internal difference in a component. For example, if you copy a safety routine from Project1 to Project2 and TagA is program-scoped in Project1, but controller-scoped in Project2, then the safety signature for the routine changes.

Unlike the safety application signature, the controller safety signature always changes with any firmware release change, so that you complete some validation testing at the functional controller level, even if no changes were made to the safety project.

Figure 74. Controller and Safety Application Signatures

Signature for	Updated	ID
▼ Controller P15_000190_PLC	08/31/2023 10:56:56.448 AM	92EE81B3 - 6D5EEF3A - 973E5DF7 - 0248C466 - 084A0298 - 25EB080F - B0552BF4 - E63AC3D0
▼ Safety Application	08/31/2023 10:56:56.448 AM	2339EBE5 - DFFA0683 - 0B5E8205 - 080B24E5 - 8FD99865 - 790E3559 - 9E79172C - 1FC51B33
Safety Controller Attributes	08/31/2023 10:47:39.893 AM	CB50C985 - 40A8A086 - C20BF434 - 8445AD5F - D6954D00 - E414236A - 56EF9365 - 4A148457
Safety Tag Mapping	08/31/2023 10:47:39.893 AM	7624105E - 14DC1627 - 70480C08 - D145CB70 - CAF8ACF8 - F60FF95F - C3758865 - 607E245F
Controller Tags	08/31/2023 10:47:39.893 AM	94523844 - 802F6054 - 3E48F8BC - 2CD96795 - 84C96808 - 2E54924E - 558F470D - 8956086D
▼ T01_Safety	08/31/2023 10:56:56.448 AM	F959CFA - 7FE9096F - A61FC452 - C18379E0 - 934F5585 - D514FD5E - 33F87770 - 8F788833
▼ S_De1	08/31/2023 10:56:56.448 AM	84185D04 - 64F14011 - C29C8CF8 - 29C8A865 - 0F6C2163 - D31F8E93 - 72F81A8A - FD05E2B3
Parameters and Local Tags	08/31/2023 10:56:56.448 AM	018CF740 - EEBE9E4A - 6ACBA5F8 - 732A005F - 57676C7D - EAAE080C - 0F417086 - B2C44072
SR00_Main	08/31/2023 10:47:39.893 AM	07887482 - 58D02C57 - CCE231D5 - 9ABA344D - 17E49D47 - AC0A1DE3 - 6FD68F96 - 052E95F8
SR02_PLC_I_O_R070	08/31/2023 10:47:39.893 AM	D48F3380 - 1350C53E - 7708A2F0 - 71346E41 - 8D046478 - 9A828ECB - 8C31F066 - 71044374
SR11_P51_DrivesSpoolChamber	08/31/2023 10:47:39.893 AM	7588CB8A - D89A8E17 - 8DFF8133 - 63AF887C - 18FC8168 - 800AA734 - 99E9A629 - 812DE867
SR11_P52_DrivesCrossChamber	08/31/2023 10:47:39.893 AM	F71AF1F8 - B515EF3A - CCF8E898 - 9AA938FC - 47750943 - 890560F4 - 4720012D - 87885D14
SR11_P53_DrivesPivotingPlatform	08/31/2023 10:47:39.893 AM	90DE48FE - 2E89FC2C - 46D03105 - 949951F5 - F2007F45 - 6325CC6C - 8148D602 - A32783C2
SR11_P54_DrivesReactor1	08/31/2023 10:47:39.893 AM	27027869 - 79F283CA - 07AEF4CF - 048A137E - 8A473F77 - E29A011C - D7980676 - 8DE09793
SR11_P55_DrivesReactor2	08/31/2023 10:47:39.893 AM	0891D783 - 7988D678 - F7656990 - E408C187 - A98D4758 - E8C769F2 - 8E1437F4 - 877EFDAC
SR11_P56_DrivesReactor3	08/31/2023 10:47:39.893 AM	8A6C1C8E - 51D7FCE2 - 2E801A8A - 11908CC4 - F35C6654 - 8277F8D12 - 48D2194E - 312D0246
SR20_CompressedAir	08/31/2023 10:47:39.893 AM	00919E67 - 69492280 - 102D9561 - 60168987 - 0BF1ED48 - 94448331 - E804A84A - 688D847D
SR21_DoorInterlock	08/31/2023 10:47:39.893 AM	C590CC4D - E6C5AA6A - 8DFF8074E - C242D0A93 - 118FAF12 - 283E1A08 - 84172EE8 - 08885DEF
SR22_SmokeDetection	08/31/2023 10:47:39.893 AM	17E1B3FF - 78480838 - 88A84206 - D6189781 - 330877CC - D1C2360C - 7EC0A1D4 - AAC576E0
▼ S_D01	08/31/2023 10:47:39.893 AM	CD184A25 - B2281202 - A9A181CC - 0EA18119 - FDF7D1F8 - 78797419 - 47507019 - AADEF6D3

CIP Safety Systems and Safety Network Numbers

CIP Safety™ control systems are composed of CIP Safety™ devices that are interconnected via communication networks. These networks consist of devices, such as bridges, switches, routers, adapters, and redundancy modules, which may not be SIL 2 or SIL 3 certified. The secure transmission of safety-related data through standard infrastructure devices is known as black channel communication.

CIP Safety™ devices must be inherently protected from network delivery errors. The CIP Safety™ protocol is an end-node to end-node safety protocol. This configuration allows the routing of

CIP Safety™ messages to and from CIP Safety™ devices through non-certified bridges, switches, routers, adapters, and redundancy modules.

For more information about CIP Safety™ functionality and related concepts, see the following:

- ODVA website at <https://www.odva.org>
- CIP Safety: Safety Networking for Today and Beyond White Paper, publication [SAFETY-WP038](#)

Unique Node Reference

A key element of the CIP Safety™ protocol is the concept of a Unique Node Reference (also called Unique Node ID or UNID). Every CIP Safety™ device must have a UNID value that is assigned to each CIP Safety™-capable port.

IMPORTANT: It is your responsibility to make sure that all UNIDs are unique within the scope of all devices that could possibly communicate with each other.

Safety Network Numbers (SNNs)

Communication within a control system travels over subnets that are interconnected with bridging or routing components. The following are examples of subnets:

- The backplane of a chassis
- A bank of I/O modules
- An Ethernet subnet within a LAN

Rather than creating a UNID directly for each CIP Safety™ device, which can be prone to error in a large system, each subnet has a unique safety network number (SNN), and the UNID is created from the SNN + the node address.

Safety Network Number (SNN) Assignment

When you create controller projects, the programming software 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 safety controllers have up to three safety network numbers: a separate SNN for each Ethernet port, and one SNN 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.

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



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

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

Distinguish between Standard and Safety Components

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

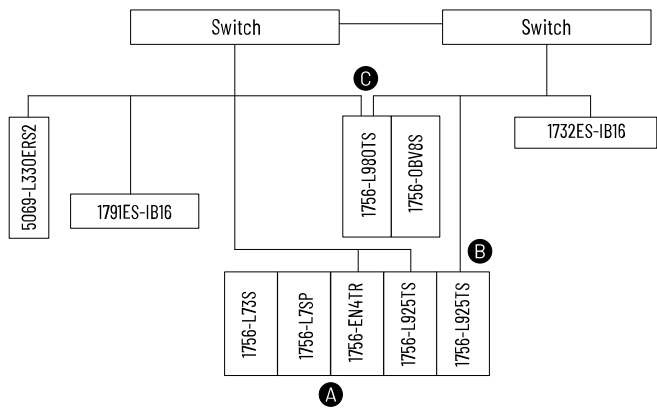
You must create and document a clear, logical, and visible distinction between the safety and standard portions of the controller project. As part of this distinction, the Studio 5000 Logix Designer® application features safety identification icons to identify the safety task, safety programs, safety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

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

Routable CIP Safety System

The following example illustrates the extent of a routable CIP Safety™ system. In this example, the system is not interconnected to another CIP Safety™ system through a larger, plant-wide Ethernet backbone.

Figure 75. Routable CIP Safety System



Item	Description
A	For a backplane port, an SNN is assigned to the backplane and the node address is the slot number of the device.
B	For an Ethernet port, an SNN is assigned to the EtherNet/IP™ network and the node address is the IP address of the device.
C	For a controller in Dual-IP mode and connected to two separate EtherNet/IP™ networks, they must not share SNN values because the switches can incorrectly route packets between them.

Considerations for Assigning SNNs

When you create a controller project, the application generates an SNN value automatically whenever a new subnet contains CIP Safety™ devices:

- Each CIP Safety™-capable port on the controller is assigned an SNN.
- 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.

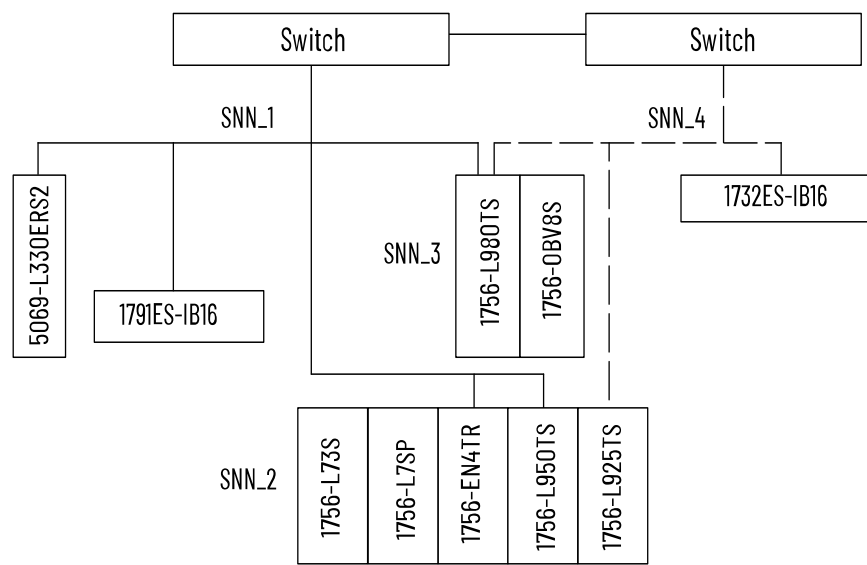
If the entire CIP Safety™ system consists of one controller project, these automatically generated SNN values are sufficient.

If there are multiple controllers that must interact or access the same safety I/O, the CIP Safety™ system designer must coordinate the SNN values between the separate project files. The application provides copy/paste access to the SNN assignments to enable this coordination.

You can also choose to map out the entire routable system (perhaps for the entire plant) and manually assign SNN values to each subnet. The application provides a manual entry method for assigning SNN values to enable this design methodology.

The following example shows how SNNs can be assigned to subnets.

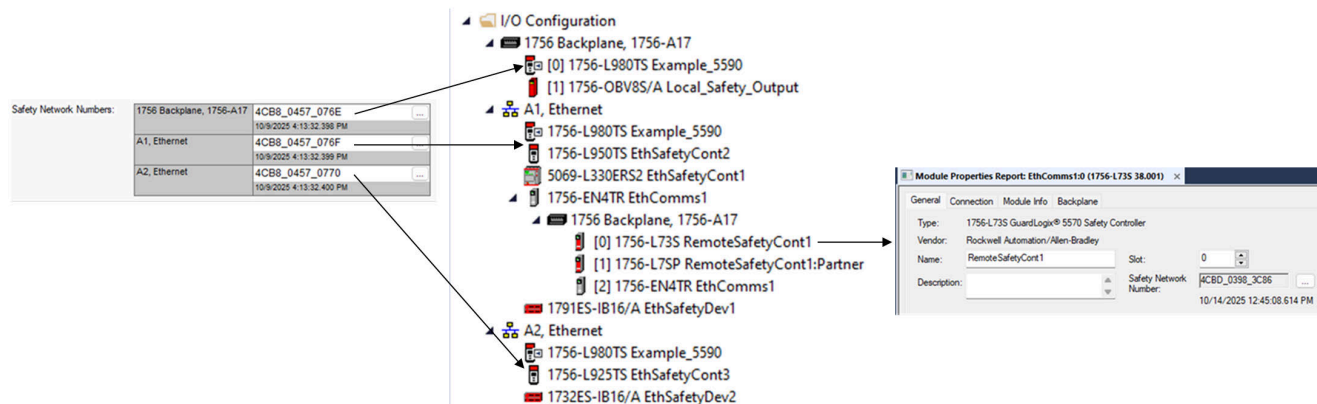
Figure 76. SNN Assignment Example



Subnet	Type	SNN Assignment
SNN_1	EtherNet/IP™	5069-L330ERS2 Ethernet port 1, 1791ES-IB16, 1756-L980TS Ethernet port 1, and 1756-L950TS Ethernet port 1
SNN_2	Backplane	1756-L73S, 1756-L950TS, and 1756-L925TS backplane port
SNN_3	Backplane	1756-L980TS backplane and 1756-OBV8S
SNN_4	EtherNet/IP™	1756-L980TS Ethernet port 2, 1756-L925TS Ethernet port 2, 1732ES-IB16

The following figure shows how the preceding example corresponds to the Controller Organizer I/O tree.

Figure 77. Controller Organizer



The configuration profile for each CIP Safety™ device in the I/O tree includes a parameter for the SNN value that the controller uses when it opens the CIP Safety™ connection to that device. This parameter automatically adopts the SNN value that is already established by the SNNs known to the project:

- Safety devices, including controllers, that are direct children of a controller adopt the SNN that matches the controller for the port that is used to connect to the safety module.
 - Safety devices directly under the backplane port adopt the backplane port SNN of the controller.
 - Safety devices directly under an Ethernet port adopt that Ethernet port SNN of the controller.
- Safety devices, including controllers, on a remote subnet adopt the SNN value that is already assigned to that subnet, or a new SNN is generated for the first CIP Safety™ device on that subnet.

We recommend that you assign each controller SNN to the already established SNN for the subnet. This recommendation enables the Logix Designer application to assign the correct SNN to each safety I/O module and safety controller that are added to the project.

If safety I/O is copied from an existing project during controller program development, the SNN value from the original location is retained. To create an SNN structure that resembles the newly created I/O, you can manually change the SNN of copied devices to follow the SNN structure of the new project by using copy/paste SNN from other I/O on the subnet or parent device. If you copy safety I/O into a new remote rack, then a new time-based SNN can be established and populated throughout the remote rack.

How SNNs Get to Safety Devices

Most CIP Safety™ I/O modules in the factory default state accept an SNN that is assigned by the controller that owns that module. The SNN value that the programming software automatically adopts for the connection of that module is accepted when the controller opens the initial connection to the module.

IMPORTANT: CIP Safety™ I/O modules retain their UNID (SNN + node) once it has been assigned and must be reset before they can be reused with another value.

Some devices, such as another safety controller in the I/O tree, receive their SNN configuration from a programming workstation. For these devices, you must manually configure the connection to use the same SNN that has been programmed into that device if the programming software did not automatically assign the correct SNN.

SNN Formats

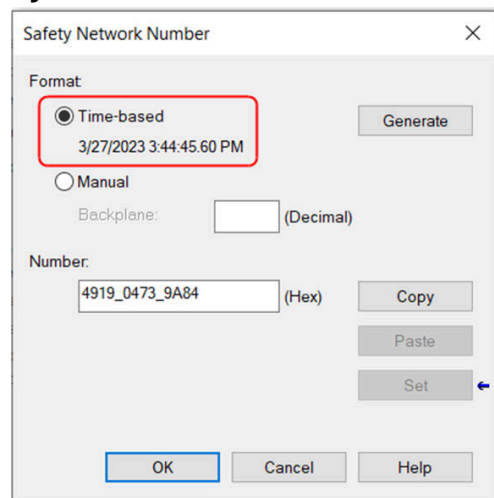
SNNs used by the system are 6-byte hexadecimal numbers. SNNs can be set and viewed in one of two formats:

- Time-based
- Manual

Time-based SNN Format and Assignment

When the time-based format is selected, the SNN represents a date and time based on the local clock of the computer that generated the SNN.

Figure 78. Time-based SNN Format



The assignment of time-based SNNs is automatic when you create a safety project or add EtherNet/IP™ by changing the IP mode or controller type. Time-based SNNs generated by the software are always unique to the project, whether generated by project creation or IP mode change. Devices that are created directly under the controller port default to having the same SNN as that port on the controller.

IMPORTANT: If you have a network diagram for your application, you must edit the SNNs of the controller to match your network diagram. We recommend that you edit the SNNs before you add devices to the I/O configuration in Controller Organizer.

When you add CIP Safety™ I/O devices to ports under an adapter, as opposed to the controller, the following applies:

- If no other device under the port uses an SNN, a time-based SNN is automatically assigned.
- If another device under the port uses an SNN, the device is assigned the same SNN as the first device in address order.

Manual SNN Format and Assignment

When the manual format is selected, the SNN represents a network type and must have a decimal value from 1...9999.

Figure 79. Manual SNN Format

The screenshot shows a dialog box titled "Safety Network Number". It has a "Format" section with two radio buttons: "Time-based" and "Manual". The "Manual" radio button is selected and is enclosed in a red rectangular box. Below the "Manual" radio button is a text field labeled "Backplane:" containing the value "0", followed by the text "(Decimal)". Below this is a "Number:" section with a text field containing the value "0001_0000_0000" and the text "(Hex)". To the right of the "Number" field are buttons for "Copy", "Paste", and "Set". At the bottom of the dialog are buttons for "OK", "Cancel", and "Help". A status bar at the bottom left says "Uninitialized Safety Network Number."

Manual manipulation of an SNN is required for the following reasons:

- To make sure that each safety controller port on the same subnet has the same SNN in all projects
- To copy safety projects



ATTENTION: If a safety project is copied into another project with different hardware or in another physical location, and the new project is within the same routable safety system, every SNN must be changed in the second system. SNN values cannot be repeated. For information about how to change the SNN, see the controller user manual.

IMPORTANT: If you assign an SNN 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 we recommend 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 Studio 5000 Logix Designer® application, and you may not see a warning.

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

Monitor Safety Status and Handle Faults

There are multiple methods to detect and react to faults in the system. The first way that you can handle faults is to verify that you have completed the checklists for your application as described in [Checklists for Safety Applications on page 305](#).

For details about the operation of status indicators, see the user manual for the controller.

IMPORTANT: Status indicators do not provide detailed diagnostics for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

System Status

You can monitor the system status with the following diagnostic indicators.

IMPORTANT: It is your responsibility to determine what data is most appropriate to initiate a shutdown sequence.

Safety I/O Module Diagnostics

Safety I/O modules provide pulse test and monitoring capabilities. If the module detects a failure, it sets the offending input or output to its safe state and reports the failure to the controller. The failure indication is made via input or output status and is maintained for a configurable amount of time after the failure is repaired.

I/O Device Connection Status

The CIP Safety™ protocol allows the recipients of I/O data to determine the status of that data:

- The controller detects input connection failures and then sets all input data to the safe state and the associated input status to faulted.
- The output device detects output connection failures and then de-energizes its outputs.
- Generally, the safety controller also has input connections from output devices. The safety controller determines the status of these input connections, but the input connection status is not the primary mechanism to de-energize outputs.

IMPORTANT: You are responsible for providing application logic to latch I/O failures and to verify that the system restarts properly.

De-energize to Trip System

Safety controllers are part of a de-energize to trip system, which means that off is the safe state. Some, but not all, safety I/O device faults cause all device inputs or outputs to be set to safe state. Faults that are associated to a specific input channel result in that specific channel being set to a safe state. For example, a pulse test fault that is specific to channel 0 results in channel 0 input data being set to the safe state. If a fault is general to the device and not to a specific channel, the combined status bit displays the fault status and all device data is set to the safe state.

Get System Value (GSV) and Set System Value (SSV) Instructions

The GSV and SSV instructions let you get (GSV) and set (SSV) controller system data that is stored in device objects. When you enter a GSV/SSV instruction, the programming software displays the valid object classes, object names, and attribute names for each instruction. Restrictions exist for using the GSV and SSV instructions with safety components.

IMPORTANT: The safety task cannot perform GSV or SSV operations on standard attributes.

The standard task can GSV diagnostic information from safety objects and SSV can inhibit some safety I/O devices.

For more information about GSV and SSV instructions, see the Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

Safety Status

You can use the following to monitor safety status:

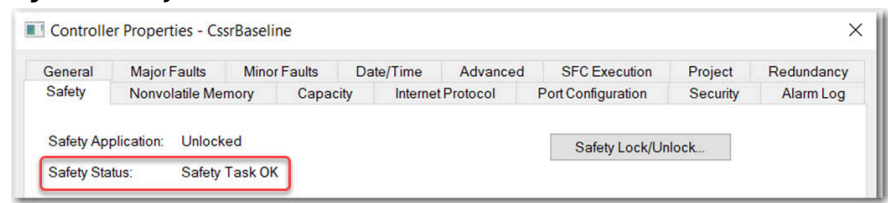
- Safety task status in the controller properties
- Safety I/O status

Safety Task Status

The safety task status appears on the Safety tab of the controller properties and is one of the following:

- Safety Task Inoperable
- Safety Task OK

Figure 80. Safety Task Status



Safety I/O Status

Connection Status (.ConnectionFaulted) is the status of the safety connection between the controller and the safety I/O module:

- When the connection is operating properly, this bit is LO (0).
- When the connection is not operating properly, this bit is HI (1). All other module-defined tags are LO and considered invalid data.

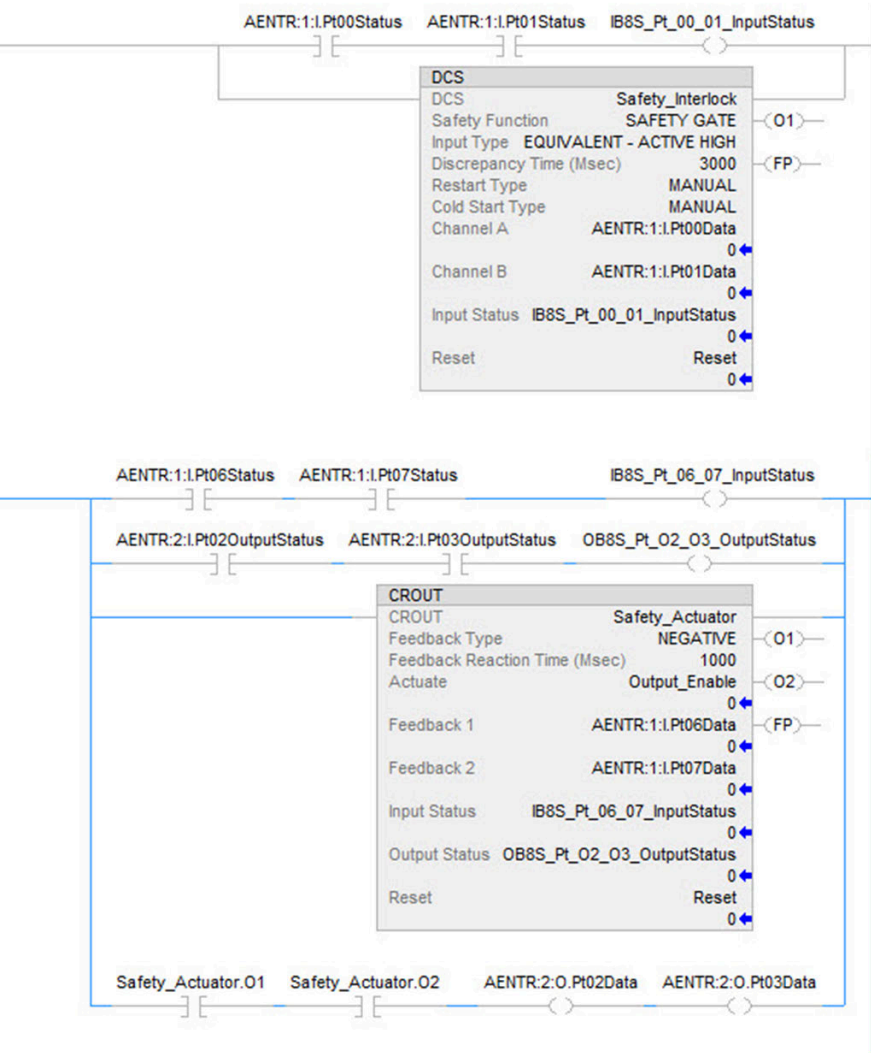
Point Status or Channel Status is available for safety inputs and safety outputs. When a status tag is HI (1), it indicates the following:

- An individual channel is functioning and wired correctly.
- The safety connection between the controller and the safety I/O module on which the channel resides is operating properly.

The safety instructions have built-in safety I/O status monitoring. Input Status and Output Status are parameters for the safety input and output instructions. The DCS instruction and other dual-channel safety instructions have Input Status for input channels A and B. The CROUT instruction has Input Status for Feedbacks 1 and 2 and Output Status for the output channels that are driven by the CROUT outputs 01 and 02. The status tags in these instructions must be HI (1) for the safety instruction output tags (01 for input instructions and 01/02 for CROUT) to be energized.

For proper safety instruction operation, it is important to drive the input status and output status tags BEFORE/ABOVE the safety instruction as shown in the following example.

Figure 81. Instruction Examples



When you use instructions, such as XIC and OTE, to directly reference safety I/O data points without the use of a safety-rated instruction, you are responsible for interrogating the safety I/O status:

- Before you use a safety input channel as an interlock, verify that the safety input channel status is HI (1).
- Before you energize a safety output channel, verify that the safety output channel status is HI (1).

Safety Faults

Safety systems can experience the following faults.

Nonrecoverable Controller Faults

These faults occur when the internal diagnostics of the controller discovers a fault. If a nonrecoverable controller fault occurs, standard and safety task execution stops and outgoing connections stop. Safety I/O devices respond to the loss of output data by transitioning to the safe state. Recovery requires that you download the application program again.

Nonrecoverable Safety Faults in the Safety Application

If a nonrecoverable safety fault occurs in the safety application, the safety logic and the safety protocol are ended. Safety task watchdog and control partnership faults fall into this category.

When the safety task encounters a nonrecoverable safety fault, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.



ATTENTION: Overriding a safety fault does not clear the fault. If you override a safety fault, it is your responsibility to prove that operation of your system is still safe.

You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

Several nonrecoverable safety faults can be cleared, with or without a safety task signature, to enable the safety task to run. The safety task inoperable fault requires that you download the application again for the safety task to run.

Recoverable Safety Faults in the Safety Application

If a recoverable fault occurs in a safety program, the system can halt the execution of the safety task, depending upon if the Program Fault Handler in the safety program (if one exists) handles the fault.

When a recoverable fault is cleared programmatically, the safety task continues without interruption.

When a recoverable fault in the safety application is not cleared programmatically, a Type 14, Code 2 recoverable safety fault occurs. The safety task execution is stopped, and safety protocol connections are closed and reopened to reinitialize them. Safety outputs are placed in the safe state and the producer of safety-consumed tags commands the consumers to place them in a safe state, as well.

If the recoverable safety fault is not handled, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to reduce the risk of these faults, rather than handling them at runtime.

View Faults

The Recent Faults dialog box on the Major Faults tab of the Controller Properties dialog box contains two subtabs, one for standard faults and one for safety faults.

The status display on the controller also shows fault codes with a brief status message. For more information about status indicators, see the following:

- Controller Status Indicators on page

Fault Codes

Safety controllers show fault codes on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD or MINORFAULTRECORD attribute.

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

Fault Routine for Safety Applications

If a fault condition occurs that is severe enough for the controller to shut down, the controller generates a major fault and stops the execution of logic.

Some applications do not want all safety faults to shut down the entire system. In those situations, use a fault routine to clear a specific fault and let the standard control portion of your system continue to operate or configure some outputs to remain ON.



ATTENTION: You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to eliminate these faults, rather than handling them at runtime.

The controller supports two levels for handling major faults in a safety application:

- Safety Program Fault Routine
- Controller Fault Handler

Both routines can use the GSV and SSV instructions.

Each safety program can have its own fault routine. The controller executes the program's fault routine when an instruction fault occurs. If the program's fault routine does not clear the fault, or if a program fault routine does not exist, the safety task faults and shuts down.

When the safety task faults, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

The controller fault handler is an optional component that executes when the program fault routine cannot clear the fault or does not exist.

You can create one program for the controller fault handler. After you create that program, you must configure a routine as the main routine.

The Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#), provides details on creating and testing a fault routine.

GSV/SSV Instructions in a Safety Application

For standard tasks, you can use the GSV instruction to get values for the available attributes. When using the SSV instruction, the software displays only the attributes that you can set.

For the safety task, the GSV and SSV instructions are more restricted. The SSV instructions in safety and standard tasks cannot set bit 0 (major fault on error) in the mode attribute of a safety I/O device.



ATTENTION: Use the SSV instruction carefully. Making changes to objects can cause unexpected controller operation or injury to personnel.

FaultRecord Attributes

Create a user-defined structure to simplify access to the MajorFaultRecord and SafetyTaskFaultRecord attributes.

Table 55. Parameters for Accessing FaultRecord Attributes

Name	Data Type	Style	Description
TimeLow	DINT	Decimal	Lower 32 bits of the fault time stamp value
TimeHigh	DINT	Decimal	Upper 32 bits of the fault time stamp value
Type	INT	Decimal	Fault type (program, I/O, or other)
Code	INT	Decimal	Unique code for this fault (dependent on fault type)
Info	DINT[8]	Hexadecimal	Fault-specific information (dependent on fault type and code)

Fault Information

The SafetyStatus and SafetyTaskFaultRecord attributes can capture information about nonrecoverable faults. Use a GSV instruction in the controller fault handler to capture and store fault information. The GSV instruction can be used in a standard task with a controller fault handler routine that clears the fault and lets the standard tasks continue executing.

For more information on using the GSV and SSV instructions in safety applications, refer to the Input/Output Instructions chapter of the Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

Safety Partner Fault

If the SIL configuration is set to SIL 2 and a safety partner is installed in the slot next the safety primary, these actions occur:

- On the 1756-L9SP safety partner, the MOD status indicator flashes red.
- The controller logs a Type 14, Code 12 minor fault that indicates that the controller is configured for SIL 2, and a safety partner is present.
- The programming application returns an error when an attempt is made to download a SIL 2 application.

Troubleshoot the Controller

There are many options available to troubleshoot the controller if issues occur during normal operation.

You can use the Studio 5000 Logix Designer® application to view fault conditions in these ways:

- Module status in the I/O Configuration Tree
- Categories on I/O Module Properties Dialog
- Notification in the Tag Monitor
- Fault Information in the Controller Properties Dialog
- Ethernet Port Diagnostics
- Advanced Time Sync dialog

You can also use:

- Diagnostic information in Linux-based software
- Controller Webpages

Reset Button

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

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

A controller has two stages of reset:

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

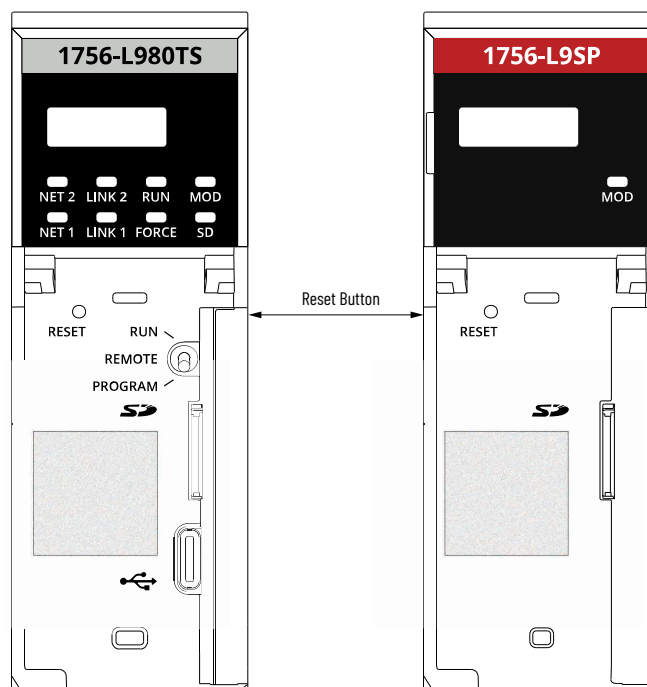
The Safety Partner reset returns the safety partner to out-of-box settings, including firmware.

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



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

Figure 82. Reset Button



Stage 1 Reset

The stage 1 reset does the following:

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

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

1. Power down the controller.
2. Open the front door on the controller.
3. 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.
4. While holding in the reset button, power up the controller.
5. Continue to hold the reset button while the 4-character display cycles through CLR, 4, 3, 2, 1, Project Cleared.
6. After Project Cleared appears, release the reset button.

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

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

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

Stage 2 Reset

The stage 2 reset does the following:

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

To perform a Stage 2 reset, complete these steps. This process assumes that a memory card is installed in the controller.

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

Safety Partner Reset

Follow these steps to perform a safety partner reset.

1. Power down the safety partner.
2. Use a small tool with a diameter of a paper clip to press and hold the reset button. This button is recessed 5 mm (0.19 in.) behind the panel.
3. While holding in the reset button, power up the safety partner.

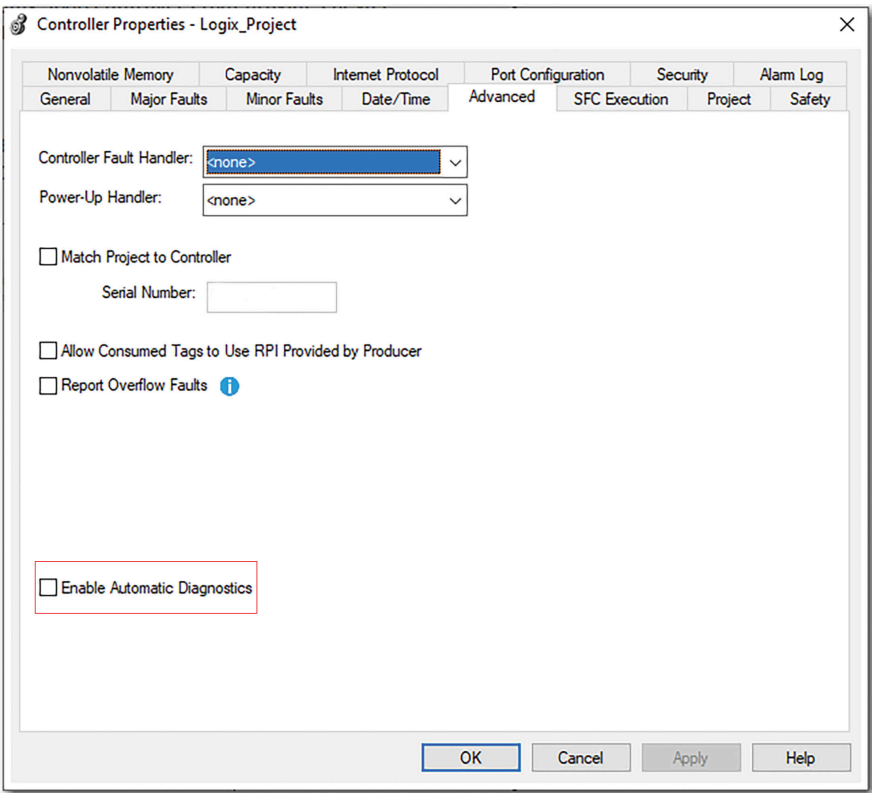
- 4. Continue to hold the reset button while the 4-character display cycles through DFLT, 4, 3, 2, 1, Factory Default.
- 5. After Factory Default appears, release the reset button

Automatic Diagnostics

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 controllers with firmware revision 33 or later. You can disable and enable the whole feature while online or offline from the Advanced tab on the Controller Properties dialog box. You can also disable Automatic Diagnostics for a specific device in the device's configuration.

Figure 83. Controller Properties Advanced Tab



Considerations for Communication Loss Diagnostics

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

Table 56. Connection and Device Behavior

Type of Connection	Device Behavior
Direct connection to a controller	The device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter.

Table 56. Connection and Device Behavior (continued)

Type of Connection	Device Behavior
No connection to a controller	Communication adapters that do not have a connection to the controller do not report communication loss diagnostics. We recommend that you configure your communications adapters for a status connection to make sure that they report any communication loss diagnostic in a timely manner.
Data connection	The device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter.
Rack-optimized connection	The device does not report communication loss diagnostics. The communication adapter reports communication loss diagnostics. A device with a rack-optimized connection has a reduced set of diagnostics as compared to a direct connection.

When enabled, the Automatic Diagnostics feature enables the following:

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

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

Controller Diagnostics with the Logix Designer Application

A warning symbol appears in the controller organizer next to the I/O module under these conditions:

- If there are faults or other conditions in the I/O module
- If the connection to the I/O module fails while in run mode

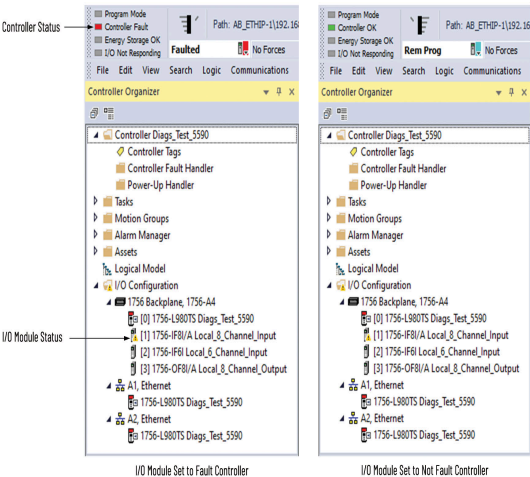
When the I/O module is configured to cause a major fault on the controller and an I/O module fault occurs, the following can result:

- Controller state displays Faulted.
- Controller status displays Controller Fault and blinks red.
- I/O module status displays I/O Not Responding and blinks green.

When the I/O module is not configured to cause a major fault on the controller and an I/O module fault occurs, the following result:

- Controller state displays the current state, for example, Rem Run.
- Controller status displays Controller OK and is steady green.
- I/O module status displays I/O Not Responding and blinks green.

Figure 84. I/O Fault on the Controller



IMPORTANT: Safety Consideration

You cannot configure safety connections to automatically fault the controller

Notification in the Tag Monitor

General module faults are also reported in the Tag Monitor. Diagnostic faults are reported only in the Tag Monitor. When the Value field is set to 1, a fault is present.

Figure 85. 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 86. 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	

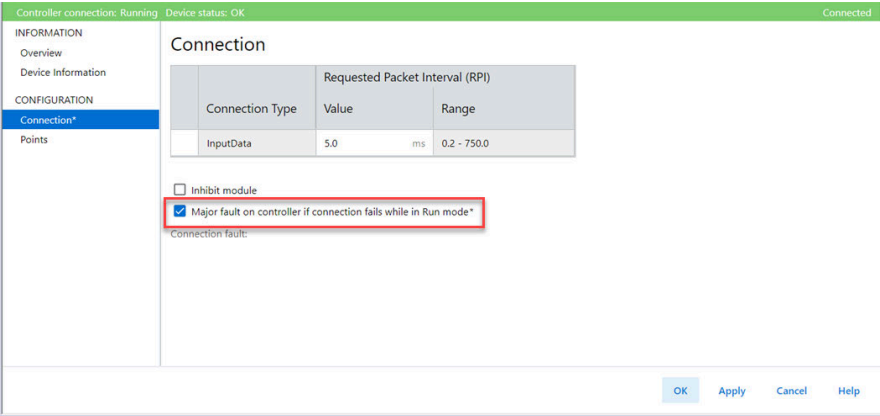
Enable Major Fault on Controller

To display recent I/O fault information on the Major Faults tab of the controller properties, you must first select Major Fault on Controller if Connection Fails While in Run Mode on the Connection view of the I/O Properties dialog box.



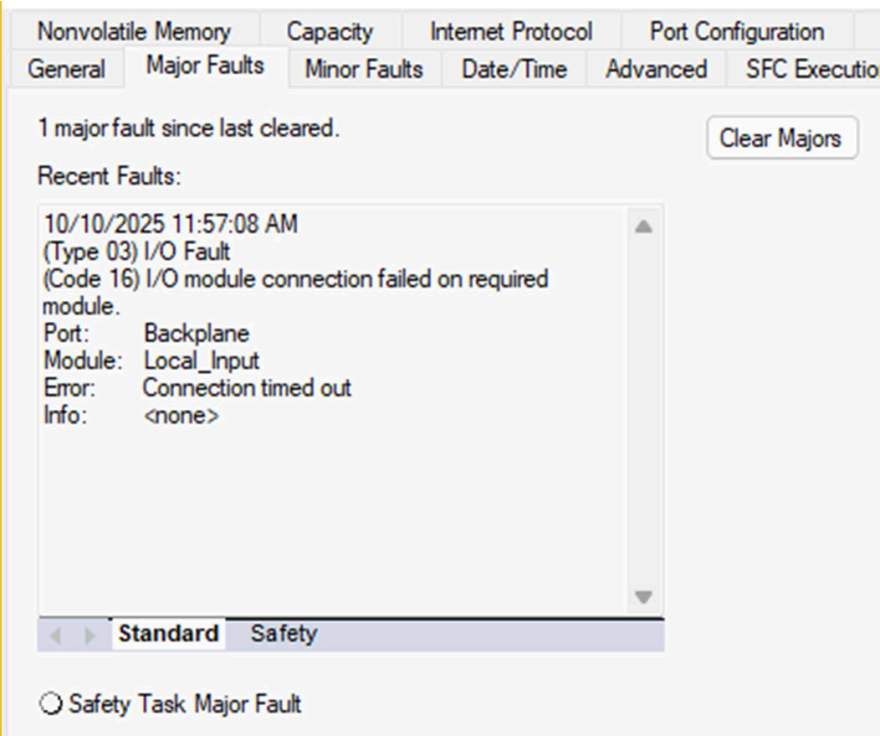
WARNING: If you select this option, a connection fault on the I/O module can cause a major fault on the controller. A major fault on the controller causes the outputs to go to their configured fault state.

Figure 87. Enable Major Fault on Controller



When you are monitoring the configuration properties of a module in the Studio 5000 Logix Designer® application and receive a communication fault message, the Major Faults tab for the controller properties indicates the type of fault under Recent Faults.

Figure 88. Major Faults Tab in Controller Properties





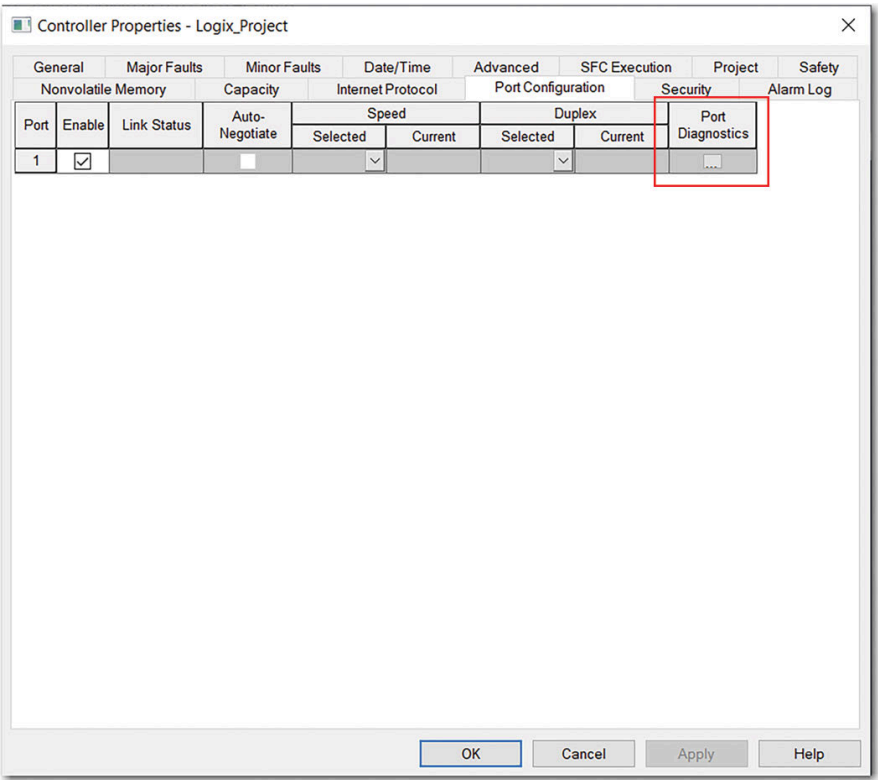
You can use the Minor Faults and Networks tabs to check for minor faults and network fault, respectively.

Port Diagnostics

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

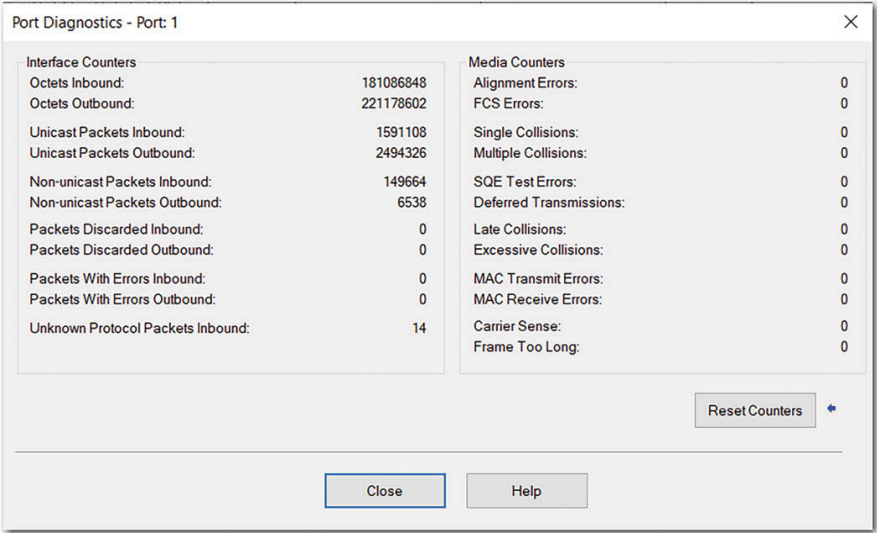
- 1. Access the Controller Properties.
- 2. On the Controller Properties dialog box, click the Port Configuration tab.
- 3. Click the Ellipse button in the Port Diagnostics column.

Figure 89. Ethernet Port Diagnostics



The Port Diagnostics dialog box displays diagnostic details.

Figure 90. Port Diagnostics Details



Parameters	Description
Interface Counters	The Interface Counters values have no value when you are offline or online and there is a communication error.
Octets Inbound	Displays the number of octets that are received on the interface.
Octets Outbound	Displays the number of octets that are transmitted to the interface.
Unicast Packets Inbound	Displays the number of unicast packets that are received on the interface.
Unicast Packets Outbound	Displays the number of unicast packets that are transmitted on the interface.
Non-unicast Packets Inbound	Displays the number of non-unicast packets that are received on the interface.
Non-unicast Packets Outbound	Displays the number of non-unicast packets that are transmitted on the interface.
Packets Discarded Inbound	Displays the number of inbound packets that are received on the interface but discarded.
Packets Discarded Outbound	Displays the number of outbound packets that are transmitted on the interface but discarded.
Packets With Errors Inbound	Displays the number of inbound packets that contain errors (excludes discarded inbound packets).
Packets With Errors Outbound	Displays the number of outbound packets that contain errors (excludes discarded outbound packets).
Unknown Protocol Packets Inbound	Displays the number of inbound packets with unknown protocol.
Media Counters	The Media Counters values have no value when you are offline or online and there is a communication error.
Alignment Errors	Displays the number of frames received that are not an integral number of octets in length.
FCS Errors	Displays the number of frames received that do not pass the FCS check.
Single Collisions	Displays the number of successfully transmitted frames that experienced exactly one collision.
Multiple Collisions	Displays the number of successfully transmitted frames that experienced multiple collisions.

Parameters	Description
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. The Reset Counter appears dimmed when offline or when online and a communication error occurs.

Advanced Time Sync

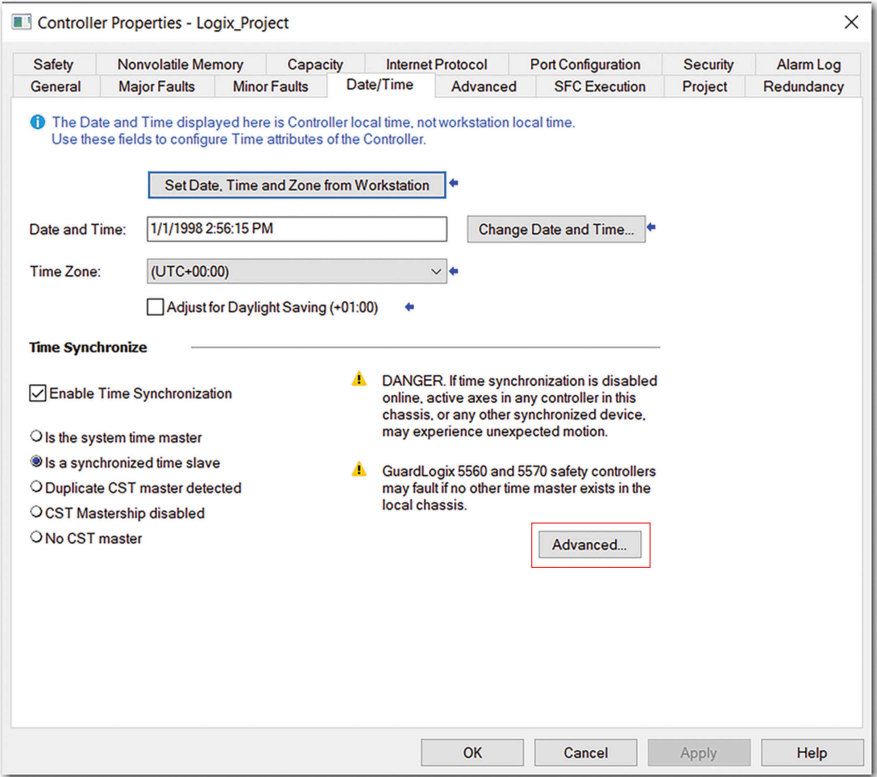
The Advanced Time Sync dialog displays information that is related to CIP Sync™ time synchronization. The information appears only if the project is online and Time Synchronization is enabled on the Date/Time tab.

IMPORTANT: Precision Time Protocol (PTP) Software

- Access to software that manages PTP on a control system network must be limited to users who are trained on the administration of industrial control system time including PTP. This includes the PTP update tool that is supplied by Rockwell Automation, or other publicly available PTP management software. Incorrect updates while a control system is running can disrupt the operation of the control system, including major faults and some devices taken offline.
- When disabling PTP on a controller, to give the controller time to process the disable, use a two-second delay before setting the WallClockTime (WCT) in the controller. Otherwise, there is a risk of the Grandmaster clock overwriting the WCT.

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

Figure 91. Controller Properties Date/Time Tab



The Advanced Time Sync dialog box opens.

Figure 92. Advanced Time Sync

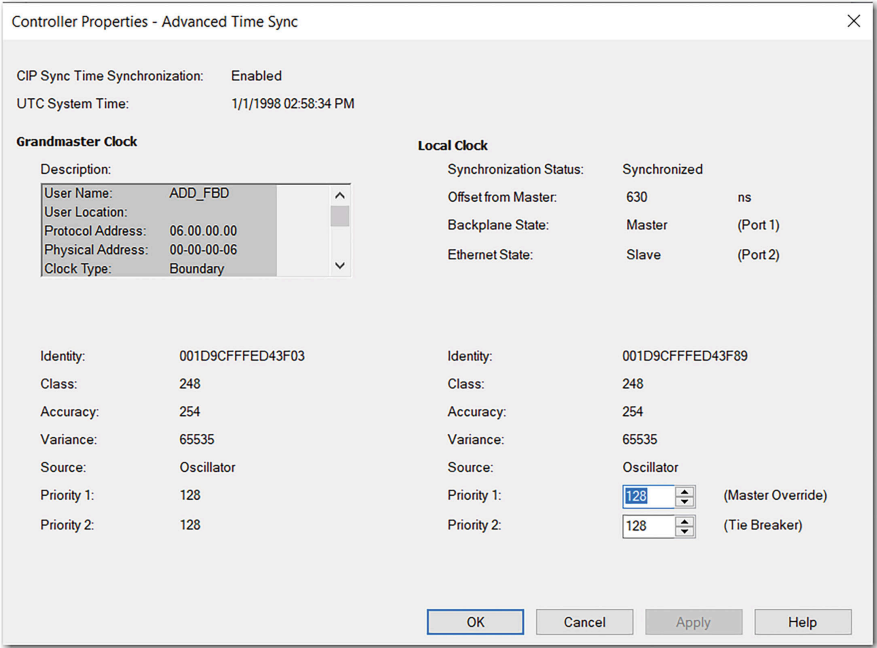


Table 57. Advanced Time Sync Parameters

Grandmaster Clock	
Description	Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified: • User Name • User Location • Protocol Address • Physical Address • Clock Type • Manufacturer Name • Model • Serial Number • Hardware Revision • Firmware Revision • Software Revision • Profile Identity • Physical Protocol • Network Protocol • Port Number Use the vertical scroll bar to view the data.
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0...255 with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the Grandmaster clock. The available values are: • Atomic Clock • GPS • Radio • PTP • NTP • HAND set • Other • Oscillator
Priority 1 / Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The priority values range from 0...255. The highest priority is zero. The default value for both settings is 128.
Local Clock	

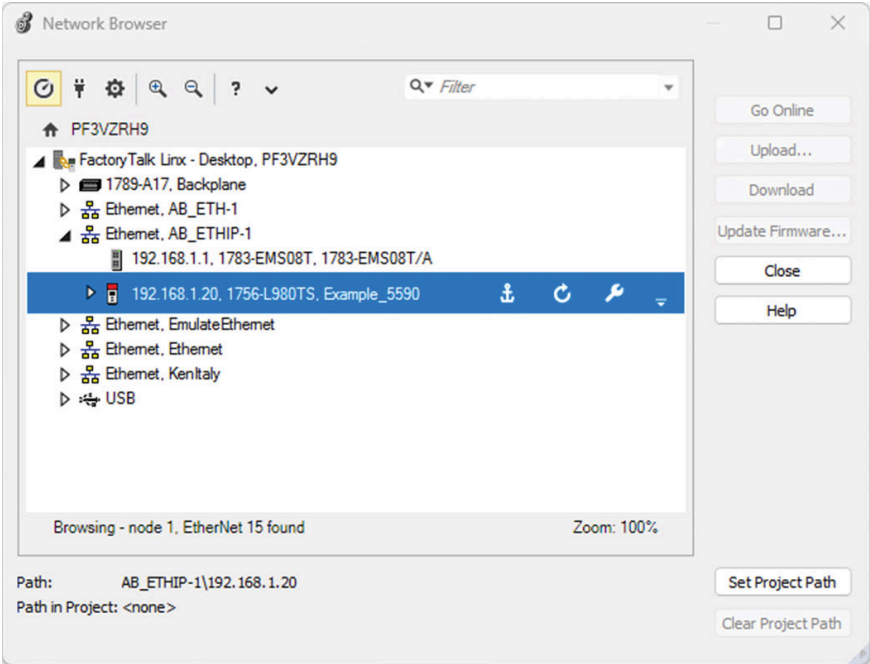
Table 57. Advanced Time Sync Parameters (continued)

Grandmaster Clock	
Synchronization Status	Displays whether the local clock is synchronized or not synchronized with the Grandmaster reference clock. A clock is synchronized if it has one port in the slave state and is receiving updates from the master.
Offset to Master	Displays the amount of deviation between the local clock and the Grandmaster clock in nanoseconds.
Backplane State	Displays the current state of the backplane. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Ethernet State	Displays the state of the Ethernet port. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the local clock. Values are defined from 0...255, with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the local clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the local clock. The available values are: • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP • HAND set • Other • Oscillator

Controller Diagnostics with Linux-based Software

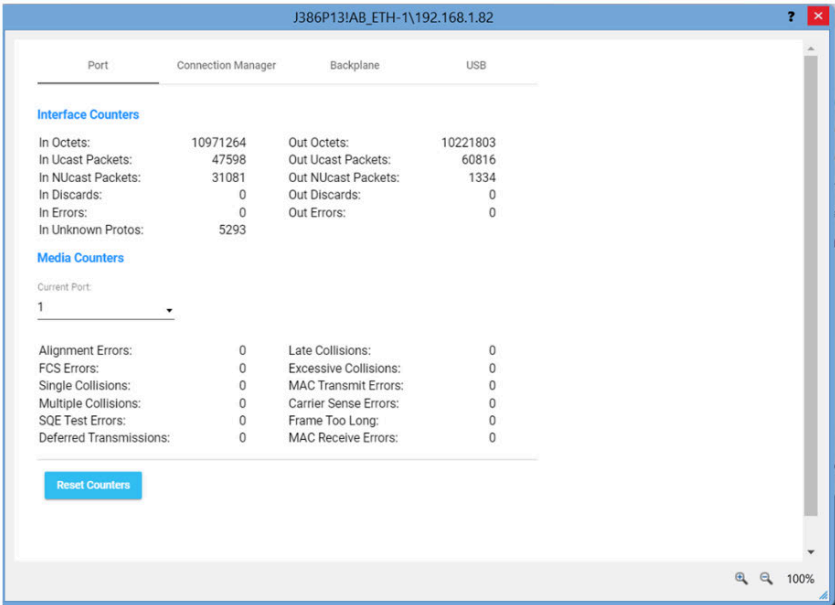
You can also view diagnostic information in Linux-based software.

1. From the Communications menu, select Who Active or Network Browser.
2. Navigate to the controller on the EtherNet/IP™ network.



3. Right-click the controller and choose Device Statistics.

The Statistics dialog box shows a variety of information.



Controller Webpages

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

IMPORTANT: Controller webpages are disabled by default .

- To enable the controller webpages, select the checkbox on the Security tab of the controller properties.

Controller Properties - Logix_Project

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

Audit Value:

Tracked State Value:

- For CIP Security™ applications, you can also use FactoryTalk® Policy Manager to enable the webpages. FactoryTalk® Policy Manager overrides the Controller Properties checkbox.

To access the diagnostic webpages, follow these steps.

1. Open your web browser.
2. In the Address field, type the IP address of the controller and press Enter.
3. To access the diagnostic webpages, use the links in the left-side navigation bar. Some links are only accessible if you open the folder in which they exist.

EtherNet/IP settings and safety applications can slightly modify the web pages. In general, the web pages offer:

- Home webpage provides device information and controller status
- Faults webpage shows major and minor faults on the controller.
- Diagnostics webpages provide communications and messaging data for the controller.

- Tasks webpage shows CPU utilization of the control and communications cores and summarizes the tasks that are running in the controller.
- Browse Chassis webpage lets you view module information, backplane statistics, and connection statistics for modules in the local chassis.

Status Indicators

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

IMPORTANT: Status indicators do not provide detailed diagnostics for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

The controller has eight status indicators and one four-character scrolling status display. The 1756-L9SP safety partner has the four-character scrolling status display and the MOD status indicator.

Figure 93. Status Indicators

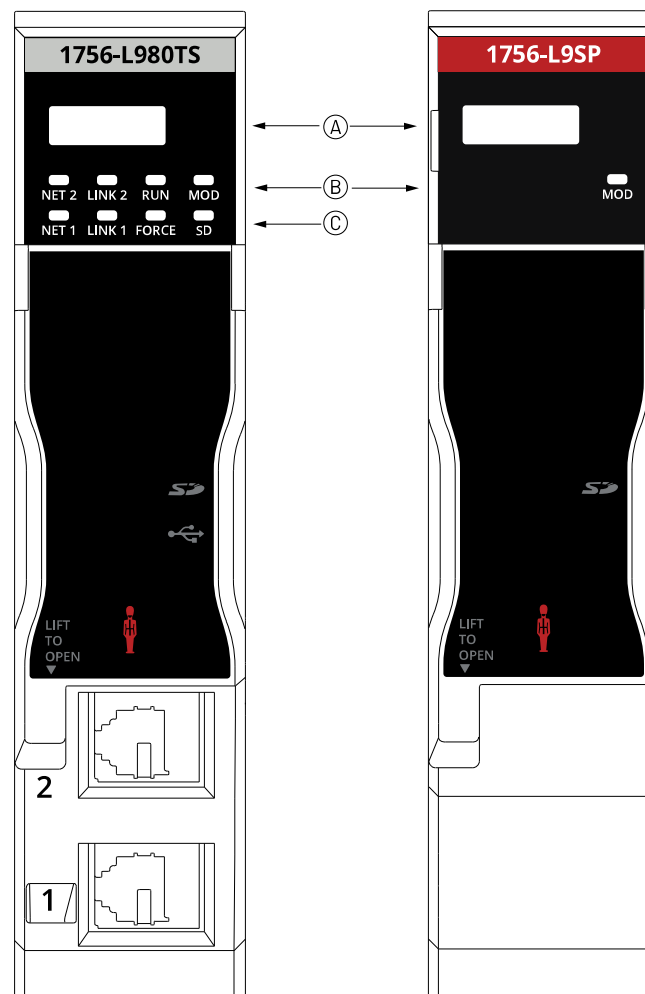


Table 58. Status Indicators

Letter	Item	Description
A	4-character display	Scrolls information about the module.

Table 58. Status Indicators (continued)

Letter	Item	Description
B	Module Status Indicators	Indicates the current state of the module (MOD, RUN, FORCE, SD).
C	Ethernet Status Indicators	Indicates the current state of transmission of data on the EtherNet/IP™ network (LINK, NET).

MOD Indicator

The MOD status indicator shows the state of the controller.

Table 59. Controller MOD Status Indicator

State	Description
Off	No power is applied to the device.
Steady red	The device has a Major Unrecoverable Fault
Flashing red	The device has a Major Recoverable Fault.
Steady green	The device is operating normally.
Flashing green	The device is in one of the following states: - The device is not configured. - The module requires a firmware update. - Firmware update in progress. - The module is saving a project to internal or external non-volatile memory. - The charge of the capacitor in the ESM is being discharged upon powerdown.. - The module is experiencing a Hardware Preservation Fault due to a high internal module temperature. In this condition, only the status indicator receives power. Once the module cools down to an acceptable temperature, then full power is applied.
Flashing green/red	The device is performing its power up testing.

Safety Partner MOD Indicator

The safety partner has an MOD status indicator.

Table 60. Safety Partner MOD Status Indicator

State	Description
Off	No power is applied.
Steady green	The safety partner is operating with no faults.
Flashing green	One of the following is true: - The safety partner is completing power-up diagnostics. - The charge of the capacitor in the ESM is being discharged upon powerdown. - The safety partner is powered but is inoperable.

Table 60. Safety Partner MOD Status Indicator (continued)

State	Description
	- 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	The controller is configured for SIL 2 operation, but a safety partner is installed.

RUN Indicator

The RUN status indicator shows the current mode of the controller.

To change the controller mode, you can use the controller switch on the front of the controller or the Controller Status menu in the Studio 5000 Logix Designer® application.

Table 61. RUN Status Indicator

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

FORCE Indicator

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

Table 62. FORCE Status Indicator

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

SD Indicator

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

Table 63. SD Status Indicator

State	Description
Off	No activity is occurring with the SD card.

Table 63. SD Status Indicator (continued)

State	Description
Flashing green	The controller is reading from or writing to the SD card.
Steady green	NOTE: Do not remove the SD card while the controller is reading or writing. Allow the read/write to complete without interruption. If you interrupt the read/write, data corruption or loss can occur.
Flashing red	The SD card does not have a valid file system.
Steady red	The controller does not recognize the SD card.

EtherNet/IP Indicators

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

Table 64. EtherNet/IP Status Indicators

Indicator	State	Description
NET	Off	- The controller is not configured, or does not have an IP address. - The port is administratively disabled. - In a dual-port controller, the EtherNet/IP mode is Linear/DLR mode. In this case, the NET A2 indicator is off. The NET A1 indicator remains on.
	Flashing green	The controller has an IP address, but no active connections are established.
	Steady green	The controller has an IP address and at least one established active connection.
	Steady red	Duplicate IP address or invalid configuration.
LINK	Off	No activity. One of these conditions exists: - No link exists on the port. - Verify that the RJ45 cables are properly seated in the adapter and connected devices. - The port is administratively disabled. - In a dual-port controller, LINK A2 only - The controller is the active ring supervisor in a DLR network and has detected a rapid ring fault.
	Flashing green	All of these conditions exist: - The port is enabled. - A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device. - There is activity on the port.
	Steady green	On a single-port controller, a link exists on the port, but no traffic is being received.

Table 64. EtherNet/IP Status Indicators (continued)

Indicator	State	Description
		On a dual-port controller, all of these conditions exist: • The port is enabled. • A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device. • LINK A2 only - The controller is the active ring supervisor in a DLR network, and the ring is not broken. This is a normal operation. • There is no activity on the port.

General Status Messages

The scrolling messages that are described in this table are typically indicated upon powerup, power down, and while the controller is running to show the status of the controller.

Table 65. Controller General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Determine if the controller is powered and determine the state of the controller
Identity Mismatch—Contact Tech Support	If a firmware update identifies the controller as not authentic, the hardware is permanently disabled.
TEST	The controller is conducting power-up tests.
CHRG	The embedded energy storage circuit is charging.
PASS	Power-up tests have been successfully completed.
Saving...Do Not Remove SD Card	The controller is about to save an image to the SD card.
SAVE	A project is being saved to the SD card. Allow the save to complete before: • Removing the SD card. • Disconnecting the power. IMPORTANT: Do not remove the SD card while the controller is saving to the SD card. Allow the save to complete without interruption. If you interrupt the save, data corruption or loss can occur.
LOAD	A project is being loaded from the SD card. Allow the load to complete before doing the following: • Removing the SD card. • Disconnecting the power. IMPORTANT: Do not remove the SD card while the controller is loading from the SD card. Allow the load to complete without interruption. If you interrupt the load, data corruption or loss can occur.
UPDT	A firmware update is being conducted from the SD card upon powerup. If you do not want the firmware to update upon powerup, change the Load Image property of the controller.
Rev XX.xxx	The major and minor revision of the firmware of the controller.

Table 65. Controller General Status Messages (continued)

Message	Interpretation
Catalog number	The controller catalog number and series.
Link Down	The message appears when the Ethernet port does not have a connection. The message scrolls continuously during operation.
Link Disabled	The message appears when you have disabled the Ethernet port. The message scrolls continuously during operation.
Link <x> crossload-redund-en	The message appears when the controller is configured for front port synchronization and shows the relevant Ethernet ports (1 or 1/2). The message scrolls continuously during operation.
DHCP- 00:00:XX:XX:XX:XX	The message appears when the controller is set for DHCP but not configured on a network. The message shows the MAC address of the controller. The message scrolls continuously during operation if no IP address is set.
Ethernet Port Rate/Duplex State	The current port rate and duplex state when the Ethernet port has a connection. The message scrolls continuously during operation.
IP address	The IP address of the controller. Appears on powerup, then scrolls continuously during operation. If the IP address is not yet set, then the MAC address appears.
Duplicate IP - 00:00:XX:XX:XX:XX	The message appears when the controller detects a device on the network that has the same IP address as the controller Ethernet port. The message shows the MAC address of the device with the duplicate IP address. The message scrolls continuously during operation.
No Project	No project is loaded on the controller. To load a project, do one of the following: • Download a project to the controller • Use an SD card to load a project to the controller
Project Name	The name of the project that is loaded on the controller.
BUSY	The I/O modules that are associated with the controller are not yet fully powered. Allow time for powerup and I/O module self-testing.
Corrupt Certificate Received	The security certificate that is associated with the firmware is corrupted. Go to rok.auto/support and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Corrupt Image Received	The firmware file is corrupted. Go to rok.auto/support and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Backup Energy HW Failure - Save Project	A failure with the embedded storage circuit has occurred, and the controller is incapable of saving the program if a powerdown occurs. If you see this message, then save your program to the SD card before you remove power and then replace the controller.
Backup Energy Low - Save Project	The embedded storage circuit does not have sufficient energy to enable the controller to save the program if a powerdown occurs. If you see this message, then save your program to the SD card before you remove power, and then replace the controller.

Table 65. Controller General Status Messages (continued)

Message	Interpretation
Flash in Progress	A firmware update that is initiated via ControlFLASH Plus®, ControlFLASH™ or AutoFlash software is in progress. Allow the firmware update to complete without interruption.
Firmware Installation Required	The controller is using boot firmware (revision 1.xxx) and requires a firmware update.
SD Card Locked	An SD card that is locked is installed.
SD Card Unprotected	The controller SD card has been unprotected and is available for remote read/write operations.
Download in Progress	An active download is occurring
Aborting Download	An active download is being canceled. This may be due to a user-initiated cancel, a download failure, or connection loss. After completion, the No Project status message displays.

Safety Status Messages

In addition to the general status messages, these safety messages can display as scrolling messages.

Table 66. Safety Status Messages

Message	Interpretation
No Safety Signature	Safety Task is in Run mode without a safety signature. Generate a safety signature.
Safety Unlocked	The controller is in Run mode with a safety signature but is not safety-locked. Safety-lock the controller.
Safety Partner Missing	The safety partner is missing or unavailable. Make sure that the safety partner is seated properly in the slot that is immediately to the right of the safety controller. The controller displays this message only in a SIL 3/PLc configuration.
Hardware Incompatible	ControlLogix and GuardLogix only The safety partner and primary controller hardware are incompatible. The controller displays this message only in a SIL 3/PLc configuration.
Firmware Incompatible	ControlLogix and GuardLogix only The safety partner and primary controller firmware revision levels are incompatible. Update the modules to the correct firmware revision. The controller displays this message only in a SIL 3/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

The safety partner display can show these scrolling messages.

Table 67. Safety Partner Status Messages

Message	Interpretation
L9SP	Standard display text. If there is a major nonrecoverable fault, then the fault code scrolls across the display.
Flash in Progress	A firmware update is in progress. Allow the firmware update to complete without interruption.

Fault Messages

If the controller displays a fault, these scrolling messages can appear on the status display. For more information about how to monitor and handle major and minor controller faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#).

Table 68. 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. Major faults of Type 1, Codes 60, 61, 62 include a unique 9-character code that you can provide to Rockwell Automation® support for troubleshooting.
I/O Fault Local:X #XXXX message	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated.
I/O Fault ModuleName #XXXX message	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module is indicated with the fault code and a brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named My_Module is not open. Take corrective action specific to the type of fault indicated.
I/O Fault ModuleParent:X #XXXX message	An I/O fault has occurred on a module in a remote chassis. The parent name of the module is indicated because no module name is configured in the I/O Configuration tree of the Logix Designer application. In addition, the fault code is indicated with a brief description of the fault. For example, I/O Fault My_CNet:3 #0107 Connection Not Found indicates that a connection to a module in slot 3 of the chassis with the communication module named My_CNet is not open. Take corrective action specific to the type of fault indicated.
X I/O Faults	I/O faults are present and X = the number of I/O faults present. If there are multiple I/O faults, the controller indicates the first fault reported. As each I/O fault is resolved, the number of indicated faults decreases and the I/O Fault message indicates the next reported fault. Take corrective action specific to the type of fault indicated.

Major Fault Messages

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

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

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

I/O Fault Codes

The controller indicates I/O faults on the status display in one of these formats:

- I/O Fault Local:X #XXXX message
- I/O Fault *ModuleName* #XXXX message
- I/O Fault *ModuleParent:X* #XXXX message

The first part of the format is used to indicate the location of the module with a fault. How the location is indicated depends on your I/O configuration and the properties of the module that are specified in the Studio 5000 Logix Designer® application.

The latter part of the format, #XXXX message, can be used to diagnose the type of I/O fault and potential corrective actions.

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

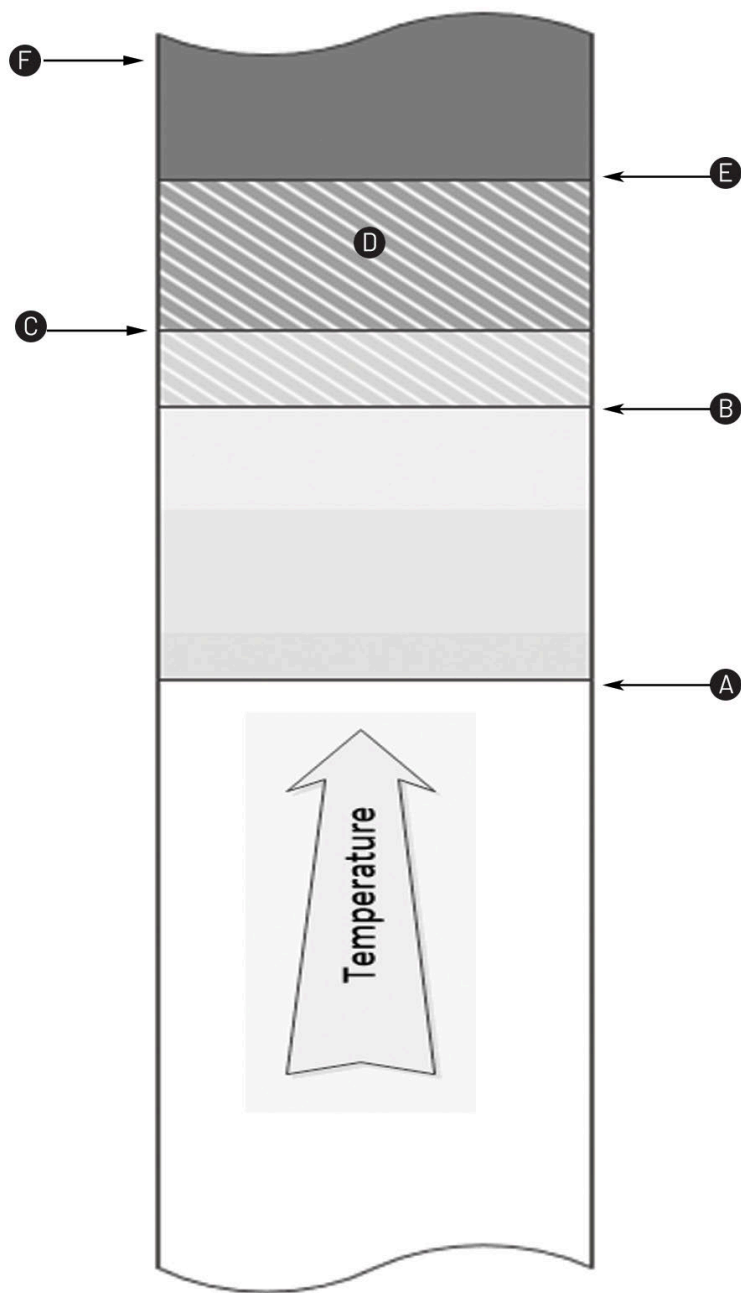
For suggested recovery methods for major faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication [1756-PM014](#).

Thermal Monitoring and Thermal Fault Behavior

The controllers can monitor internal module temperatures and act as the temperature increases.

IMPORTANT: If you follow the recommended limits for ambient (inlet) temperature and apply the required clearances around the chassis, the controller should not reach the initial warning (minor fault) temperature. See the 1756 ControlLogix and GuardLogix Controllers Technical Data, publication [1756-TD001](#).

Figure 94. Thermal Monitoring



Item	Description
A	Threshold for controller to declare a 'T17:C35 Controller internal temperature is approaching operating limit' minor fault and set the Diagnostics minor fault bit. The fault is recorded in the minor fault log but is not displayed on the front panel. If the temperature returns to an acceptable range, the Diagnostics minor fault bit clears, but the minor fault record remains.
B	Threshold for the controller to declare a 'CPU Temperature Fault' major recoverable fault. If a fault handler does not clear the fault, then the module enters fault mode, records the fault in the major fault log, and displays 'T17:C34 CPU Temperature Fault' on the front panel.
C	Hardware Preservation Hysteresis Limit.

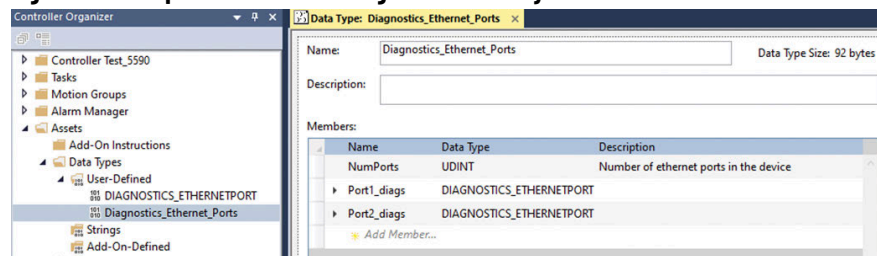
Item	Description
D	Power does not become enabled when in this range.
E	Threshold for the controller to declare a 'Hardware Preservation Fault', resetting the module and disabling power. In the disabled power condition, only the OK status indicator is illuminated, and it is red. The module does not apply power until it has cooled below the Hardware Preservation Hysteresis limit. The module then enters fault mode, records the fault in the major fault log, and displays 'CPU Temperature Fault' on the front panel.
F	All power to the controller is disabled except to run the red OK status indicator and monitor the temperature.

IMPORTANT: The presence of any temperature warning indicates that you must act to reduce the ambient temperature of the module. Instructions for using relay ladder logic to check for a minor fault can be found in the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#). A GSV instruction can read the MinorFaultBits attribute of the FaultLog class name. If the Diagnostics minor fault bit (Bit 17) is set, then a temperature minor fault can be present. Check the Minor Faults tab of the Controller Properties dialog box in the Logix Designer application to see if the minor fault is a temperature warning.

Access Diagnostic Assembly Tags

Use diagnostic assembly tags to access controller status from the controller webpages and other diagnostic information. Each assembly has specific elements. You create UDTs and use MSG instructions to access the data in these elements.

Figure 95. Example Ethernet Ports Diagnostic Assembly



The available diagnostic assemblies include:

Table 69. Diagnostic Assemblies

Diagnostic Assembly	Description
Home	Provides device information and controller status.
Home (Safety)	Safety-related data for a safety-enabled controller.
Module Diagnostics	Module communication diagnostics.
Ethernet Statistics	Ethernet port diagnostics.
Faults	Faults data that shows major and minor faults on the controller.
OPC UA	OPC webpage data that includes number of currently used OPC UA nodes, OPC UA nodes limit, and OPC UA nodes per second statistics.
PTP	1588 PTP Time Sync webpage data.
Concurrent Connections	Concurrent Connection data information that includes Branch Failure, Failure Count, and Packets Lost.
Backplane Statistics	Diagnostics for a specific slot in a chassis.
Standard Network Diagnostics	Standard network diagnostics includes four main diagnostic assemblies for Single Port controllers, Device Level Ring (DLR), Dual-IP configuration, and PRP (Parallel Redundancy Protocol). - Single Port supports ControlLogix® 5580 controllers. - DLR supports ControlLogix® 5590 controllers, CompactLogix® 5380 controllers, and 1756-EN4TR communication modules. - Dual-IP supports ControlLogix® 5590 controllers and CompactLogix® 5380 controllers. - PRP supports 1756-EN4TR communication modules.

Create a MSG Instruction to Access a Diagnostic Assembly

Use a CIP™ Generic MSG to access diagnostic assembly data.

- 1. Configure the Configuration tab on the Message Configuration dialog box as described below.

Message Configuration - Diags_Ethernet_Ports

Configuration*

Communication

Tag

Message Type:

CIP Generic

Service Type:

Get Attribute Single

Source Element:

Source Length:

0

(Bytes)

Service Code:

e

(Hex)

Class:

4

(Hex)

Destination Element:

Diagnostics_Ethernet

Instance:

32933

Attribute:

3

(Hex)

New Tag...

☐ Enable

☐ Enable Waiting

☐ Start

☐ Done

Done Length: 0

☐ Error Code:

Extended Error Code:

☐ Timed Out

Error Path:

Error Text:

OK

Cancel

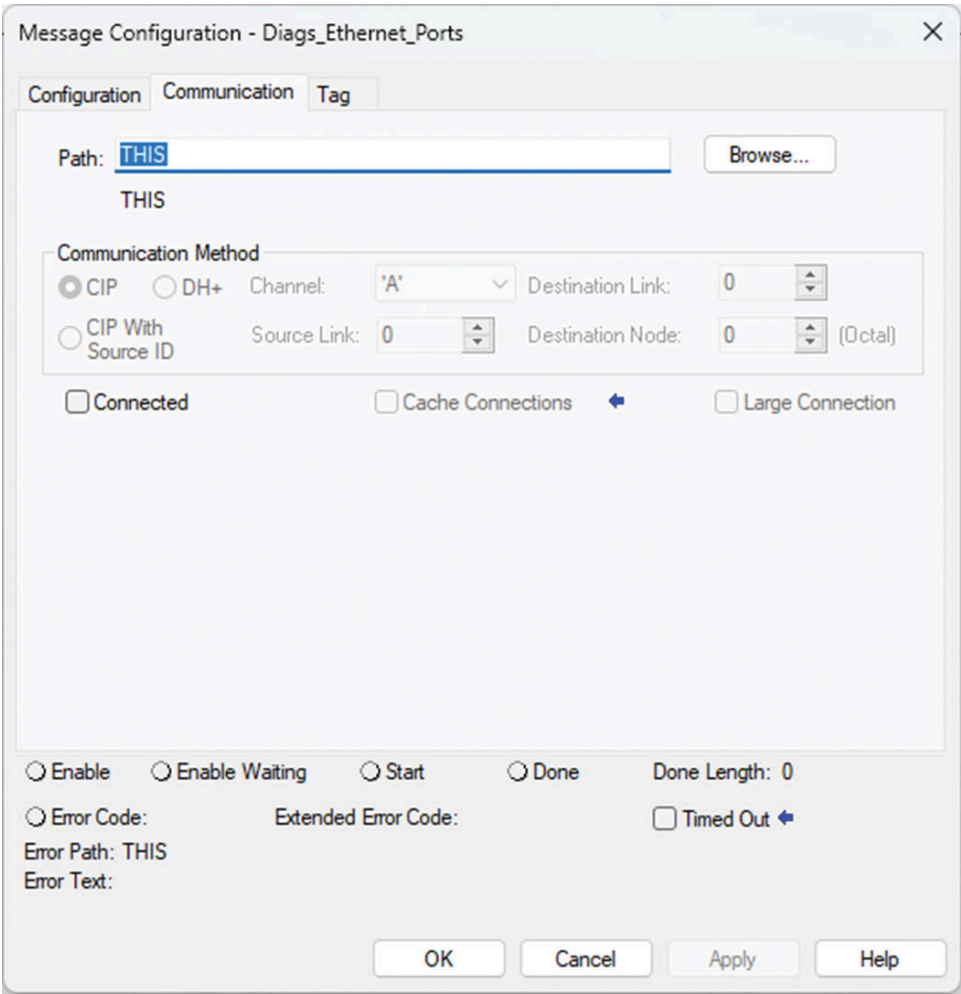
Apply

Help

Table 70. Configure MSG Instruction

Field	Value
Message Type	CIP Generic
Service Type	Get Attribute Single
Class	4
Attribute	3
Instance	Specific to the diagnostic assembly. Must be in decimal format.
Destination Element	Controller tag of the UDT for the diagnostic assembly.

- 2. On the Communication tab, specify a Path of THIS for the local controller, or specify a remote controller.



Concurrent Connections Diagnostic Assembly

- Concurrent Connection data information that includes Branch Failure, Failure Count, and Packets Lost.
- Instance = 32952
 - Size = 12 Bytes

Table 71. Diagnostic Assembly Members

Member	Data Type	Description
BranchFailure	BOOL	This attribute indicates that one or more branches towards target(s) of any concurrent connections in which this device is a participant is not open (was not opened or timed out).
FailureCount	UDINT	This attribute is incremented every time when the Concurrent Connections Branch Failure attribute transitions from 0 to 1.
PacketsLost	UDINT	For each concurrent connection, as long as it remains open when the consumer on the branch of concurrent connection is processing the packet, it shall subtract the last received Concurrent Connection Sequence Count on this branch from the Concurrent Connection Sequence Count of this packet. If the value exceeds positive one (+1), then that value minus one is the number of concurrent connection packets that have been lost. A concurrent connection branch timeout does not cause Concurrent Connection Packets Lost to increment.

Ethernet Port Diagnostics Assembly

Ethernet Statistics webpage data.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_ETHERNETPORT user-defined data type (UDT). This data type includes the information captured for each Ethernet port. Create this UDT before you create the Ethernet Port Diagnostics UDT.

Structure for the DIAGNOSTICS_ETHERNETPORT User-defined Data Type

Table 72. Members for User-defined Data Type

Member	Data Type	Description
PortNumber	UDINT	Number of the port. Represents the instance number of the TCP/IP Interface Object.
IPAddress	USINT[4]	IP address of the port.
MacAddress	USINT[6]	Mac address of the port.
TCPConnections	UINT	TCP connections opened through the port.
CIPConnections	UINT	Total number of class 0/1 and 3 CIP connections opened through the port (sum of CIP I/O Connections attribute and CIP Explicit Connections attribute).
CIPLostPackets	UDINT	Number of lost CIP packets sent via port.
CIPTimeouts	UDINT	Number of timeouted CIP connections sent via port.
HMIPacketRate	UDINT	HMI packet rate sent via port.
IOPacketRate	UDINT	I/O packet rate sent via port.
EthernetErrors	UDINT	Number of ethernet errors in the port.
CPUUtilization	UINT	Utilization of the CPU (same for all ports).

Ethernet Port Diagnostics Assembly

- Instance = 32933
- Size = 180 Bytes

Table 73. Diagnostic Assembly Members

Member	Data Type	Description
NumPorts	UDINT	Number of ethernet ports in the device
Port1	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.
Port2	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.
Port3	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.

Table 73. Diagnostic Assembly Members (continued)

Member	Data Type	Description
Port4	DIAGNOSTICS_ETHERNETPORT	Information about each port. If port does not exist - it is empty.

Home Webpage Diagnostic Assembly

Home webpage data that provides device information and controller status.

- Instance = 32930
- Size = 270 Bytes

Table 74. Diagnostic Assembly Members

Member	Data Type	Description
CatalogString	STRING_32	Textual catalog or model number.
ProductCode	UINT	Identification of a particular product of an individual vendor.
MajorRevision	USINT	Major revision of the module.
MinorRevision	USINT	Minor revision of the module.
CIPSerialNumber	UDINT	Serial number of device.
WarrantySerialNumber	STRING_32	Serial number of product warranty.
ManufactureDate	UINT	Date the product was manufactured.
ProjectName	STRING	Name of the project downloaded into the module.
StatusBits (Hidden)	UDINT	Summary status of device.
RunMode	BOOL	Indicates whether controller is in the run mode.
KeySwitchRemote	BOOL	Specifies whether the key is in the "remote" position.
IOForcesExist	BOOL	Indicates whether IO forces exists. It is true only when "Force" LED is amber or flashing.
IOForcesActive	BOOL	Indicates whether IO forces are enabled. Logix Designer labels it "Forces" / "No Forces". It is true only when "Force" LED is amber.
SDCardFault	BOOL	Specifies whether SD card fault appeared. It is true if SD LED is solid or flashing red.
SDCardActivity	BOOL	Specifies whether SD card is active. It is true if SD LED is solid or flashing green.
MajorFault	BOOL	A value that indicates whether the module has a major fault. It is bit 4.
MinorFault	BOOL	A value that indicates whether the module has a minor fault. It is bit 5.
IOFault	BOOL	A value that indicates whether the module has a IO fault.

Table 74. Diagnostic Assembly Members (continued)

Member	Data Type	Description
EnergyStorageStatus	BOOL	From LogixDesigner this is: minor_fault_bits.10 If minor_fault_bits.10 is on, depending on the controller, the battery is low or the ESM or UPS needs to be replaced or is missing.
StatusDisplayText	STRING	Scrolling string includes: • Project Name • Ethernet Address • Link State (Up Down) • Link Speed • IO Fault • Redundancy State
MajorHardwareRevision	USINT	Major revision of the module hardware.
MinorHardwareRevision	USINT	Minor revision of the hardware module.
HardwareSeries	SINT[2]	Two ASCII characters describing the hardware series. It is Rockwell extension to the Identity object.

Home (Safety) Diagnostic Assembly

Safety-related data on the Home webpage for a safety-enabled controller.

- Instance = 32931
- Size = 96 Bytes

Table 75. Diagnostic Assembly Members

Member	Data Type	Description
SafetyStatus	BOOL	SIL 2/SIL3 Status information of the safety task and the partnership between the controller and its safety partners.
SafetyLocked	BOOL	Indicates if the safety application is in the locked state.
SafetySigned	BOOL	Indicates if a Safety Signature has been created and the controller is in a protected state.
SafetySignatureID	UDINT	ID portion of the safety signature CRC over safety memory. Returns zero when no snapshot exists, or on controllers that do not support a four-byte safety signature.
SafetySignatureTimestampString	STRING	Software generated timestamp that indicates when a Safety Signature was generated. Contains the Safety Signature Timestamp String when a valid snapshot exists. Maximum length is 40 characters. Format of string is "mm/dd/yyyy, hh:mm:ss.iii <AM or PM>" where iii = milliseconds. This string is set to "Non-existing" when no snapshot exists.

Module Diagnostics Diagnostic Assembly

Module Diagnostics webpage data.

- Instance = 32932
- Size = 20 Bytes

Table 76. Diagnostic Assembly Members

Member	Data Type	Description
IOConnections	UINT	Number of I/O connections (class 0/1).
MessagingConnections	UINT	Number of messaging connections (class 3).
MaxObservedConnections	UINT	Maximum number of observed class 3 connections.
IOCommsUtilizationActual	UINT	Represents the current I/O communications utilization for I/O traffic.
IOCommsUtilizationTheoretical	UINT	Based on information agreed during Forward Open procedure. Represents the theoretical I/O communications utilization for I/O traffic.
IOPPSActual	UDINT	I/O messages packets per second.
IOPPSTheoretical	UDINT	Based on information agreed during Forward Open procedure. The theoretical value for I/O messages packets per second.

OPC UA Diagnostic Assembly

OPC webpage data that includes number of currently used OPC UA nodes, OPC UA nodes limit, and OPC UA nodes per second statistics.

- Instance = 32940
- Size = 12 Bytes

Table 77. Diagnostic Assembly Members

Member	Data Type	Description
UsedNodes	UDINT	Number of currently used OPC UA user defined nodes for a server associated with this instance.
MaxNodes	UDINT	Maximum possible number of OPC UA user defined nodes that a client can write or read from a server associated with this instance.
NodesPerSecond	UDINT	Current number of read or written scalar nodes per second. Scalar node means node with one basic type value or with one string. Vector and matrix nodes are counted as the number of its atomic elements.

PTP Diagnostic Assembly

1588 PTP Time Sync webpage data.

- Instance = 32941
- Size = 88 Bytes

Table 78. Diagnostic Assembly Members

Member	Data Type	Description
Enabled	BOOL	Is PTP enabled.

Table 78. Diagnostic Assembly Members (continued)

Member	Data Type	Description
TimeTransmitter	BOOL	Is The Grandmaster
SyncValid	BOOL	Sync status.
DomainNumber	USINT	Domain number
StepsRemoved	UINT	Steps removed.
SyncStatus	UDINT	CipSyncSynchronizationStatus. Available options are: init (0), synchronization hold timed out (1), synchronization hold (2) and synchronized (3).
UTCTime	STRING_32	SystemTime in user-friendly type. Counted using SystemTime.
SystemTime	ULINT	SystemTimeNanoseconds
OffsetFromTimeTransmitter	ULINT	Offset from master
MaxOffsetFromTimeTransmitter	ULINT	Max Offset from master.
AvgPathDelayTime	ULINT	Mean path delay to master.
SystemToLocalClockOffset	ULINT	Offset between system time and local time.

Faults Diagnostic Assembly

Faults webpage data that shows major and minor faults on the controller.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_FAULTDETAILS user-defined data type. This data type includes the information captured for each fault. Create this UDT before you create the Fault UDTs.

Structure for the DIAGNOSTICS_FAULTDETAILS User-defined Data Type

Table 79. Members of User-defined Data Type

Member	Data Type	Description
Timestamp	ULINT	The moment when the fault occurred. It's format is the UNIX timestamp in microseconds.
Code	UDINT	Fault code.
Type	UDINT	Type number of the fault code.
Description_1	STRING	Part 1 of the fault description.
Description_2	STRING	Part 2 of the fault description.

Diagnostic Faults_A Assembly

- Instance = 32934
- Size = 392 Bytes

Table 80. Diagnostic Assembly Members

Member	Data Type	Description
MajorFaultsReported	UDINT	Count of all Major Faults reported
MinorFaultsReported	UDINT	Count of all Minor Faults reported
MajorFault1	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MajorFault2	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_B Assembly

- Instance = 32935
- Size = 192 Bytes

Table 81. Diagnostic Assembly Members

Member	Data Type	Description
MajorFault3	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_C Assembly

- Instance = 32936
- Size = 384 Bytes

Table 82. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault1	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault2	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_D Assembly

- Instance = 32937
- Size = 384 Bytes

Table 83. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault3	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault4	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_E Assembly

- Instance = 32938
- Size = 384 Bytes

Table 84. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault5	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault6	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

Diagnostic Faults_F Assembly

- Instance = 32939
- Size = 384 Bytes

Table 85. Diagnostic Assembly Members

Member	Data Type	Description
MinorFault7	DIAGNOSTICS_FAULTDETAILS	Fault details structure.
MinorFault68	DIAGNOSTICS_FAULTDETAILS	Fault details structure.

ControlLogix Backplane Statistics

Diagnostics for a specific slot in a chassis.

IMPORTANT: This assembly includes the structure for the DIAGNOSTICS_CHASSIS_SLOTS_DATA user-defined data type. This data type includes the information captured for each slot. Create this UDT before you create the Chassis Diagnostics UDTs.

Structure for the ControlLogix DIAGNOSTICS_CHASSIS_SLOTS_DATA User-defined Data Type**Table 86. Members of User-defined Data Type**

Member	Data Type	Description
MajorRevision	UDINT	Major revision of the module in the slot (for specific module in chassis).
MinorRevision	UDINT	Minor revision of the module in the slot (for specific module in chassis).
SerialNumber	UDINT	Serial number of the module in the slot (for specific module in chassis).
Slot	USINT	Slot number (for specific module in chassis).
Status	USINT	Current status of ICP object: 0 normal communications, bit 0 set = RX Disabled, bit 1 set = Multicast RX Disabled, bit 2 set = RA/GA Mismatch
RxBadMulticastCRC	UDINT	Number of multicast frames received with bad CRC (for specific module in chassis).

Table 86. Members of User-defined Data Type (continued)

Member	Data Type	Description
RxBadMulticastCRCThreshold	UDINT	Threshold of the number of multicast frames received with bad CRC (for specific module in chassis).
RxBadCRC	UDINT	Number of frames received with bad CRC (for specific module in chassis).
RxBusTimeouts	UDINT	Number of timeouts on received frames (for specific module in chassis).
TxBadCRC	UDINT	Number of frames sent with bad CRC (for specific module in chassis).
TxBusTimeouts	UDINT	Number of timeouts on sent frames (for specific module in chassis).
TxRetryLimit	UDINT	Retry limit for sent frames (for specific module in chassis).

ControlLogix Chassis Diagnostics_A Assembly

- Instance = 32942
- Size = 444 Bytes

Table 87. Diagnostic Assembly Members

Member	Data Type	Description
ChassisSize	USINT	Size of the chassis in terms of number of slots and is programmed at time of manufacture into the rack's non-volatile storage.
Slot00	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot01	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot02	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot03	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot04	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot05	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot06	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot07	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot08	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot09	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.

ControlLogix Chassis Diagnostics_B Assembly

- Instance = 32943
- Size = 312 Bytes

Table 88. Diagnostic Assembly Members

Member	Data Type	Description
ChassisSize	USINT	Size of the rack in terms of number of slots and is programmed at time of manufacture into the rack's non-volatile storage.
Slot10	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot11	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot12	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot13	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot14	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot15	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.
Slot16	DIAGNOSTICS_CHASSIS_SLOTS_DATA	Diagnostics of a specific slot. Details can be found in the structure description.

Standard Network Diagnostic Assemblies

Standard network diagnostics includes four main diagnostic assemblies for Single Port controllers, Device Level Ring (DLR), Dual-IP configuration, and PRP (Parallel Redundancy Protocol).

- Single Port supports ControlLogix® 5580 controllers.
- DLR supports ControlLogix® 5590 controllers, CompactLogix® 5380 controllers, and 1756-EN4TR communication modules.
- Dual-IP supports ControlLogix® 5590 controllers and CompactLogix® 5380 controllers.
- PRP supports 1756-EN4TR communication modules.

IMPORTANT: This assembly includes six structures that are used to create user-defined data types that capture the information used in the main diagnostic assemblies. Create these UDTs before you create the main Standard Network Diagnostics UDTs.

The instance number is 210 for the main assemblies, and the device will return the assembly that matches what it is configured for (for example, DLR, PRP, Dual-IP).

Table 89. Structure of Standard Network Diagnostic Assemblies

Main Diagnostic Assemblies	StandardDiag_ConnMgr	StandardDiag_DLRSupervisor	StandardDiag_EthernetLink	StandardDiag_PRP	StandardDiag_TCP	StandardDiag_TimeSync
StandardNetworkDiagnostic_DLRSup	✓	✓	✓	—	✓	✓
StandardNetworkDiagnostic_DualIP	✓	—	✓	—	✓	✓

Table 89. Structure of Standard Network Diagnostic Assemblies (continued)

Main Diagnostic Assemblies	StandardDiag_ConnMgr	StandardDiag_DLRSupervisor	StandardDiag_EthernetLink	StandardDiag_PRP	StandardDiag_TCP	StandardDiag_TimeSync
StandardNetworkDiagnostic_L8	✓	—	✓	—	✓	✓
StandardNetworkDiagnostic_PRP	✓	—	✓	✓	✓	✓

Structures for the Standard Network Diagnostics User-defined Data Types

Use these structures to create user-defined data types that capture the information used in the main diagnostic assemblies. Create these UDTs before you create the main Standard Network Diagnostics Diagnostic Assemblies.

Structure for the StandardDiag_ConnMgr User-defined Data Type

Provides status on I/O and Explicit Messaging connections.

Table 90. StandardDiag_ConnMgr User-defined Data Type

Member	Data Type	Description
MissedIOpacketsCnt	UDINT	Cumulative count of missed IO packets.
NumIOConnection	UDINT	Number of IO connections established.
MessagesPerSecond	UDINT	Number of messages per second being processed.
IOPacketsPerSecond	UDINT	Number of IO packets per second being processed.
NumMessagingConnections	UDINT	Number of messaging connections established.
ConnectionTimeoutsCnt	UINT	Cumulative count of connection timeouts that have occurred.
CPU_Utilization	UINT	CPU utilization measured in tenths of percentage (i.e. 1000 = 100%).
IO_Utilization	UINT	IO capacity utilization measured in tenths of percentage (i.e. 1000 = 100%).
ConcurrentCommsBranchFail	BOOL	One or more concurrent communications branch is currently not transmitting/receiving data.
ConcurrentCommsConnFailCnt	UDINT	Cumulative count of concurrent communications failures.
ConcurrentCommsPacketsLostCnt	UDINT	Cumulative count of concurrent communication packets missed Read/Write.
Pad	UDINT	Reserved

Structure for the StandardDiag_DLRSupervisor User-defined Data Type

Provides status on the Device Level Ring.

Table 91. StandardDiag_DLRSupervisor User-defined Data Type

Member	Data Type	Description
Network_Status	SINT	0 = Normal; 1 = Ring Fault; 2 = Loop Detected; 3 = Partial Fault; 4 = Rapid Fault/Restore Read/Write.
Ring_Supervisor_Status	SINT	0 = Backup; 1 = Active; 2 = Non supervisor; 3 = non-DLR topology; 4 = Unsupported parameter.
Ring_Faults_Count	UINT	Cumulative count of ring faults.
Pad	SINT[4]	Reserved

Structure for StandardDiag_EthernetLink User-defined Data Type

Provides status on the Ethernet link.

Table 92. StandardDiag_EthernetLink User-defined Data Type

Member	Data Type	Description
LinkStatus	BOOL	Indicates whether or not the module is connected to an active network. 0 = inactive link; 1 = active link.
Duplex	BOOL	Indicates the duplex mode currently in use. 0 = half duplex; 1 = full duplex.
NegotiationStatus0	BOOL	Indicates the status of link auto-negotiation.
NegotiationStatus1	BOOL	Indicates the status of link auto-negotiation.
NegotiationStatus2	BOOL	Indicates the status of link auto-negotiation.
Pad	BOOL	Reserved
HardwareFault	BOOL	0 = no local hardware fault; 1 = local hardware fault.
InterfaceSpeed	UDINT	Interface speed currently in use (10, 100, 1000).
LinkDownCnt	UDINT	Link Down Counter. Counts the number of times a Link Down transition event was detected on this port.
EthernetErrors	UDINT	Sum of error counts from Interface Counters and Media Counters.

NegotiationStatus

The status is a 3-bit field, where NegotiationStatus0 is the least significant bit.

Bit	Auto-negotiation in progress.	Auto-negotiation and speed detection failed. Using default values for speed and duplex.	Auto negotiation failed but detected speed. Duplex set to default value	Successfully negotiated speed and duplex	Auto-negotiation not attempted. Forced speed and duplex
NegotiationStatus0	0	1	0	1	0
NegotiationStatus1	0	0	1	1	0
NegotiationStatus2	0	0	0	0	1

In this example, the controller tags of the destination element show that speed and duplex were successfully negotiated.

Dual_IP_Diags.EthernetPort_1.NegotiationStatus0	1	Decimal	BOOL
Dual_IP_Diags.EthernetPort_1.NegotiationStatus1	1	Decimal	BOOL
Dual_IP_Diags.EthernetPort_1.NegotiationStatus2	0	Decimal	BOOL

Structure for theStandardDiag_PRP User-defined Data Type

Provides status on the PRP ports.

Table 93. StandardDiag_PRP User-defined Data Type

Member	Data Type	Description
Warning_LAN_A	BOOL	A potential problem with the PRP port exists.
Warning_LAN_B	BOOL	A potential problem with the PRP port exists.
Pad	SINT[4]	Reserved

Structure for the StandardDiag_TCP User-defined Data Type

Provides status on the TCP/IP network interface.

Table 94. StandardDiag_TCP User-defined Data Type

Member	Data Type	Description
NonCIPMessagesPerSecond	UDINT	Non-CIP messages per second.
NumTCPConnections	UINT	Number of active TCP connections.

Structure for the StandardDiag_TimeSync User-defined Data Type

Provides status on time synchronization.

Table 95. StandardDiag_Time Sync User-defined Data Type

Member	Data Type	Description
IsSynchronized	BOOL	Local clock is synchronized with Time Transmitter.
OffsetFromTimeTransmitter	ULINT	Offset between local clock and Time Transmitter clock in nanoseconds.
GrandMasterID	SINT[8]	GrandMaster Clock Identity.

Main Standard Network Diagnostics Assemblies

Use the data types you created with the [Structures for the Standard Network Diagnostics User-defined Data Types on page 275](#) to create these diagnostic assemblies.

StandardNetworkDiagnostic_DLRSup

- Instance = 210
- Size = 120 Bytes

Table 96. StandardNetworkDiagnostic_DLRSup Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
DLR	StandardDiag_DLRSupervisor	Provides status on the Device Level Ring.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_DualIP

- Instance = 210
- Size = 120 Bytes

Table 97. StandardNetworkDiagnostic_DualIP Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCPPort_1	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TCPPort_2	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_L8

- Instance = 210
- Size = 96 Bytes

Table 98. StandardNetworkDiagnostic_L8 Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.

Table 98. StandardNetworkDiagnostic_L8 Diagnostic Assembly (continued)

Member	Data Type	Description
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

StandardNetworkDiagnostic_PRP

- Instance = 210
- Size = 120 Bytes

Table 99. StandardNetworkDiagnostic_PRP Diagnostic Assembly

Member	Data Type	Description
MemberListSignature	UDINT	Change in this value indicates that the members of this structure have changed.
ConnMgr	StandardDiag_ConnMgr	Provides status on I/O and Explicit Messaging connections.
EthernetPort_1	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
EthernetPort_2	StandardDiag_EthernetLink	Provides status on the Ethernet link on this port.
TCP	StandardDiag_TCP	Provides status on the TCP/IP network interface.
PRP	StandardDiag_PRP	Provides status on the PRP ports.
TimeSync	StandardDiag_TimeSync	Provides status on time synchronization.

Change Controller Project Type

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

Changing the project affects the following:

- Supported features
- Physical configuration of the project (safety partner and safety I/O)
- Controller properties
- Project components such as tasks, programs, routines, and tags
- Safety Add-On Instructions

When you change one controller type to another, the class of tags, routines, and programs remain unaltered. Any I/O devices that are no longer compatible with the target controller are deleted. If needed, the representation of the safety partner is updated to appear appropriately for the target controller.

Change from a Standard to a Safety Project

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

- The safety task is created only if the maximum number of downloadable tasks has not been reached. The safety task is initialized with its default values.



If your project already contains 32 tasks, and you try to change from standard to a safety, the project does not convert and stays as a standard project.

- Safety components are created (such as, safety task and safety program).
- The safety project defaults to safety level SIL 2/PLd.
- A time-based safety network number (SNN) is generated for the local chassis.
- A time-based safety network number (SNN) is also generated for the embedded EtherNet/IP™ port.
- Standard features that are not supported by the safety project are removed from the Controller Properties dialog box.

Change from a Safety to a Standard Project

Upon confirmation of a change from a safety project to a standard project, some components are changed, and others are deleted, as described below:

- The safety partner is deleted from the I/O chassis, if it existed.
- Safety I/O devices and their tags are deleted.
- The safety task, programs, and routines are changed to a standard task, programs, and routines.
- All safety tags, except safety consume tags, are changed to standard tags.
- Safety consume tags are deleted.
- Safety tag mappings are deleted.
- The safety network numbers (SNN) are deleted.
- Safety-lock and safety-unlock passwords are deleted.

- If the standard project supports features that were not available to the safety project, those new features are visible in the Controller Properties dialog box.



Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

If the safety project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the project type.

Safety Application Instructions

Safety application instructions are certified for use in SIL 2 or SIL 3 applications.



ATTENTION: Safety application instructions are the only instructions that can be used in the safety task for SIL 2 or SIL 3 applications.

For more information about using instructions, see the following:

- Logix 5000 Safety Application Instruction Set Reference Manual, publication [1756-RM095](#)
- Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#)

Safety Instructions

Mnemonic	Name	Description
CROUT	Configurable Redundant Output	Controls and monitors redundant outputs.
DCA	Dual Channel Input - Analog (integer version)	Monitors two analog values for deviation and range tolerance.
DCAF	Dual Channel Input - Analog (floating point version)	Monitors two analog values for deviation and range tolerance.
DCM	Dual Channel Input - Monitor	Monitors dual-input safety devices.
DCS	Dual Channel Input - Stop	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch.
DCSRT	Dual Channel Input - Start	Energizes dual-input safety devices whose main function is to start a machine safely, for example an enable pendant.
DCST	Dual Channel Input - Stop With Test	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device.
DCSTL	Dual Channel Input - Stop With Test and Lock	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device. It can monitor a feedback

Mnemonic	Name	Description
		signal from a safety device and issue a lock request to a safety device.
DCSTM	Dual Channel Input - Stop With Test and Mute	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device and the ability to mute the safety device.
FSBM	Four Sensor Bi-directional Muting	Automatically disables the protective function of a light curtain temporarily, by using four sensors that are arranged sequentially before and after the sensing field of the light curtain.
SMAT	Safety Mat	Indicates whether the safety mat is occupied.
THRSe	Two-Hand Run Station - Enhanced	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control one output. Features configurable channel-to-channel discrepancy time and enhanced capability for bypassing a two-hand run station.
TSAM	Two Sensor Asymmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged asymmetrically.
TSSM	Two Sensor Symmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged symmetrically.

Metal Form Instructions

AVC	Name	Description
AVC	Auxiliary Valve Control	Controls an auxiliary valve that is used with a main valve.

AVC	Name	Description
CBIM	Clutch Brake Inch Mode	Used for press applications where minor slide adjustments are required, such as press setup.
CBCM	Clutch Brake Continuous Mode	Used for press applications where continuous operation is desired.
CBSSM	Clutch Brake Single Stroke Mode	Used in single-cycle press applications.
CPM	Crankshaft Position Monitor	Used to determine the slide position of the press.
CSM	Camshaft Monitor	Monitors motion for the start, stop, and run operations of a camshaft.
EPMS	Eight-position Mode Selector	Monitors eight safety inputs to control one of the eight outputs that correspond to the active input.
MMVC	Maintenance Manual Valve Control	Used to drive a valve manually during maintenance operations.
MVC	Main Valve Control	Controls and monitors a main valve.

Ladder Diagram Safety Instructions

Routines in the safety task can use the following types of ladder diagram safety instructions.

When instructions that result in values with decimal place are used with REAL or LREAL operands, Rockwell Automation has verified the precision to 6 decimal places.

Process

Mnemonic	Name	Description	Logix Designer Application
FGEN	Function Generator	Converts an input based on a piece-wise linear function.	Version 38 or later

Advanced Math

Rockwell Automation has not done independent mathematical analysis of the numerical algorithms used in any of the following advanced math instructions. If you require a specific degree of accuracy, you must functionally test this instruction over your expected input domain.

Mnemonic	Name	Description	Logix Designer Application
EXPT	X to the Power of Y	Returns the value of X to the power of Y.	Version 36 or later
XPY	X to the Power of Y	Returns the value of X to the power of Y.	Version 35 or earlier
LN	Natural Log	Compute the natural log of a number.	Version 36 or later
LOG	Log Base 10	Compute the log base 10 of a number.	All versions

Array (File)

Mnemonic	Name	Description	Logix Designer Application
AVE	File Average	Calculate the mean/average over a set of values.	All versions
COP	Copy File	Copy binary data from one tag to another (no type conversion). When you use the COP instruction in a safety routine, you must verify that the length is a constant and that the source and destination length are the same.	All versions
FAL	File Arithmetic and Logic	Perform copy, arithmetic, logic, and function operations on data that is stored in an array.	All versions
FLL	File Fill	Fill the elements of an array with the source value, while leaving the source value unchanged.	All versions
FSC	File Search and Compare	Compare the values in an array, element by element.	All versions
SIZE	Size in Elements	Find the size of a dimension of an array.	All versions

Mnemonic	Name	Description	Logix Designer Application
STD	File Standard Deviation	Calculate the standard deviation over a set of values.	All versions
BSL	Bit Shift Left	Shifts the specified number of bits to the left.	All versions
BSR	Bit Shift Right	Shifts the specified number of bits to the right.	All versions
FFL	FIFO Load	Store a value into an array by using first-in/first-out semantics.	All versions
FFU	FIFO Unload	Retrieve a value from an array by using last-in/first-out semantics.	All versions
LFL	LIFO Load	Store a value into an array by using last-in/first-out semantics.	All versions
LFU	LIFO Unload	Retrieve a value from an array by using last-in/first-out semantics.	All versions

Bit

Mnemonic	Name	Description	Logix Designer Application
ONS	One Shot	Allows an event to occur one time.	All versions
OSR	One Shot Falling	Sets an output bit for one scan on the true-to-false (falling) edge of rung state.	All versions
OSF	One Shot Rising	Sets an output bit for one scan on the false-to-true (rising) edge of rung state.	All versions
OTE	Output Energize	Controls a bit (it performs both Set and Clear operations based on rung state).	All versions
OTL	Output Latch	Set a bit (retentive).	All versions

Mnemonic	Name	Description	Logix Designer Application
OTU	Output Unlatch	Clear bit (retentive).	All versions
XIC	Examine if Closed	Examines the data bit to set or clear the rung condition.	All versions
XIO	Examine if Open	Examines the data bit to set or clear the rung condition.	All versions

Time/Counter

Mnemonic	Name	Description	Logix Designer Application
CTD	Count Down	Count down.	All versions
CTU	Count Up	Count up.	All versions
RES	Reset	Reset a timer or counter.	All versions
RTO	Retentive Timer On	Accumulate time.	All versions
TOF	Off-delay Timer	Time how long a timer is disabled.	All versions
TON	On-delay Timer	Time how long a timer is enabled.	All versions

Compare

Mnemonic	Name	Description	Logix Designer Application
EQ	Equal To	Test whether two values are equal.	Version 36 or later
EQU	Equal To	Test whether two values are equal.	Version 35 or earlier
CMP	Compare	Perform a comparison on the arithmetic operations that you specify in the expression.	All versions
GE	Greater Than Or Equal To	Test whether one value is greater than or equal to a second value.	Version 36 or later

Mnemonic	Name	Description	Logix Designer Application
GEQ	Greater Than Or Equal To	Test whether one value is greater than or equal to a second value.	Version 35 or earlier
GT	Greater Than	Test whether one value is greater than a second value.	Version 36 or later
GRT	Greater Than	Test whether one value is greater than a second value.	Version 35 or earlier
IsINF	Is Infinity	Check if floating point value is +/- infinity.	All versions
IsNaN	Is Not a Number	Check if floating point value is Not-a-Number.	All versions
LE	Less Than or Equal To	Test whether one value is less than or equal to a second value.	Version 36 or later
LEQ	Less Than or Equal To	Test whether one value is less than or equal to a second value.	Version 35 or earlier
LT	Less Than	Test whether one value is less than a second value.	Version 36 or later
LES	Less Than	Test whether one value is less than a second value.	Version 35 or earlier
LIMIT	Limit	Test whether a value falls within a specified range.	Version 36 or later
LIM	Limit	Test whether a value falls within a specified range.	Version 35 or earlier
MEQ	Mask Equal To	Pass source and compare values through a mask and test whether they are equal.	All versions
NE	Not Equal	Test whether one value is not equal to a second value.	Version 36 or later
NEQ	Not Equal	Test whether one value is not equal to a second value.	Version 35 or earlier

Move/Logical

Mnemonic	Name	Description	Logix Designer Application
AND	Bitwise AND	Perform bitwise AND operation.	All versions
CLR	Clear	Clear a value.	All versions
MOVE	Move	Copy a value.	Version 36 or later
MOV	Move	Copy a value.	Version 35 or earlier
MVM	Masked Move	Copy a specific part of an integer.	All versions
NOT	Bitwise Not	Perform bitwise NOT operation.	All versions
OR	Bitwise Or	Perform bitwise OR operation.	All versions
SWPB	Swap Byte	Rearrange the bytes of a value.	All versions
XOR	Bitwise Exclusive Or	Perform bitwise exclusive OR operation.	All versions

Program Control

Mnemonic	Name	Description	Logix Designer Application
AFI	Always False Instruction	Forces a rung to false (rung continues to execute).	All versions
EVENT	Trigger Event Task	Triggers one execution of an event task. The event instruction triggers a scan of the standard task.	All versions
JMP	Jump To Label	Scan of logic jumps to a labeled location within the same routine.	All versions
JSR	Jump to Subroutine	Jump to a separate routine.	All versions
LBL	Label	Identifies a target location for a JMP instruction.	All versions

Mnemonic	Name	Description	Logix Designer Application
MCR	Master Control Reset	Forces every rung in a section of logic to execute in the False state.	All versions
NOP	No Operation	Insert a placeholder in the logic.	All versions
RET	Return	Return the results of a subroutine.	All versions
SBR	Subroutine	Accept data that is passed to a subroutine by the JSR instruction.	All versions
TND	Temporary End	Mark a temporary end that halts routine execution.	All versions

Compute/Math

Rockwell Automation has done no independent mathematical analysis of the numerical algorithms used in the SQR or SQR instructions. If you require a specific degree of accuracy, you must functionally test this instruction over your expected input domain.

Mnemonic	Name	Description	Logix Designer Application
ABS	Absolute Value	Take the absolute value of a value.	All versions
ADD	Add	Add two values.	All versions
CPT	Compute	Perform the arithmetic operation that is defined in the expression.	All versions
DIV	Divide	Divide two values.	All versions
MOD	Modulo	Determine the remainder after one value is divided by a second value.	All versions
MUL	Multiply	Multiply two values.	All versions
NEG	Negate	Take the opposite sign of a value.	All versions
SQRT	Square Root	Calculate the square root of a value.	Version 36 or later
SQR	Square Root	Calculate the square root of a value.	Version 35 or earlier

Mnemonic	Name	Description	Logix Designer Application
SUB	Subtract	Subtract two values.	All versions

Trigonometric

Rockwell Automation has not done independent mathematical analysis of the numerical algorithms in any of the following trigonometric instructions. If you require a specific degree of accuracy, you must functionally test this instruction over your expected input domain.

Mnemonic	Name	Description	Logix Designer Application
ACOS	Arc Cosine	Compute the arc-cosine of a number.	Version 36 or later
ACS	Arc Cosine	Compute the arc-cosine of a number.	Version 35 or earlier
ASIN	Arc Sine	Compute the arc-sine of a number.	Version 36 or later
ASN	Arc Sine	Compute the arc-sine of a number.	Version 35 or earlier
ATAN	Arc Tangent	Compute the arc tangent in radians of y/x based on the sign of a value to determine the correct quadrant.	Version 36 or later
ATN	Arc Tangent	Compute the arc tangent in radians of y/x based on the sign of a value to determine the correct quadrant.	Version 35 or earlier
ATAN2	Arc Tangent 2	Compute the arc tangent in radians of y/x based on the signs of both values to determine the correct quadrant.	All versions
COS	Cosine	Compute the cosine of a number.	All versions
SIN	Sine	Compute the sin of a number.	All versions
TAN	Tangent	Compute the tangent of a number.	All versions

I/O

For special considerations when using the GSV and SSV instructions, see the controller user manual.

Mnemonic	Name	Description	Logix Designer Application
GSV	Get System Value	Get controller status information.	All versions
SSV	Set System Value	Set controller status information.	All versions

Math Conversion

Mnemonic	Name	Description	Logix Designer Application
DEG	Degrees	Convert radians into degrees.	All versions
BCD_TO	Convert to Integer	Convert the BCD value to an integer value.	Version 36 or later
FRD	Convert to Integer	Convert the BCD value to an integer value.	Version 35 or earlier
RAD	Radian	Convert degrees into radians.	All versions
TO_BCD	Convert to BCD	Convert the integer value to a BCD value.	Version 36 or later
TOD	Convert to BCD	Convert the integer value to a BCD value.	Version 35 or earlier
TRUNC	Truncate	Remove the fractional part of a value.	Version 36 or later
TRN	Truncate	Remove the fractional part of a value.	Version 35 or earlier

Drive Safety Instructions

Motion safety instructions are available when using a controller and safe speed or position inputs with the Studio 5000 Logix Designer® application.

Motion safety instructions are available when using a ControlLogix® 5590 controller, GuardLogix® 5580 controller, or Compact GuardLogix® 5380 controller and safe speed or position inputs with the Studio 5000 Logix Designer® application. ControlLogix® 5590 controllers support version 38 or later. GuardLogix® 5580 controllers and Compact GuardLogix® 5380 controllers support version 31 or later.

IMPORTANT: If you use motion direct commands, see the user manual for the drive for information on how to use this feature in safety applications:

- Kinetix 5500 Servo Drives User Manual, publication [2198-UM001](#)
- Kinetix 5700 Servo Drives User Manual, publication [2198-UM002](#)
- PowerFlex® 527 Adjustable Frequency AC Drive User Manual, publication [520-UM002](#)
- PowerFlex 755/755T Integrated Safety – Safe Torque Off Option Module User Manual, publication [750-UM004](#)
- PowerFlex 755/755T Integrated Safety Functions Option Module User Manual, publication [750-UM005](#)

Mnemonic	Name	Description
SBC	Safe Brake Control	The Safe Brake Control (SBC) instruction: • Controls safety outputs that actuate a brake. • Sets timing between brake and Torque Off Request outputs. • Monitors brake feedback and I/O status.
SDI	Safe Direction	The Safe Direction instruction monitors position of a motor or axis to detect movement of more than a defined amount in the unintended direction.
SFX	Safe Feedback Scaling	The Safety Feedback Interface instruction converts motor velocity and position feedback from a drive module into user scaling units. It also defines an absolute reference position.
SLP	Safely-limited Position	The Safely-limited Position instruction monitors the position of a motor or axis to verify that the position does not deviate above or below defined limits.
SLS	Safely-limited Speed	The Safely-limited Speed instruction monitors the speed of an axis and sets the SLS Limit output if the speed exceeds the Active Limit input value for the instruction.
SOS	Safe Operating Stop	The Safe Operating Stop instruction monitors the speed or position of a motor or axis to verify that the deviation from standstill speed or position is not more than a defined amount.

Mnemonic	Name	Description
SS1	Safe Stop 1	The Safe Stop 1 instruction monitors the deceleration of an axis according to the specified velocity ramp to zero speed and controls its output (O1) to initiate Safe Torque Off (STO).
SS2	Safe Stop 2	The Safe Stop 2 instruction initiates and monitors the motor deceleration within set limits to verify that the motor is brought to an operational stop. Once stopped, SS2 continues to monitor the operational stop of the motor.

Safety Reaction Times

The input reaction time is the time from when the signal changes on an input terminal to when safety data is sent to the controller.

The output reaction time is the time from when safety data is received from the controller to when the output terminal changes state.

For information on how to determine the input and output reaction times, see the product documentation for your specific safety I/O device.

Connection Reaction Time Limit

The Connection Reaction Time Limit (CRTL) is the maximum age of safety packets on the associated connection. If the age of the data that is used by the consuming device exceeds the CRTL, a connection fault occurs.

The CRTL is defined by the values in the following table.

Table 100. Connection Reaction Time Limit Values

Value	Default	Description
Requested packet interval (RPI)	10 ms (input RPI)	The RPI determines how often the input and output packets are placed on the network.
Timeout multiplier	2	The timeout multiplier determines the number of retries before a timeout occurs. IMPORTANT: For any safety connection, do not set the timeout multiplier lower than 2. If the timeout multiplier is lower than 2, you risk the controller not meeting time coordination requirements during a loss of redundancy.
Network delay multiplier	200%	The network delay multiplier accounts for known delays on the network. When known delays occur, timeouts can be avoided with this parameter.

If you adjust these values, then you can adjust the CRTL. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state (Off).

IMPORTANT: The default values generate an input connection reaction time limit of 40 ms. If no edits are made to the defaults, verify this connection reaction time limit is used in the safety reaction time calculations.

IMPORTANT: For applications with safety I/O, the default connection reaction time limit can result in connection loss to the safety I/O modules. In some cases, it is necessary to increase the values from their defaults. Make sure that you use the new connection reaction time limit in the safety reaction time calculations.

The following equations determine the CRTL:

Input Connection Reaction Time Limit = Input RPI x [Timeout Multiplier + Network Delay Multiplier]

Output Connection Reaction Time Limit = Safety Task Period x [Timeout Multiplier + Network Delay Multiplier - 1]

The CTRL is shown on the Safety view of the Module Properties dialog box.

Figure 96. Connection Reaction Time Limit

INFORMATION Overview Device Information CONFIGURATION Connection Safety Points	Safety						
		Connection Type	Requested Packet Interval (RPI)	Connection Reaction Time Limit	Max Observed Network Delay		
					Time		Action
		Safety Input	10 ms	40.1 ms	1.7 ms		Reset ←
		Safety Output	20 ms	60 ms	3.7 ms		Reset ←

Specify the Requested Packet Interval (RPI)

The RPI specifies the period that data updates over a connection. For example, an input module produces data at the RPI that you assign.

For safety input connections, you can set the RPI on the Safety view of the Module Properties dialog box. The RPI is entered in 1 ms increments.

The CTRL is adjusted immediately when you change the RPI value.

Figure 97. Requested Packet Interval

INFORMATION Overview Device Information CONFIGURATION Connection Safety Points	Safety						
		Connection Type	Requested Packet Interval (RPI)	Connection Reaction Time Limit	Max Observed Network Delay		
					Time		Action
		Safety Input	10 ms	40.1 ms	1.7 ms		Reset ←
		Safety Output	20 ms	60 ms	3.7 ms		Reset ←

For safety output connections, the RPI is fixed at the safety task period. If the corresponding CTRL is not satisfactory, you can adjust the safety task period on the Safety Task Properties dialog box.

For typical applications, the default CTRL for input connections of 4 x RPI and the default CTRL for output connections of 3 x RPI is usually sufficient. For more complex requirements, use the Advanced button to modify the CTRL parameters.

View the Maximum Observed Network Delay

The maximum observed network delay is shown on the Safety view of the Module Properties dialog box. When online, click Reset to reset the maximum observed network delay.

Figure 98. Reset the Max Observed Network Delay

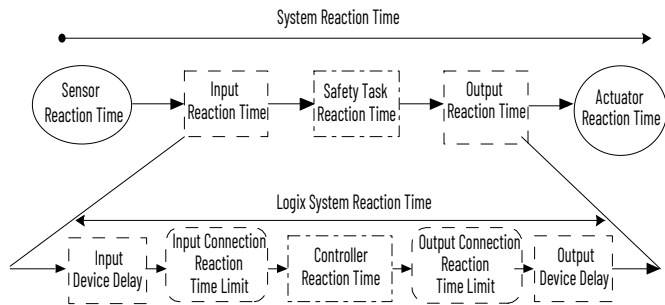
INFORMATION Overview Device Information CONFIGURATION Connection Safety Points	Safety					
		Connection Type	Requested Packet Interval (RPI)	Connection Reaction Time Limit	Max Observed Network Delay	
					Time	Action
		Safety Input	10 ms	40.1 ms	1.7 ms	Reset
		Safety Output	20 ms	60 ms	3.7 ms	Reset

System Reaction Time

To determine the system reaction time of any control chain, add the reaction times of all the components of the safety chain:

System Reaction Time = Sensor Reaction Time + Logix System Reaction Time + Actuator Reaction Time

Figure 99. System Reaction Time



Safety Task Reaction Time

The safety task reaction time is the worst-case delay from any input change that is presented to the controller until the output producer sets the processed output. To determine the safety task reaction time, use the following equation:

Safety task reaction time = (safety task period + safety task watchdog) × 1.01

The multiplier is for potential clock drift.

Safety Task Period and Safety Task Watchdog

The safety task period is the interval at which the safety task executes.

The safety task watchdog time is the maximum permissible time for safety task processing. If the time to process a safety task exceeds the safety task watchdog time, a nonrecoverable safety fault occurs in the controller, which results in a transition to the safe state (Off).

You define the safety task watchdog time, which must be less than or equal to the safety task period. You can set the safety task watchdog time in the safety task properties. This value can be modified online, regardless of controller mode, but it cannot be changed when the controller is safety-locked or once a safety signature is created.

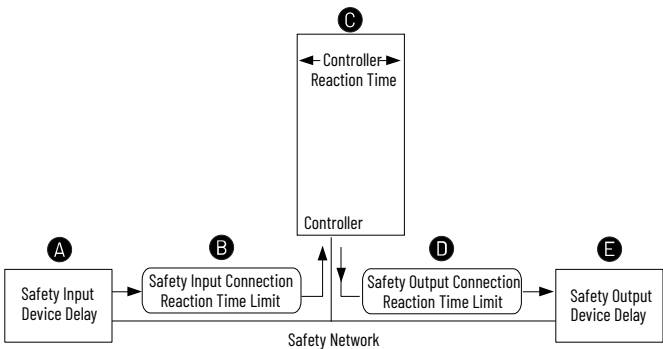
Logix System Reaction Time

The following sections provide information on how to calculate the Logix system reaction time.

Simple Input-Logic-Output Chain

This section describes the Logix system reaction time for any simple input-logic-output chain.

Figure 100. Worst Case Reaction Time



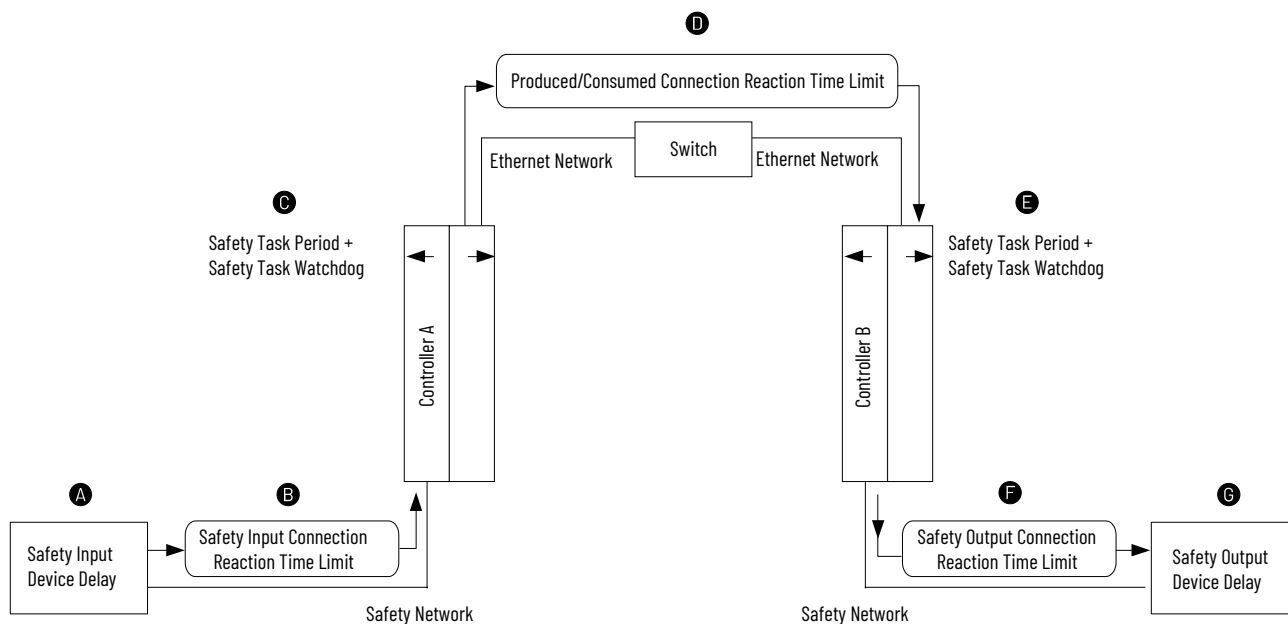
The Logix system reaction time for any simple input to logic to output chain consists of the following components.

Item	Description
A	Safety input device reaction time plus input delay time, if applicable.
B	Safety input connection reaction time limit. Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety input device connection RPI.
C	Controller reaction time. See Safety Task Reaction Time on page 297 .
D	Safety output connection reaction time limit. Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety task period.
E	Safety output device reaction time.

Logic Chain Using Produced/Consumed Safety Tags

This section describes the Logix system reaction time for any input to controller A logic to controller B logic to output chain.

Figure 101. Reaction Time with Produced/Consumed Safety Tags



The Logix system reaction time for any input to controller A logic to controller B logic to output chain consists of the following components.

Item	Description
A	Safety input device reaction time plus input delay time, if applicable
B	Safety input connection reaction time limit
C	Safety task period plus safety task watchdog time for controller A
D	Produced/consumed safety connection reaction time limit
E	Safety task period plus safety task watchdog time for controller B
F	Safety output connection reaction time limit
G	Safety output device reaction time

Factors That Affect Logix Reaction-time Components

A number of factors can influence the Logix system reaction time components.

Network traffic and EMC create a lower limit for the values that you can successfully use for the timeout multiplier and network delay multiplier.

The instructions in your safety task and any higher priority tasks in the controller create a lower limit for the values that you can successfully use for Safety Task Period and Safety Task Watchdog.

Table 101. System Reaction Time Components

Reaction Time Component	Factors
Input device delay	- Input device reaction time - On-Off and Off-On delay settings for each input channel
Safety input connection reaction time limit	- Input device settings: - Requested packet interval (RPI) - Timeout multiplier - Network delay multiplier - The amount of network communication traffic. - The EMC environment of the system
Safety task period and safety task watchdog	- Safety task period setting - Safety task watchdog setting - The number and execution time of instructions in the safety task The instructions in your safety task create a lower limit for the values that you can successfully use for the safety task period and safety task watchdog.
Output connection reaction time limit	- Safety task period setting - Output device settings: - Timeout multiplier - Network delay multiplier - The amount of network communication traffic - The EMC environment of the system
Output module delay	Output module reaction time

Configure the Safety Input Module Delay Time

To configure input module delay time in the Logix Designer application, follow these steps.

1. In the configuration tree, right-click the safety input module and select Properties.
2. In the navigation pane, select Points.
3. Adjust the input delay time as required for your application.

Figure 102. Input Delay Time

Module Properties: Rack1:1 (5094-IB16S 1.001) ×

5094-IB16S, R1_Slot1
Parent: Rack1
Slot: 1
Controller connection: Offline

INFORMATION

Overview

Device Information

CONFIGURATION

Connection

Safety

Points

Points

Input Points						
Point	Point Mode	Test Source	Input Delay Time		Diagnostics	
			Off → On	On → Off		
00	Safety	None	5 ms	5 ms		
01	Safety	None	0 ms	0 ms		
02	Not Used	None	0 ms	0 ms		
03	Not Used	None	0 ms	0 ms		
04	Not Used	None	0 ms	0 ms		
05	Not Used	None	0 ms	0 ms		
06	Not Used	None	0 ms	0 ms		

Configure the Input and Output Safety Connection Reaction Time Limits

To configure connection reaction time limit settings, follow these steps.

- 1. In the configuration tree, right-click your safety I/O module and select Properties.
- 2. In navigation pane, select Safety.
- 3. On the Safety view, click Advanced.

Module Properties: Rack1:1 (5094-IB16S 1.001) ×

5094-IB16S, R1_Slot1
Parent: Rack1
Slot: 1
Controller connection: Offline

INFORMATION

Overview

Device Information

CONFIGURATION

Connection

Safety

Points

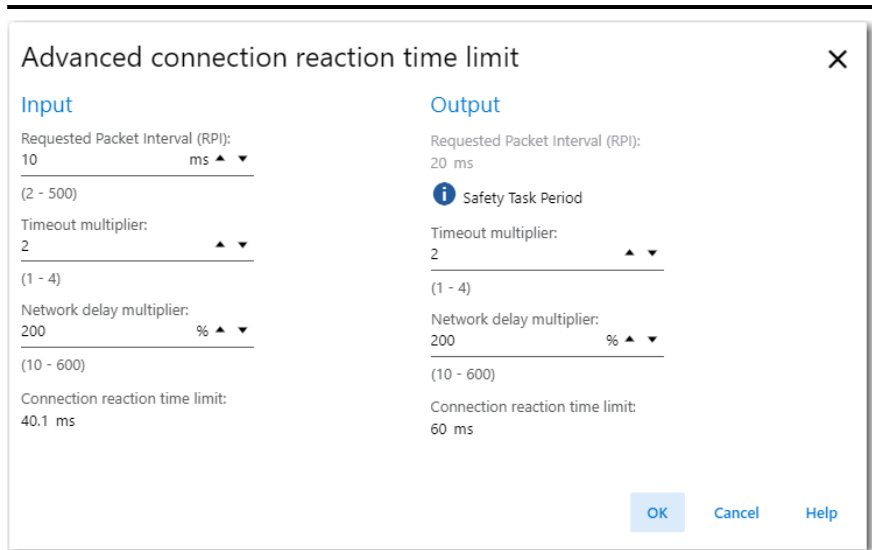
Safety

Connection Type	Requested Packet Interval (RPI)	Connection Reaction Time Limit	Max Observed Network Delay		Action
			Time		
Safety Input	10 ms	40.1 ms			Reset
Safety Output	20 ms	60 ms			Reset

Advanced...

- 4. On the Advanced Connection Reaction Time Limit dialog box, configure the parameters and click OK.

IMPORTANT: The values you define for the timeout multiplier and the network delay multiplier provide resilience for variations in network reliability and performance. Use caution when reducing the values as this increases the likelihood of false trips.



The dialog box is titled "Advanced connection reaction time limit" and has a close button (X) in the top right corner. It is divided into two main sections: "Input" on the left and "Output" on the right. Both sections have a blue header. The "Input" section contains: "Requested Packet Interval (RPI):" with a value of 10 ms and a range of (2 - 500); "Timeout multiplier:" with a value of 2 and a range of (1 - 4); "Network delay multiplier:" with a value of 200 % and a range of (10 - 600); and "Connection reaction time limit:" with a value of 40.1 ms. The "Output" section contains: "Requested Packet Interval (RPI):" with a value of 20 ms; an information icon (i) followed by "Safety Task Period"; "Timeout multiplier:" with a value of 2 and a range of (1 - 4); "Network delay multiplier:" with a value of 200 % and a range of (10 - 600); and "Connection reaction time limit:" with a value of 60 ms. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

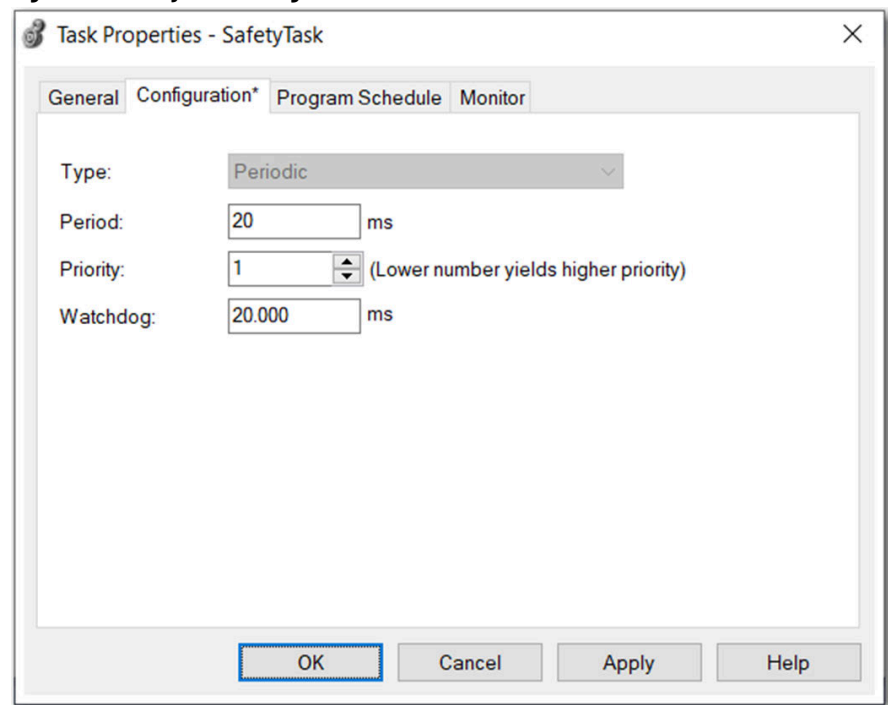
Parameter	Input Value	Input Range	Output Value	Output Range
Requested Packet Interval (RPI)	10 ms	(2 - 500)	20 ms	-
Timeout multiplier	2	(1 - 4)	2	(1 - 4)
Network delay multiplier	200 %	(10 - 600)	200 %	(10 - 600)
Connection reaction time limit	40.1 ms	-	60 ms	-

Configure the Safety Task Period and Watchdog

The safety task is a periodic timed task.

To configure the safety task period and watchdog, follow these steps.

1. In the configuration tree, right-click the safety task.
2. On the Task Properties dialog box, select the Configuration tab.
3. Configure the parameters as described in [Safety Task on page 177](#).

Figure 103. Safety Task Configuration

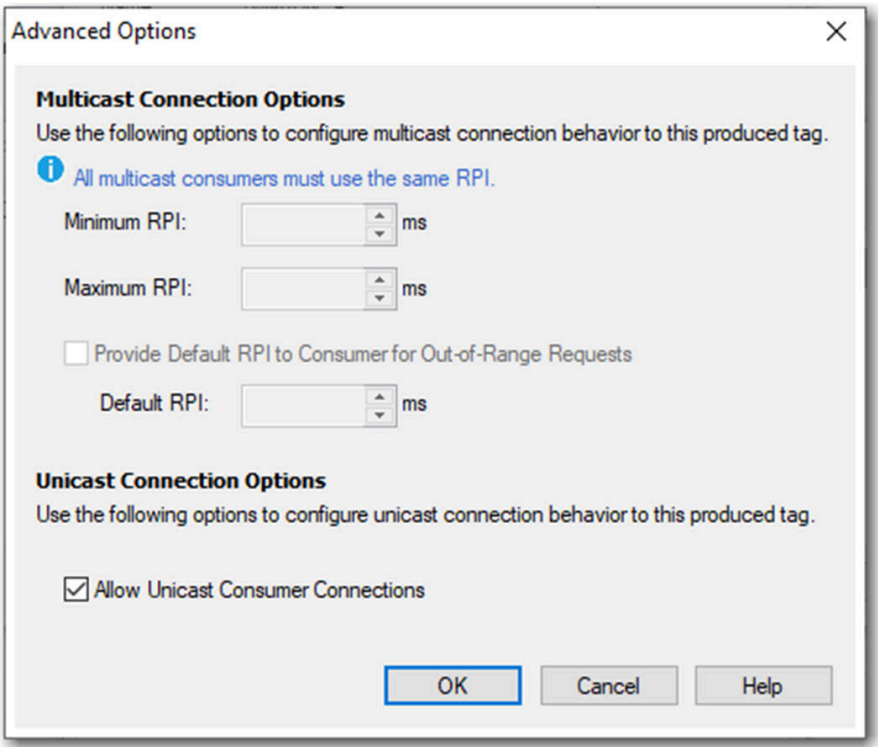
The priority of the safety task is not a safety concern, as the safety task watchdog monitors if a higher priority task interrupts the task. However, a higher priority safety task provides more consistent safety task performance. Safety Task priority = 1 is recommended.

Access Produced/Consumed Tag Data

To access safety tag connection data, follow these steps.

1. In the configuration tree, right-click Controller Tags and select Edit Tags.
2. In the Tag Editor, right-click the name of the tag and select Edit Properties.
3. Click Connection.
4. On the Safety tab, click Advanced.

Figure 104. Advanced Options Dialog Box



Checklists for Safety Applications

Checklists for safety applications are required to plan, program, and start a safety application. Use the checklists as planning guides and during project validation testing. When you use the checklists as planning guides, they can be saved as a record of the plan.

The checklists provide a sample of safety considerations and are not intended to be a complete list of items to verify. Your particular safety application can have additional safety requirements.



Make copies of the checklists to keep for future use.

Checklist for the Controller System

✓	System Requirements
	Are you using only the certified components for your SIL level, with the corresponding firmware release, as listed at https://rok.auto/certifications ?
	Have you calculated the safety response time of the system for each safety function?
	Does the response time of the system include both the user-defined safety-task program watchdog (software watchdog) time and the safety task rate/period?
	Is the system response time in proper relation to the process safety time?
	Have probability (PFD/PFH) values been calculated for each safety function?
	Have you performed all appropriate project validation tests?
	If necessary, have you created a prescan routine to initialize safety critical data?
	Have you determined how your system can handle faults?
	Does each network in the safety system have a unique safety network number?
	Is each safety device configured with the correct safety network number?
	Have you generated a safety signature?
	Have you uploaded and recorded the safety signature for future comparison?
	After a download, have you verified that the safety signature in the controller matches the recorded safety signature?
	Do you have an alternate mechanism in place to preserve the safety integrity of the system when making online edits?

✓	System Requirements
	Have you considered the checklists for using SIL inputs and outputs?

Checklist for Safety Inputs

For programming or startup, an individual checklist can be completed for every safety input in the system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

✓	Input Device Requirements
	Have you followed installation instructions and precautions to conform to applicable safety standards?
	Have you performed project validation tests on the system and devices?
	Are control, diagnostics, and alarm functions performed in sequence in application logic?
	Have you uploaded and compared the configuration of each device to the configuration sent by the configuration tool?
	Are devices wired in compliance with the target standard and required safety level?
	Have you verified that the electrical specifications of the sensor and input are compatible?

Checklist for Safety Outputs

For programming or startup, an individual requirement checklist must be completed for every safety output in the system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

✓	Output Device Requirements
	Have you followed installation instructions and precautions to conform to applicable safety standards?
	Have you performed project validation tests on the system and devices?
	Have you uploaded and compared the configuration of each device to the configuration sent by the configuration tool?
	Have you verified that test outputs are not used as safety outputs?
	Are devices wired in compliance with the target standard and required safety level?

✓	Output Device Requirements
	Have you verified that the electrical specifications of the output and the actuator are compatible?

Checklist to Develop a Safety Application Program

Use the following checklist to help maintain safety when you create or modify a safety application program.

✓	System Requirements
	Does your controller support the version of the Studio 5000 Logix Designer® application used to create the safety application program?
	Were the programming guidelines followed during the creation of the safety application program?
	Does the safety application program contain only a ladder diagram?
	Does the safety application program contain only safety instructions?
	Does the safety application program clearly differentiate between safety and standard tags?
	Are only safety tags used for safety routines?
	Have you verified that safety routines do not attempt to read from or write to standard tags?
	Have you verified that no safety tags are aliased to standard tags and vice versa?
	Is each safety output tag correctly configured and connected to a physical output channel?
	Have you verified that all mapped tags have been conditioned in safety application logic?
	Have you defined the process parameters that the fault routines monitor?
	Have you sealed any safety Add-On Instructions with an instruction signature and recorded the safety instruction signature? Optional for one time use Add-On Instructions. Required Add-On Instructions are reused on different applications.
	Did you measure potential alarm bursts during system commissioning and change the project if measured scan times are not acceptable?
	Has an independent safety reviewer reviewed the program, if necessary?
	Has the review been documented and signed?

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)



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

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

Allen-Bradley®, ArmorBlock®, Compact 5000® I/O, CompactLogix®, ControlBus™, ControlFLASH™, ControlFLASH Plus®, ControlLogix®, ControlLogix-XT™, DH+™, expanding human possibility®, FactoryTalk®, FLEX 5000®, GuardLogix®, Kinetix®, Logix 5000®, On-Machine™, PanelConnect™, PanelView™, PlantPAx®, PLC-2®, PLC-3®, PLC-5®, PointMax®, PowerFlex®, Rockwell Automation®, SLC™, Stratix®, Studio 5000®, Studio 5000 Logix Designer®, and SynchLink™ are trademarks of Rockwell Automation, Inc.

CIP™, CIP Safety™, CIP Security™, ControlNet®, DeviceNet®, and EtherNet/IP™ is a trademark of ODVA, Inc.

Windows® is a trademark of Microsoft Corporation.

microSD™ is a trademark of SD-3C.

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

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

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

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