



This manual links to Knowledgebase Article [Logix 5000 Controller Fault Codes](#) for fault codes; download the spreadsheets now for offline access.



ControlLogix 5580 and GuardLogix 5580 Controllers

Bulletin 1756



Allen-Bradley

by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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



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



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

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

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).

	Preface	11
	Catalog Numbers	11
	Summary of Changes	11
	Overview	11
	Additional Resources	12
	 Chapter 1	
ControlLogix and GuardLogix Systems	Minimum Requirements	15
	ControlLogix Controllers	16
	ControlLogix No Stored Energy (NSE) Controllers	16
	ControlLogix-XT Controllers	16
	Process Controllers	17
	Conformal Coated Products	17
	ControlLogix Redundant Controllers	17
	ControlLogix System	18
	Standalone Controller and I/O	18
	Multiple Controllers in One Chassis	19
	Multiple Devices Connected via Multiple Networks	20
	GuardLogix System	21
	Design the System	24
	CIP Security	24
	Secure Controller Systems	25
	ControlLogix 5580 Controller Features	25
	GuardLogix 5580 Controller Features	26
Features Supported By GuardLogix 5580 Controllers Via t he Safety Task	27	
	 Chapter 2	
Safety Concept of GuardLogix Controllers	Functional Safety Capability	29
	Safety Network Number	30
	Safety Signature	30
	Distinguish between Standard and Safety Components	31
	Controller Data-flow Capabilities	32
	Safety Terminology	33
	 Chapter 3	
Communication Networks	Networks Available	35
	EtherNet/IP Network Communication	37
	EtherNet/IP Link Speeds	37
	EtherNet/IP Communication Modules	40
	Double Data Rate (DDR) Backplane Communication for ControlLogix Controllers	40
	ControlNet Network Communication	41
	GuardLogix ControlNet Example	42
ControlNet Modules	43	

DeviceNet Network Communication..... 44
 DeviceNet Bridge Module and Linking Devices 45
 Connections Over DeviceNet Networks 45
 Data Highway Plus (DH+) Network Communication 45
 Communicate Over a DH+ Network 46
 Universal Remote I/O (RIO) Communication 47
 Communicate Over a Universal Remote I/O Network 48
 Foundation Fieldbus Communication 49
 HART Communication 50

Chapter 4

Connect to a Controller

Set the IP Address..... 51
 Requirements 52
 Other Methods to Set the IP Address 52
 Duplicate IP Address Detection 52
 Duplicate IP Address Resolution..... 53
 DNS Addressing 53
 Update Controller Firmware..... 55
 Firmware Upgrade Guidelines for Safety Controllers 55
 Determine Required Controller Firmware..... 56
 Obtain Controller Firmware 57
 Use ControlFLASH Plus or ControlFLASH Software to
 Update Firmware..... 57
 Use AutoFlash to Update Firmware..... 58

Chapter 5

Start Using the Controller

Create a Logix Designer Application Project..... 61
 Additional Configuration for a GuardLogix Controller..... 62
 Set the Safety Level for a GuardLogix Controller 62
 Passwords for Safety-locking and Unlocking 63
 Protect the Safety Signature in Run Mode 64
 Assign the Safety Network Number (SNN)..... 65
 Copy and Paste a Safety Controller Safety Network Number.. 69
 Go Online with the Controller 71
 Use RSWho..... 71
 Use a Recent Communication Path 72
 Additional Considerations for Going Online with a GuardLogix
 Controller 73
 Match Project to Controller..... 73
 Firmware Revision Matching 74
 Safety Status/Faults..... 74
 Safety Signature and Safety-locked and -unlocked Status 75
 Checks for Going Online with a GuardLogix Controller..... 76
 Download to the Controller 77
 Use Who Active..... 77
 Use the Controller Status Menu 78

	Additional Considerations for Download to a GuardLogix Controller	78
	Upload from the Controller	80
	Use Who Active	80
	Use the Controller Status Menu	81
	Additional Considerations for Upload from a GuardLogix Controller	82
	Choose the Controller Operation Mode	83
	Use the keyswitch to Change the Operation Mode	84
	Use the Logix Designer Application to Change the Operation Mode	85
	Reset Button	86
	Stage 1 Reset	87
	Stage 2 Reset	88
	Safety Partner Reset	89
	 Chapter 6	
Use the Secure Digital Card	Considerations for Storing and Loading a Safety Project	93
	Store to the SD Card	94
	Load from the SD Card	98
	Controller Power-up	98
	User-initiated Action	99
	Other Secure Digital Card Tasks	100
	 Chapter 7	
Manage Controller Communication	Connection Overview	101
	Nodes on an EtherNet/IP Network	102
	Devices Included in the Node Count	102
	Devices Excluded from the Node Count	103
	Controller Communication Interaction with Control Data	104
	Produce and Consume (Interlock) Data	105
	Requested Packet Interval (RPI) of Multicast Tags	106
	Send and Receive Messages	107
	Determine Whether to Cache Message Connections	108
	Socket Interface	108
	Simple Network Management Protocol (SNMP)	109
	Use a CIP Generic MSG to Enable SNMP on the Controller	109
	Use a CIP Generic MSG to Disable SNMP on the Controller	111

Standard I/O Modules

Chapter 8

Selecting ControlLogix I/O Modules..... 113

 Electronic Keying..... 114

Local I/O Modules..... 115

 Add Local I/O to the I/O Configuration..... 115

Remote I/O Modules..... 120

 Add Remote I/O to the Ethernet Port on the Controller 121

 Add Remote I/O to a Local Communication Module 123

Add to the I/O Configuration While Online..... 127

 Modules and Devices that Can be Added While Online 128

Determine When Data is Updated..... 129

 Input Data Update Flowchart 129

 Output Data Update Flowchart 130

Safety I/O Devices

Chapter 9

Add Safety I/O Devices..... 131

Configure Safety I/O Devices 132

Using Network Address Translation (NAT) with CIP Safety Devices 134

Set the SNN of a Safety I/O Device..... 136

 Change a Safety I/O Device SNN..... 136

 Copy and Paste a Safety I/O Device SNN 138

Connection Reaction Time Limit 140

Safety I/O Device Signature..... 141

 Configuration via the Logix Designer Application..... 141

 Different Configuration Owner (data-only connection) 142

 Reset Safety I/O Device to Out-of-box Condition..... 143

I/O Device Address Format..... 144

Monitor Safety I/O Device Status 144

Replace a Safety I/O Device 145

 Configuration Ownership..... 145

 Replacement Configuration 146

 Replacement with ‘Configure Only When No Safety Signature Exists’ Enabled 147

 Replacement with ‘Configure Always’ Enabled..... 152

Develop Standard Applications

Chapter 10

Elements of a Control Application..... 153

Tasks..... 155

 Task Priority 157

Programs 157

 Scheduled and Unscheduled Programs 159

Routines..... 160

Parameters and Local Tags..... 161

 Program Parameters 162

Programming Languages	162
Add-On Instructions	163
Extended Properties	164
Access the Module Object from an Add-On Instruction	165
Monitor Controller Status	166
Monitor I/O Connections	167
Determine If I/O Communication Has Timed Out	167
Determine if I/O Communication to a Specific I/O Module has Timed Out	168
Automatic Handling of I/O Module Connection Faults	168
Sample Controller Projects	169

Chapter 11

Develop Safety Applications

Safety Task	172
Safety Task Period	173
Safety Task Execution	174
Safety Programs	174
Safety Routines	174
Safety Add-On Instructions	175
Safety Tags	175
Valid Data Types	176
Scope	176
Program Parameters	177
Produced/Consumed Safety Tags	177
Configure the SNN for a Peer Safety Controller Connection	178
Produce a Safety Tag	182
Consume Safety Tag Data	183
Safety Tag Mapping	186
Restrictions	186
Create Tag Mapping Pairs	187
Monitor Tag Mapping Status	188
Safety Application Protection	189
Safety-lock the Controller	189
Set Passwords for Safety-locking and Unlocking	191
Generate a Safety Signature	192
Programming Restrictions	194
Monitor Safety Status	195
View Status via the Online Bar	195
View Status via the Safety Tab	197
Monitor Safety Connections	198
Utilizing Status	199
Safety Faults	201
Nonrecoverable Controller Faults	201
Nonrecoverable Safety Faults in the Safety Application	201
Recoverable Faults in the Safety Application	202
View Faults	202
Fault Codes	203

Develop a Fault Routine for Safety Applications 204
 Use GSV/SSV Instructions in a Safety Application..... 205

Chapter 12

Develop Secure Applications

Controller Security Features 208
 System-level Security Features 209
 Controller-specific Security Features 211
 Verification of Security Implementation..... 212
 Configure Trusted Slot 213
 Configure User-definable Major Faults..... 214
 Create a Fault Routine 214
 Configure the Program to Use the Fault Routine..... 214
 Jump to the Fault Routine..... 215
 License-based Source and Execution Protection..... 216
 Enable License-based Protection 217
 Configure Change Detection..... 219
 Controller Audit Log..... 220
 Disable the Ethernet Port 221
 Disable the Ethernet Port on the Port Configuration Tab.... 222
 Disable the Ethernet Port with a MSG Instruction 223
 Disable the CIP Security Ports 225
 Disable the USB Port..... 228
 Disable the SD Card..... 230
 Disable the 4-character Status Display..... 232
 Disable All Categories of Messages 232
 Disable Individual Categories of Messages 234
 Disable the Controller Web Pages 236
 Studio 5000 Logix Designer Application Version 33.00.00
 and Later 236
 Studio 5000 Logix Designer Application Version 32.00.00 or Earlier
 236
 Controller Web Page Default Settings..... 237
 Use a CIP Generic MSG to Disable the Controller Web Pages 238
 Use a CIP Generic MSG to Enable the Controller Web Pages 240

Chapter 13

Develop Motion Applications

Motion Overview 244
 Program Motion Control..... 245
 Obtain Axis Information 247

Chapter 14

Troubleshoot the Controller

Automatic Diagnostics 249
 Considerations for Communication Loss Diagnostics 250
 Controller Diagnostics with Logix Designer 251
 I/O Module Properties Tab 252
 Notification in the Tag Monitor..... 253

Enable Major Fault on Controller 254
 Port Diagnostics 255
 Advanced Time Sync 257
 Controller Diagnostics with Linx-based Software 260
 Controller Web Pages 261
 Home Web Page 262
 Faults Web Page..... 263
 Tasks Webpage..... 264
 Browse Chassis Webpage..... 265

Status Indicators

Appendix A

Status Display and Indicators..... 268
 General Status Messages 269
 GuardLogix Status Messages 271
 Safety Partner Status Messages..... 271
 Fault Messages 271
 Major Fault Messages..... 272
 I/O Fault Codes 273
 Controller Status Indicators..... 274
 RUN Indicator..... 274
 FORCE Indicator 274
 SD Indicator 275
 OK Indicator 275
 Safety Partner OK Indicator 276
 EtherNet/IP Indicators..... 276
 Thermal Monitoring and Thermal Fault Behavior 277

Change Controller Type

Appendix B

Change from a Standard to a Safety Controller 279
 Change from a Safety to a Standard Controller 280
 Change Safety Controller Types..... 280

Index 281

Notes:

Catalog Numbers

This publication is applicable to these controllers:

Standard Catalog Numbers:	1756-L81E, 1756-L81EK, 1756-L82E, 1756-L82EK, 1756-L83E, 1756-L83EK, 1756-L84E, 1756-L84EK, 1756-L85E, 1756-L85EK
No Stored Energy (NSE) Catalog Numbers:	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE
ControlLogix-XT Catalog Numbers:	1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT
Process Catalog Numbers:	1756-L81EP, 1756-L83EP, 1756-L85EP
GuardLogix Catalog Numbers	1756-L81ES, 1756-L81ESK, 1756-L82ES, 1756-L82ESK, 1756-L83ES, 1756-L83ESK, 1756-L84ES, 1756-L84ESK, 1756-L8SP, 1756-L8SPK

Summary of Changes

This manual contains new and updated information as indicated in the following table.

Topic	Page
Added ControlLogix NSE, ControlLogix-XT, and ControlLogix Process controllers.	Throughout.
Updated safety signature definition.	30
Updated behavior of controller status indicators while loading a project from the SD card.	100
Added Simple Network Management Protocol (SNMP).	109
Added Automatic Diagnostics.	249
Added Considerations for Communication Loss Diagnostics.	250

Overview

This manual provides information about designing a system, operating a ControlLogix® or GuardLogix®-based controllers system, and developing applications.

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

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

Additional Resources

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

Table 1 - Additional Resources

Resource	Description	
Hardware Installation	ControlLogix 5580 Controllers Installation Instructions, publication 1756-IN043	Provides installation instructions for ControlLogix 5580 controllers.
	GuardLogix 5580 Controllers Installation Instructions, publication 1756-IN048	Provides installation instructions for GuardLogix 5580 controllers.
	ControlLogix Power Supply Installation Instructions, publication 1756-IN619	Describes how to install standard power supplies.
	ControlLogix Redundant Power Supply Installation Instructions, publication 1756-IN620	Describes how to install redundant power supplies.
	ControlLogix Chassis Installation Instructions, publication 1756-IN621	Describes how to install ControlLogix chassis.
	Replacement door labels for the 1756 I/O modules, publication IASIMP-SP021	Contains door labels for the 1756 I/O modules that are available to print.
Technical Data	1756 ControlLogix Controllers Technical Data, publication 1756-TD001	Provides specifications for ControlLogix controllers.
	1756 ControlLogix I/O Specifications Technical Data, publication 1756-TD002	Provides specifications for ControlLogix I/O modules.
	1756 ControlLogix Communications Modules Specifications Technical Data, publication 1756-TD003	Provides specifications for ControlLogix Communications Modules.
	1756 ControlLogix Integrated Motion Modules Specifications Technical Data, publication 1756-TD004	Provides specifications for ControlLogix Integrated Motion Modules.
	1756 ControlLogix Power Supplies Specifications Technical Data, publication 1756-TD005	Provides specifications for ControlLogix Power Supplies.
	1756 ControlLogix Chassis Specifications Technical Data, publication 1756-TD006	Provides specifications for ControlLogix Chassis.
Networks (ControlNet, DeviceNet, EtherNet/IP)	EtherNet/IP Network Devices User Manual, publication ENET-UM006	Describes how to configure and use EtherNet/IP™ devices with a Logix 5000™ controller and communicate with various devices on the Ethernet network.
	ControlNet Network Configuration User Manual, publication CNET-UM001	Provides information about ControlNet® networks.
	DeviceNet Media Design Installation Guide, publication DNET-UM072	Provides information about DeviceNet® networks.
Safety application requirements	GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012	Contains detailed requirements for achieving and maintaining SIL 2/PLd and SIL 3/PLe with the GuardLogix 5580 controller system, using the Studio 5000 Logix Designer® application.
Motion	Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003	Details how to design your ControlLogix system for Integrated Motion on the EtherNet/IP network applications.
	Integrated Motion on the EtherNet/IP Network Reference Manual, publication MOTION-RM003	Detailed information on axis control modes and attributes for Integrated Motion on EtherNet/IP networks.
	Motion Coordinate System User Manual, publication MOTION-UM002	Details how to create and configure a coordinated motion application system.
	SERCOS and Analog Motion Configuration and Startup User Manual, publication MOTION-UM001	Details how to configure a Sercos motion application system.

Table 1 - Additional Resources (continued)

Resource		Description
Design Considerations	Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides information to help design and plan Logix 5000 systems.
	High Availability System Reference Manual, publication HIGHAV-RM002	Provides information to help design and plan high availability systems.
	Ethernet Design Considerations Reference Manual, publication ENET-RM002	Provides additional information about network design for your system.
	FOUNDATION Fieldbus Design Considerations Reference Manual, PROCES-RM005	This document provides design choices and best practices for implementing a FOUNDATION Fieldbus network with the 1788-EN2FFR or 1788-CN2FFR linking devices.
	Using Logix 5000 Controllers as Masters or Slaves on Modbus Application Solution, publication CIG-AP129	For more information about using Modbus sample programs.
Programming Tasks and Procedures	Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Provides access to the Logix 5000 Controllers set of programming manuals. The manuals cover such topics as how to manage project files, organize tags, program logic, test routines, handle faults, and more.
	Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Provides information on the programming instructions available to use in Logix Designer application projects.
	GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety application instruction set.
Product Certifications	Product Certifications website, https://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

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

Notes:

ControlLogix and GuardLogix Systems

This chapter describes features and functions that are associated with the ControlLogix® 5580 and GuardLogix® 5580 controllers.

Topic	Page
Minimum Requirements	15
ControlLogix System	18
GuardLogix System	21
Design the System	24
CIP Security	24
Secure Controller Systems	25
ControlLogix 5580 Controller Features	25

Minimum Requirements

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers have these minimum requirements.

- ControlLogix Chassis, Series C (Series B chassis function within a derated temperature range)
- ControlLogix Chassis Power Supply
- Programming software

System	Cat. No.	Studio 5000 Logix Designer® (2)
ControlLogix	1756-L83E, 1756-L83EK ⁽¹⁾ , 1756-L85E, 1756-L85EK	Version 28.00.00 or later
	1756-L81E, 1756-L81EK, 1756-L82E, 1756-L82EK, 1756-L84E, 1756-L84EK	Version 29.00.00 or later
	1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE, 1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT, 1756-L81EP, 1756-L83EP, 1756-L85EP	Version 33.00.00 or later
GuardLogix	1756-L81ES, 1756-L81ESK, 1756-L82ES, 1756-L82ESK, 1756-L83ES, 1756-L83ESK, 1756-L84ES, 1756-L84ESK, 1756-L8SP, 1756-L8SPK	Version 31.00.00 or later ⁽³⁾

(1) Catalog numbers followed by a “K” indicate a conformal coating option.

(2) For compatible Linux-based communication software, and ControlFLASH Plus™ and ControlFLASH™ software, see the [Product Compatibility and Download Center \(PCDC\)](#).

(3) Studio 5000 Logix Designer Professional, Full Edition, or a separately licensed GuardLogix Safety Editor must be present on the workstation in order to edit a GuardLogix project.

IMPORTANT If safety connections or safety logic are required for your application, then you must use a GuardLogix 5580 controller.

ControlLogix Controllers

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

ControlLogix No Stored Energy (NSE) Controllers

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

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



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

1. Turn off power to the chassis.

After you turn off power, the controller's OK status indicator transitions from Green to Solid Red to OFF.

2. Wait at least **40 seconds** for the residual stored energy to decrease to 400 μ J or less before you remove the controller.

There is no visual indication of when the 40 seconds has expired. **You must track that time period.**

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

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

ControlLogix-XT Controllers

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

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

Process Controllers

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

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

Conformal Coated Products



ATTENTION: Conformal coated products are shipped with port protection plugs installed to provide a layer of protection from corrosive environments. In order to meet the corrosive atmosphere rating of the product, port plugs need to be installed in unused ports at all times during storage and operation. If temporary access is required, plugs can be removed, and should be reinserted after temporary access is complete.

ControlLogix Redundant Controllers

You can use ControlLogix 5580 controllers in redundant applications with the Studio 5000 Logix Designer application, version 33.00.00 or later.

For information, see these publications:

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

ControlLogix System

Applies to these controllers:

ControlLogix 5580

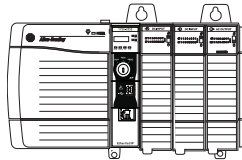
The ControlLogix system is chassis-based, which provides options for configuring a variety of communications and I/O capabilities. The ControlLogix controllers support multiple programming languages that enable sequential, process, motion, and drive control.

A variety of system configuration options are described in the following sections.

Standalone Controller and I/O

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

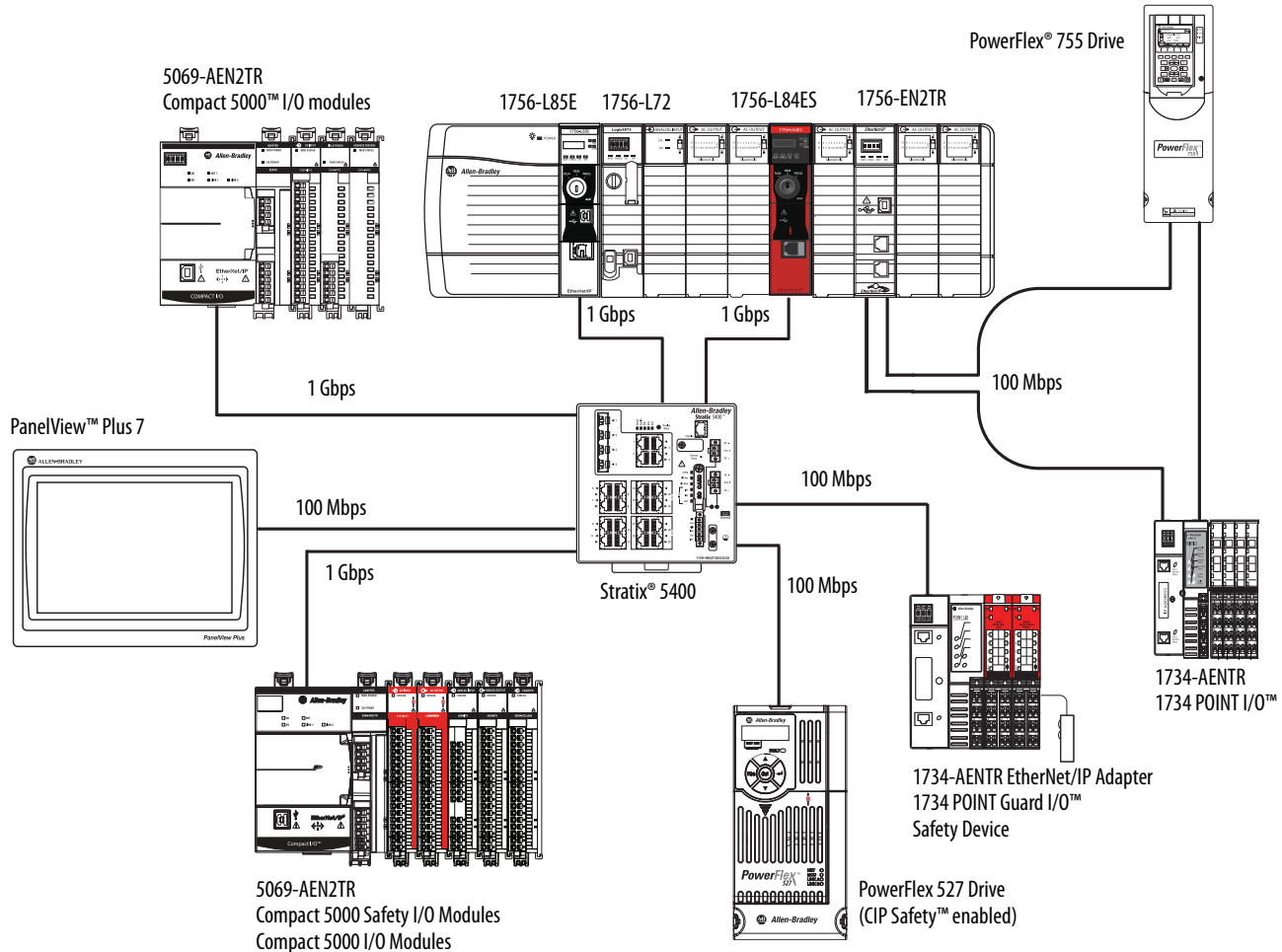
Figure 1 - Standalone Controller and I/O



Multiple Controllers in One Chassis

You can use multiple controllers in one ControlLogix chassis. This example shows a ControlLogix 5580 controller (slot 0) connected directly to the EtherNet/IP™ network, a ControlLogix 5570 controller (slot 1) connected to the network through a 1756-EN2TR module (slot 7), and a GuardLogix 5580 controller in a SIL 2/PLd configuration (slot 5) connected directly to the EtherNet/IP Network.

Figure 2 - Multiple Controllers in One Chassis



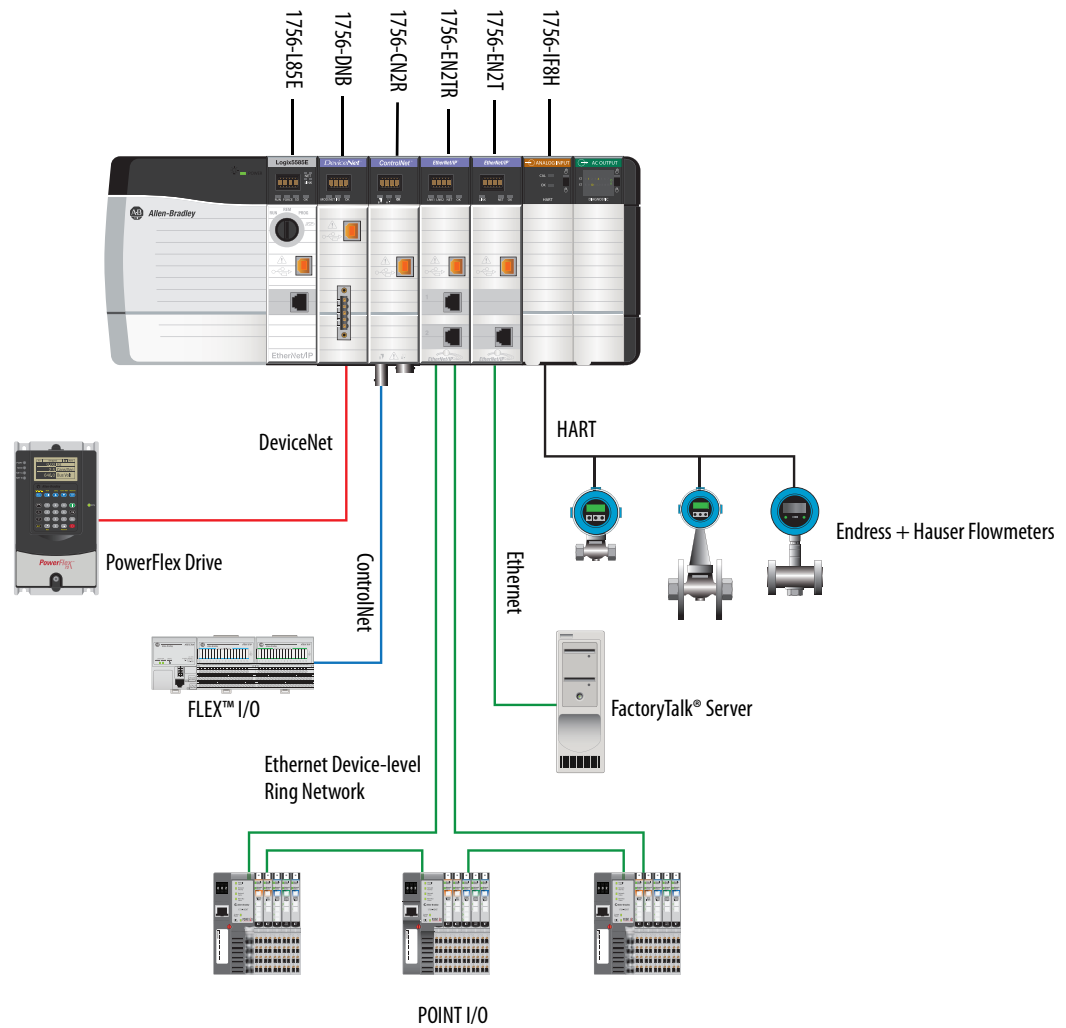
IMPORTANT You cannot bridge through the Ethernet (front) port of another controller to add remote I/O.

Multiple Devices Connected via Multiple Networks

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

- Distributed I/O via an Ethernet network
- A PowerFlex drive connected via a DeviceNet® network
- Distributed I/O via a ControlNet® network.
- Flowmeters that are connected via a HART connection

Figure 3 - Multiple Devices Connected Via Multiple Networks



GuardLogix System

Applies to these controllers:

GuardLogix 5580

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

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

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

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

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

For standard tasks, GuardLogix controllers support:

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

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

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

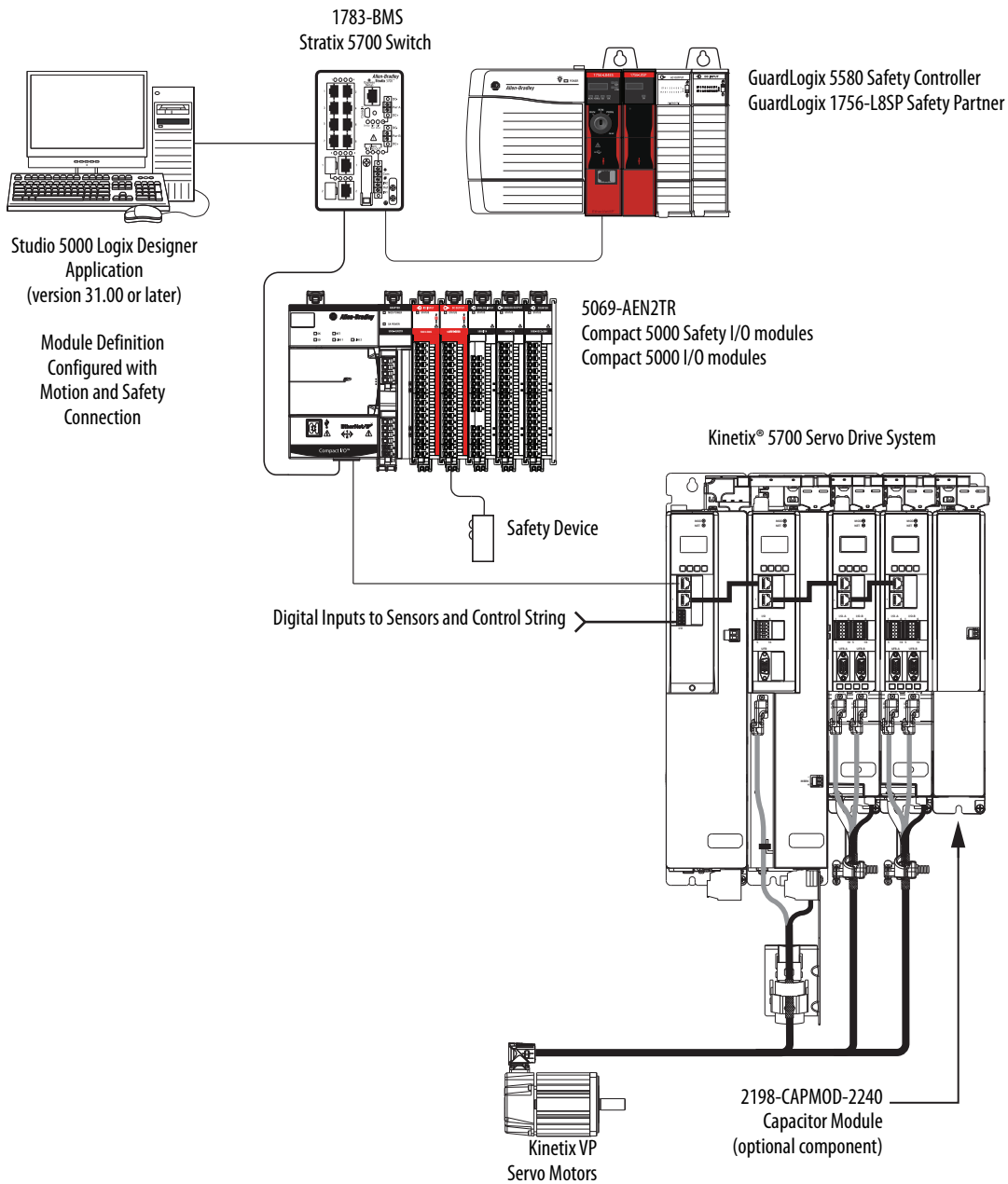
For information on Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

GuardLogix with Safety I/O and Integrated Safety Drives

In this example, a single GuardLogix safety controller makes the Motion and Safety connections.

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

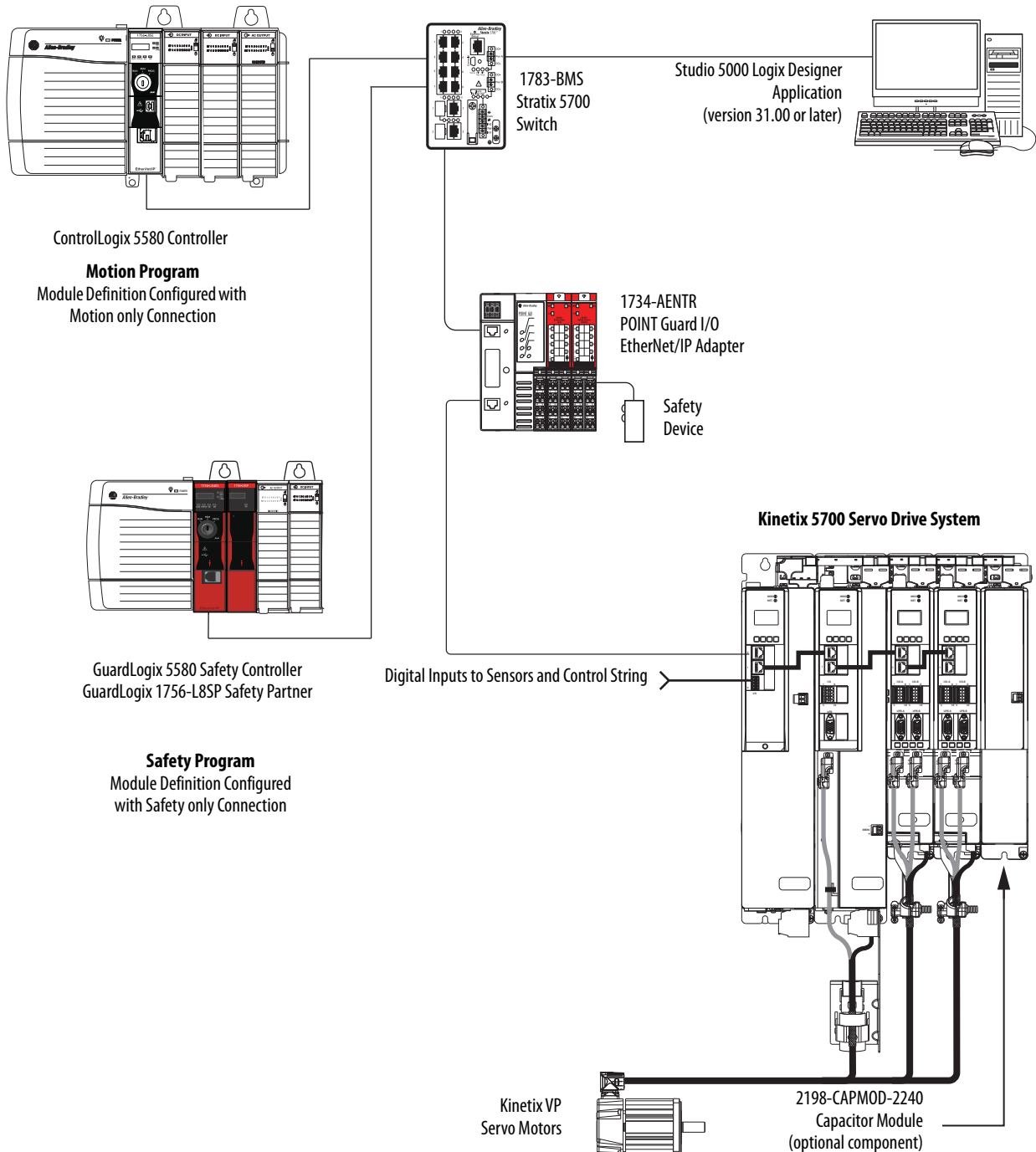
Figure 4 - Motion and Safety Configuration (single controller)



In this example, a standard controller makes the Motion-only connection and a separate GuardLogix 5580 controller makes the safety-only connection.

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

Figure 5 - Motion and Safety Configuration (multi-controller)



Design the System

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

In addition, safety systems have also have components to consider:

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

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

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

CIP Security

CIP Security™ is a standard, open-source communication method that helps to provide a secure data transport across an EtherNet/IP network.

The secure data transport is used between certain connected devices to help protect the devices from threats posed by unauthorized users with malicious intent.

Rockwell Automation uses the following products to implement CIP Security:

- FactoryTalk Policy Manager
- FactoryTalk Linx
- Studio 5000® Design Environment
- CIP Security-enabled products from Rockwell Automation, for example, the products described in this publication

For more information on CIP Security, including which products support CIP Security, see the CIP Security Application Technique, publication [SECURE-AT001](#).

Secure Controller Systems

The ControlLogix 5580 controller, firmware revision 32 supports IEC-62443-4-2 SL 1 requirements. For security features and system requirements, see [Develop Secure Applications on page 207](#).

ControlLogix 5580 Controller Features

This table lists the system, communication, and programming features available with ControlLogix 5580 controllers.

Applies to these controllers:

ControlLogix 5580

Table 1 - ControlLogix 5580 Controller Features

Feature	1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP
User Memory	3 MB	5 MB	10 MB	20 MB	40 MB
EtherNet/IP nodes supported, max ⁽¹⁾	60 nodes ⁽⁴⁾ 100 nodes ⁽⁵⁾	80 nodes ⁽⁴⁾ 175 nodes ⁽⁵⁾	100 nodes ⁽³⁾ 250 nodes ⁽⁵⁾	150 nodes ⁽⁴⁾ 250 nodes ⁽⁵⁾	300 nodes ⁽⁶⁾
Communication ports	1 - USB port, 2.0 full-speed, Type B 1 - EtherNet/IP port: 10 Mbps, 100 Mbps, 1 Gbps link speeds				
Communication options	<ul style="list-style-type: none"> • EtherNet/IP • ControlNet • DeviceNet • Data Highway Plus™ • Remote I/O • SynchLink™ • Third-party process and device networks 				
Controller tasks	<ul style="list-style-type: none"> • 32 tasks • 1000 programs/task • Event tasks: all event triggers 				
Integrated motion	<ul style="list-style-type: none"> • Integrated Motion on the EtherNet/IP network • Sercos interface⁽²⁾ • Analog options⁽²⁾: <ul style="list-style-type: none"> – Encoder input – Linear displacement transducer (LDT) input – Serial Synchronous Input (SSI) 				
Programming languages	<ul style="list-style-type: none"> • Ladder Diagram (LD) • Structured Text (ST) • Function Block Diagram (FBD) • Sequential Function Chart (SFC) 				

(1) A node is an EtherNet/IP device that you add directly to the I/O configuration, and counts toward the node limits of the controller. For more information on EtherNet/IP nodes, see the ControlLogix 5580 Controllers User Manual, publication [1756-UM543](#).

(2) With Studio 5000 Logix Designer Application Version 31 or greater.

(3) With Studio 5000 Logix Designer Application Version 28 and Version 29.

(4) With Studio 5000 Logix Designer Application Version 29.

(5) With Studio 5000 Logix Designer Application Version 30 or greater.

(6) With Studio 5000 Logix Designer Application Version 28 or greater.

GuardLogix 5580 Controller Features

Applies to these controllers:
GuardLogix 5580

This table lists the system, communication, and programming features available with GuardLogix 5580 controllers.

Table 2 - GuardLogix 5580 Controller Features

Feature	1756-L81ES	1756-L82ES	1756-L83ES	1756-L84ES
User Memory	3 MB	5 MB	10 MB	20 MB
Safety Memory	1.5 MB	2.5 MB	5 MB	6 MB
EtherNet/IP nodes supported, max	100	175	250	250
Communication ports	1 - USB port, 2.0 full-speed, Type B 1 - EtherNet/IP port: 10 Mbps, 100 Mbps, 1 Gbps link speeds			
Communication options	<ul style="list-style-type: none"> • EtherNet/IP (1756-EWEB cannot be used for safety connections) • Support for Network address translation (NAT) • ControlNet • DeviceNet • Data Highway Plus • Remote I/O • SynchLink • Third-party process and device networks 			
Controller tasks	<ul style="list-style-type: none"> • 31 standard tasks, 1 safety task • 1000 programs/task • Event tasks: all event triggers 			
Integrated motion	Integrated motion is supported in standard task only. <ul style="list-style-type: none"> • Integrated Motion on the EtherNet/IP network • Sercos interface • Analog options: <ul style="list-style-type: none"> – Encoder input – Linear displacement transducer (LDT) input – Serial Synchronous Input (SSI) 			
Programming languages	<ul style="list-style-type: none"> • For the safety task, GuardLogix controllers support Ladder Diagram only. • For standard tasks, GuardLogix controllers support: <ul style="list-style-type: none"> – Ladder Diagram (LD) – Structured Text (ST) – Function Block Diagram (FBD) – Sequential Function Chart (SFC) 			
Integrated safety	<ul style="list-style-type: none"> • Integrated safety on the EtherNet/IP network (Kinetix drives, PowerFlex drives, safety components) • Distribute and control safety I/O (over EtherNet/IP and DeviceNet networks only) • Produce and consume safety tag data. 			
Controller Features	<ul style="list-style-type: none"> • Data access control • Firmware supervisor • Secure Digital (SD) card • Safety Connections • Standard Connections 			

Features Supported By GuardLogix 5580 Controllers Via the Safety Task

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

Feature	Studio 5000 Logix Designer Application, Version 31 or Later	
	Safety Task	Standard Task
Add-on instructions	X	X
Instruction-based alarms and events	—	X
Tag-based alarms	—	X
Controller logging	X	X
Event tasks ⁽¹⁾	—	X
Function block diagrams (FBD)	—	X
Integrated motion	X ⁽²⁾	X
Analog motion	—	X
Sercos motion	—	X
Drive Safety Instructions	X	—
Ladder Diagram (LD)	X	X
Language switching	X	X
License-based source protection	—	X
Online import of program components	—	X
Online export of program components	X	X
Sequential function chart (SFC) routines	—	X
Structured Text (ST)	—	X

(1) While the safety task cannot be an Event task, standard Event tasks can be triggered with the use of the Event instruction in the safety task.

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

IMPORTANT Safety Consideration

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

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

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

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

Notes:

Safety Concept of GuardLogix Controllers

Topic	Page
Functional Safety Capability	29
Safety Network Number	30
Safety Signature	30
Distinguish between Standard and Safety Components	31
Controller Data-flow Capabilities	32
Safety Terminology	33

Functional Safety Capability

Applies to these controllers:

GuardLogix 5580

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

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

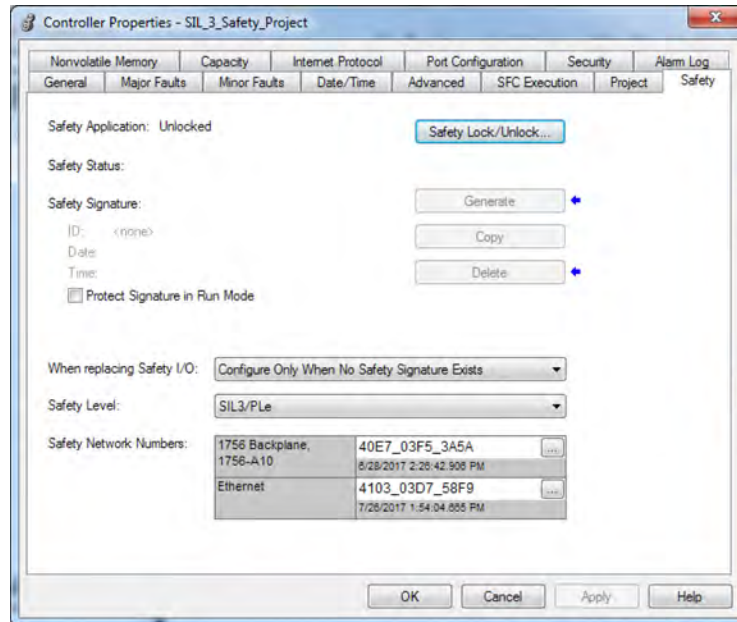
For SIL 2/PLd and SIL 3/PLe safety system requirements, including functional validation test intervals, system reaction time, and PFD/PFH calculations, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

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

Safety Network Number

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

The GuardLogix 5580 controllers require two safety network numbers: one for the Ethernet port, and one for the backplane.



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

For information on how to assign the SNN, see [Assign the Safety Network Number \(SNN\) on page 65](#).

Safety Signature

The safety signature is composed of a safety signature ID (identification number), and a timestamp (date and time). The safety signature ID applies to the entire safety portion of the controller and uniquely identifies each project, including its logic, data, and configuration.

The GuardLogix system uses the safety signature to determine project integrity and to let you verify that the correct project is downloaded to the target controller. 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.

See [Generate a Safety Signature on page 192](#) for more information.

Distinguish between Standard and Safety Components

Slots of a GuardLogix system chassis that are not used by the safety function can be populated with other ControlLogix® modules that are certified to the Low Voltage and EMC Directives. See the Rockwell Automation Product Certifications page (<http://www.rockwellautomation.com/global/certification/overview.page?>) to find the CE certificate for the ControlLogix Product Family, and determine the modules that are certified.

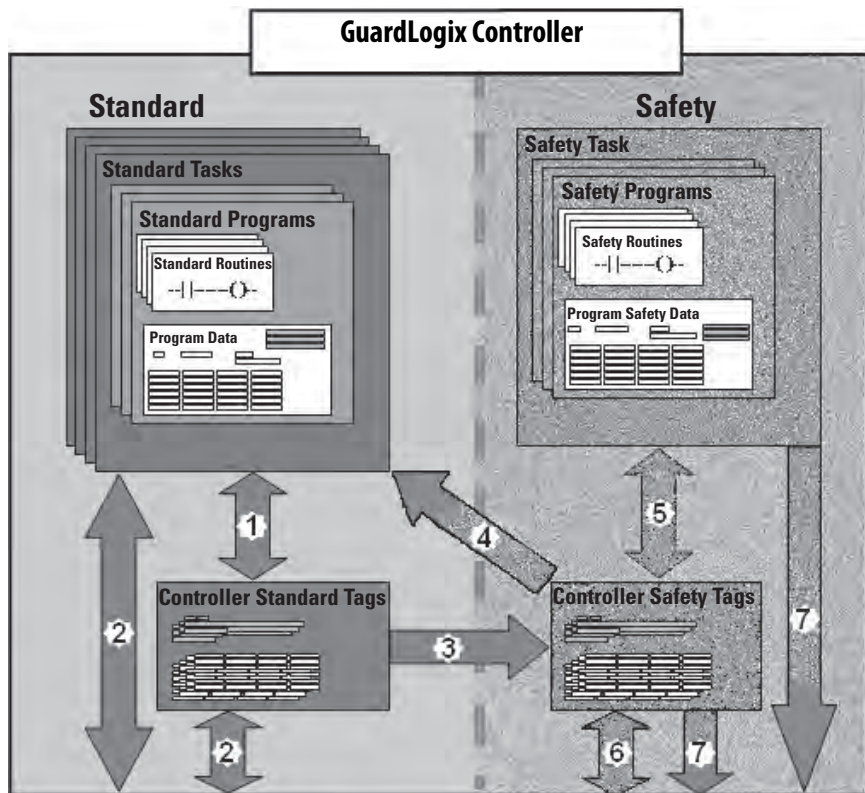
You must create and document a clear, logical, and visible distinction between the safety and standard portions of the controller project. As part of this distinction, the Studio 5000 Logix Designer® application features safety identification icons to identify the safety task, safety programs, safety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


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

Controller Data-flow Capabilities

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

Figure 6 - Data-flow Capabilities



No.	Description
1	Standard tags and logic behave the same way that they do in a standard ControlLogix controller.
2	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.
3	GuardLogix controllers are integrated controllers with the ability to move (map) standard tag data into safety tags for use within the safety task. This is the only way to get standard tag data in to the safety task. Safety logic in the safety task cannot read or write the standard tag that is the source in the tag mapping data transfer; it can only reference the safety tag destination of the mapping. But, it can read and write that safety tag.  ATTENTION: Mapped tag data must not be used to control a SIL 2/PLd or SIL 3/PLe output directly.
4	Controller-scoped safety tags can be read directly by standard logic.
5	Safety tags can be read or written by safety logic.
6	Safety tags can be exchanged between safety controllers over Ethernet or ControlNet® networks, including 1756 and 5069 GuardLogix controllers.
7	Safety tag data, program- or controller-scoped, can be read by external devices, such as HMI devices, personal computers, or other standard controllers. External devices cannot write to safety tags (whether the controller is protected or not). Once this data is read, it is considered standard data, not SIL 3/PLe data.

Safety Terminology

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

Table 3 - Safety Terms and Definitions

Abbreviation	Full Term	Definition
1oo1	One Out of One	Identifies the programmable electronic controller architecture. 1oo1 is a single-channel system.
1oo2	One Out of Two	Identifies the programmable electronic controller architecture. 1oo2 is a dual-channel system.
CIP Safety	Common Industrial Protocol – Safety Certified	SIL 3/PLe-rated version of CIP™.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
SIL	Safety Integrity Level	A relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction.
SIL CL	SIL Claim Limit	The maximum safety integrity level (SIL) that can be achieved.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
UNID	Unique Node ID (also called unique node reference)	The unique node reference is a combination of a safety network number (SNN) and the node address of the node.

Notes:

Communication Networks

Several communication networks are available.

Topic	Page
Networks Available	35
EtherNet/IP Network Communication	37
Double Data Rate (DDR) Backplane Communication for ControlLogix Controllers	40
ControlNet Network Communication	41
DeviceNet Network Communication	44
Data Highway Plus (DH+) Network Communication	45
Universal Remote I/O (RIO) Communication	47
Foundation Fieldbus Communication	49
HART Communication	50

Networks Available

[Table 4](#) describes typical application features that are used with ControlLogix® and GuardLogix® systems, and lists the networks available to support such application features.

Table 4 - Applications and Supported Networks

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

(1) The controllers also support analog and Sercos motion interfaces. For more information, See [Develop Motion Applications on page 243](#).

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

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

For more information about network design, see these publications;

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

EtherNet/IP Network Communication

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The EtherNet/IP network offers a full suite of control, configuration, and data collection services by layering the Common Industrial Protocol (CIP™) over the standard Internet protocols, such as TCP/IP and UDP. This combination of well-accepted standards provides the capability that is required to support information data exchange and control applications.

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

EtherNet/IP Link Speeds

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

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

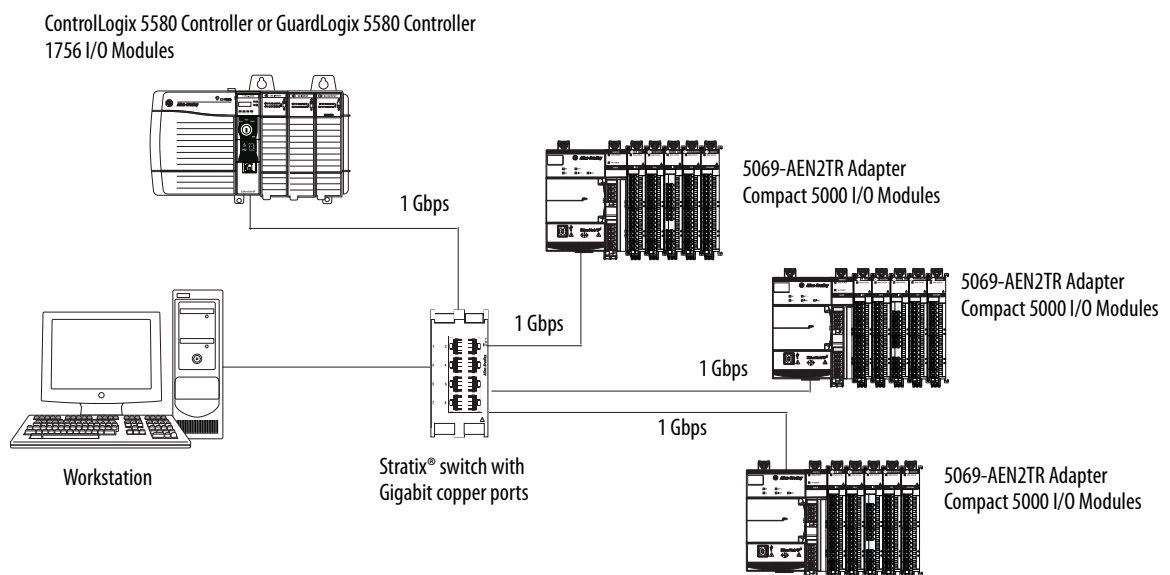
The difference in maximum link speeds impacts your controller system and, in some applications, restricts you from using the 1 Gbps link speeds on a controller.

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

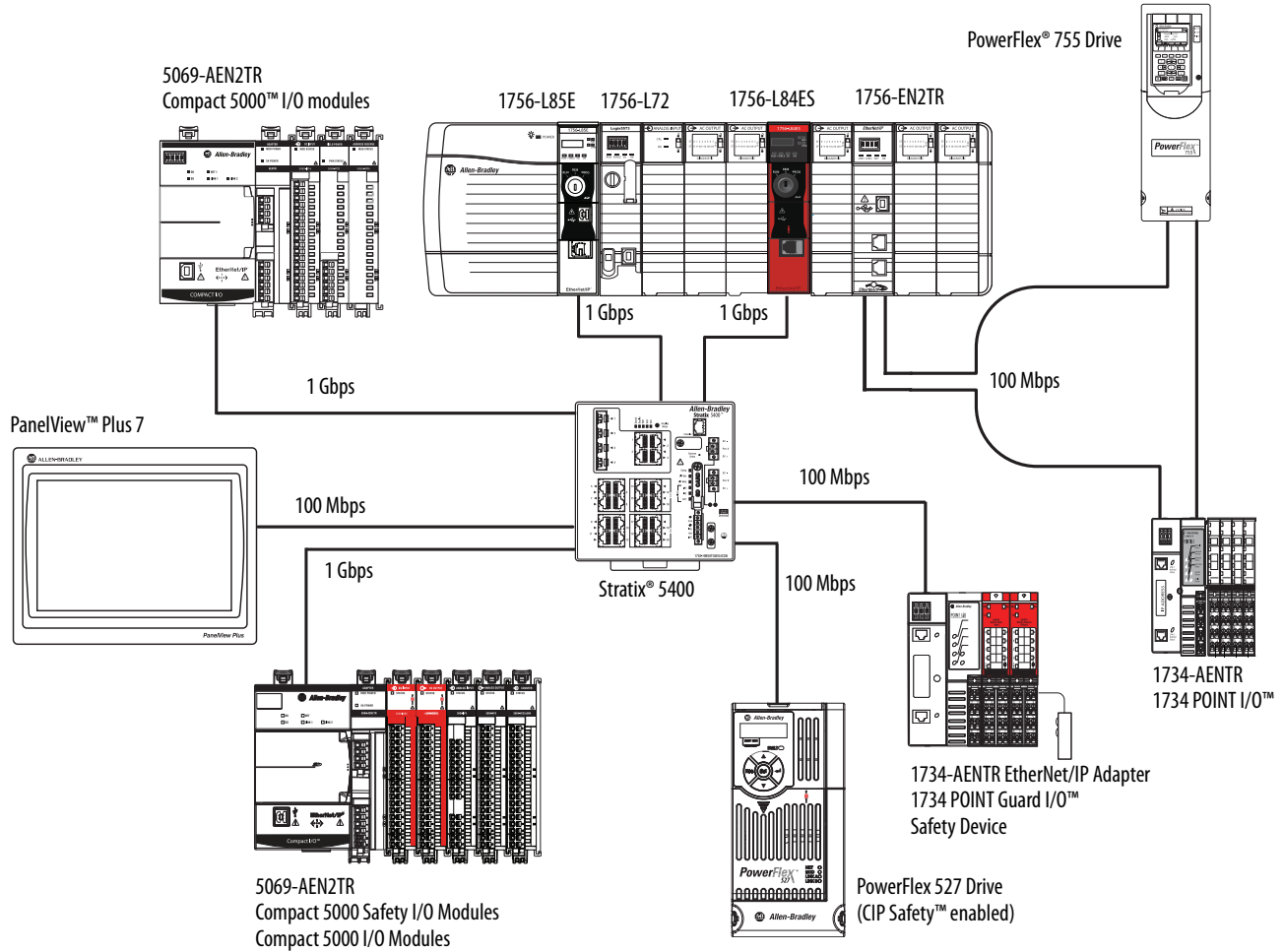
- You can use the 1 Gbps link speed on the controller port when all network devices support 1 Gbps, for example, 5069-AEN2TR adapters with Compact 5000™ I/O modules.

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

Figure 7 - 1 Gb EtherNet/IP Network Example



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



- Do not mix 1 Gbps and 100 Mbps link speeds within a single DLR ring or linear network.

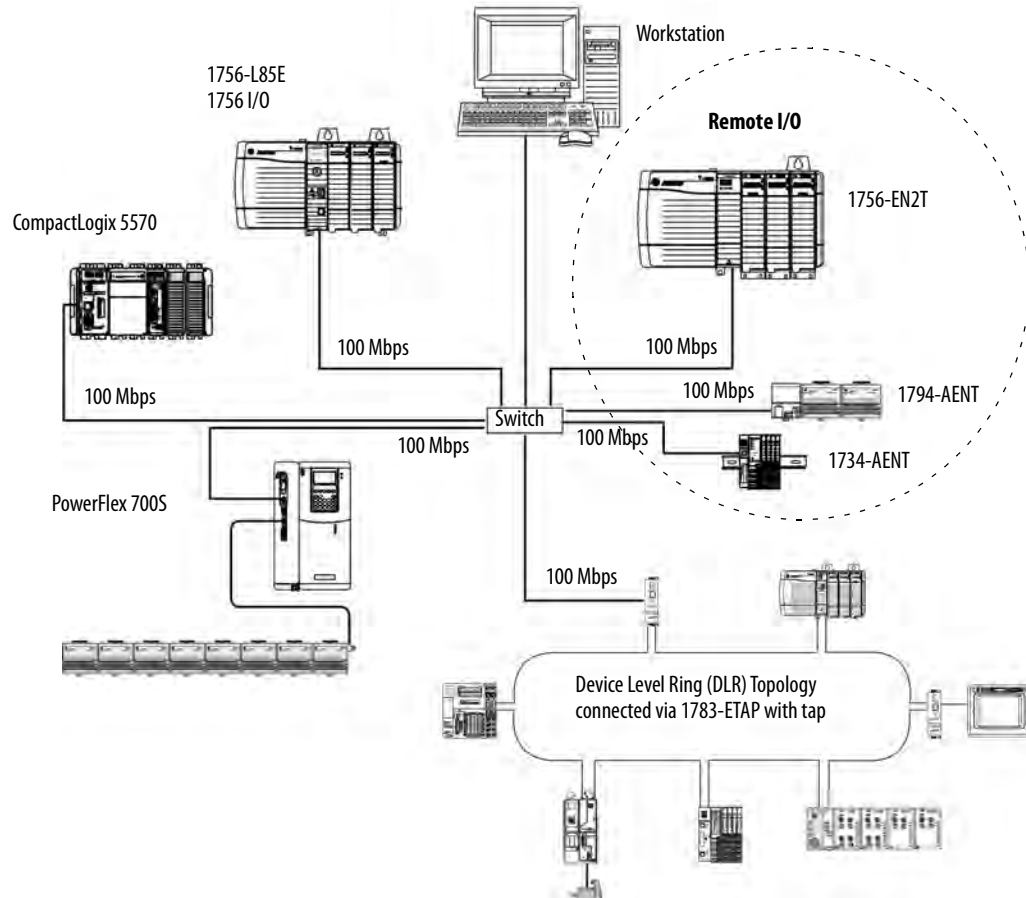
IMPORTANT Do not use different link speeds on device ports in the same EtherNet/IP network without a managed switch.

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

- ControlLogix 5580/GuardLogix 5580 Controllers
- CompactLogix™ 5380 Controllers
- 5069 communication adapters
- 5094 communication adapters

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

Figure 8 - 100 Mbps EtherNet/IP Network Example With An Unmanaged Switch



EtherNet/IP Communication Modules

For EtherNet/IP network communication, you have several modules to choose from. [Table 5](#) lists modules and their primary features.

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

Table 5 - EtherNet/IP Communication Modules

Module	Is used to
1756-L81E, 1756-L81EK ⁽¹⁾ , 1756-L81E-NSE, 1756-L81EP, 1756-L81ES, 1756-L81ESK, 1756-L81EXT, 1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82ES, 1756-L82ESK, 1756-L82EXT, 1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EP, 1756-L83ES, 1756-L83ESK, 1756-L83EXT, 1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84ES, 1756-L84ESK, 1756-L84EXT, 1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EP, 1756-L85EXT	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • Communicate with distributed I/O modules and other EtherNet/IP devices. • Bridge messages over an EtherNet/IP network. • Support 10 Mbps, 100 Mbps, 1 Gbps link speeds.
1756-EN2T, 1756-EN2TK, 1756-EN2TXT	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • Communicate with distributed I/O modules and other EtherNet/IP devices. • Bridge messages over an EtherNet/IP network. • 1756-EN2TXT operates in extreme environments with -25...70 °C (-13...158 °F) temperatures.
1756-EN2TR, 1756-EN2TRK, 1756-EN2TRXT	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Support communication on a ring topology for a Device Level Ring (DLR) single-fault tolerant ring network. • Also supports a linear topology. • 1756-EN2TRXT operates in extreme environments with -25...70 °C (-13...158 °F) temperatures.
1756-EN2F, 1756-EN2FK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Connect fiber media by an LC fiber connector on the module.
1756-EN2TP, 1756-EN2TPK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2T modules. • Support for Parallel Redundancy Protocol.
1756-EN3TR, 1756-EN3TRK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-EN2TR modules. • Extended Integrated Motion on EtherNet/IP network. • Support of up to 128 motion axes.
1756-ENBT, 1756-ENBTK	<ul style="list-style-type: none"> • Directly connect the controller to an EtherNet/IP network without requiring a bridge module. • Communicate with distributed I/O modules and other EtherNet/IP devices. • Bridge messages over an EtherNet/IP network.
1756-EN2TSC	<ul style="list-style-type: none"> • Perform the same functions as a 1756-ENBT module, with twice the capacity for more demanding applications. • Support for secure access to a control system from within the plant network.
1756-EWEB, 1756-EWEBK	<ul style="list-style-type: none"> • Perform the same functions as the 1756-ENBT modules. • Provide remote access via an Internet browser to tags in a local ControlLogix controller. <p>This module does not provide support for I/O or produced/consumed tags.</p> <p>This module does not support CIP Safety.</p>

(1) Catalog numbers followed by a "K" indicate a conformal coating option.

Double Data Rate (DDR) Backplane Communication for ControlLogix Controllers

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

ControlNet Network Communication

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

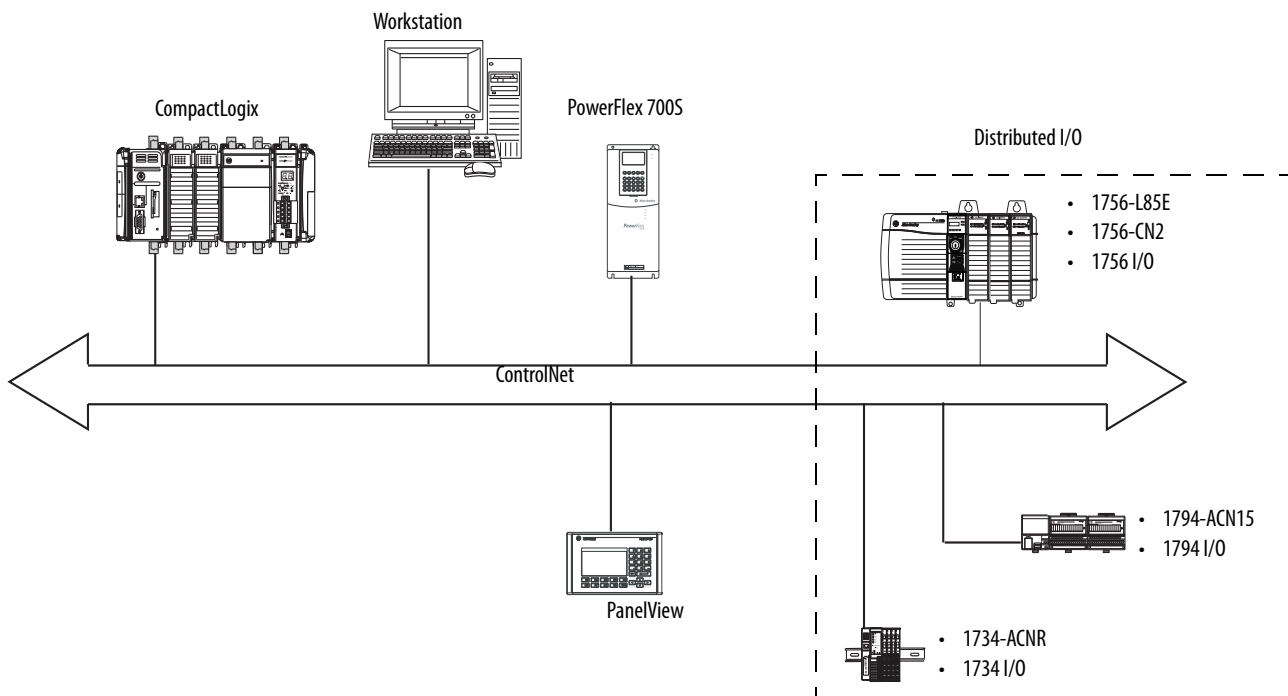
The ControlNet network often functions as the following:

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

In the example in [Figure 9](#), these actions occur via the ControlNet network:

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

Figure 9 - ControlNet Network Overview



GuardLogix ControlNet Example

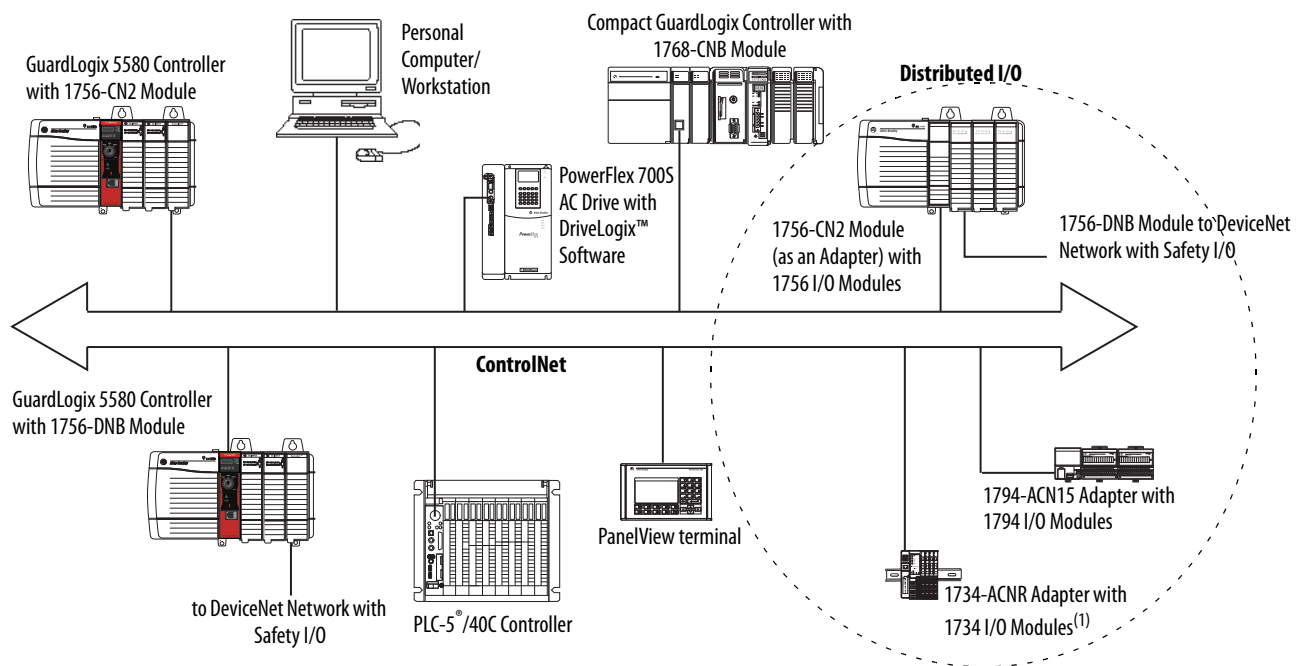
The ControlNet communication modules provide the following:

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

This example illustrates the following:

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

Figure 10 - ControlNet Communication Example



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

ControlNet Modules

[Table 6](#) lists the available ControlNet modules and their primary features.

Table 6 - ControlLogix ControlNet modules

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

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

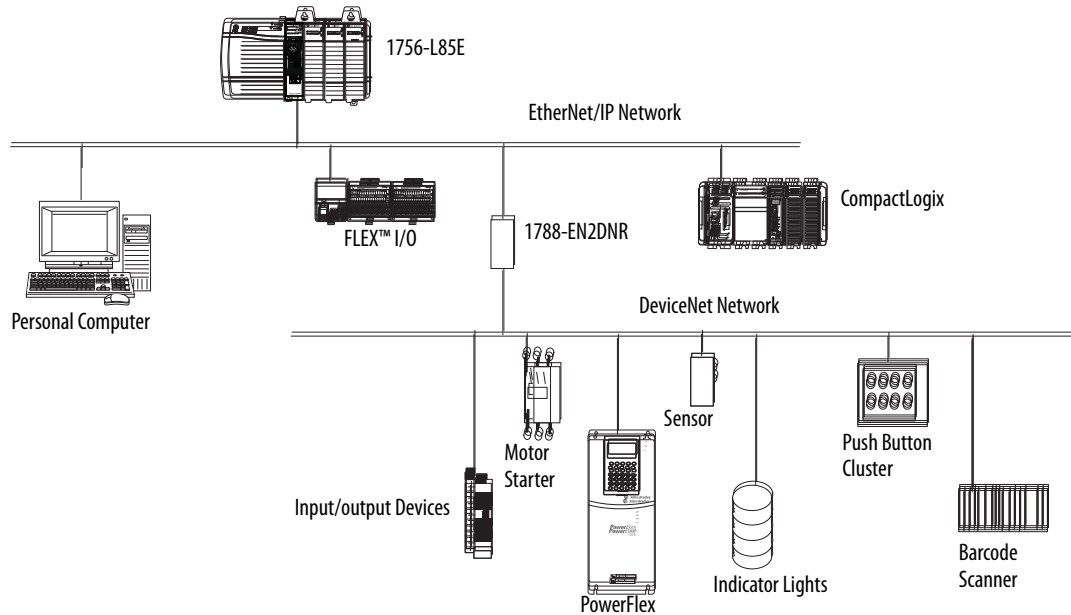
DeviceNet Network Communication

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

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

Figure 11 - ControlLogix DeviceNet Network Overview



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

For more information about using DeviceNet modules and devices, see DeviceNet Modules in Logix 5000 Control Systems User Manual, publication [DNET-UM004](#).

DeviceNet Bridge Module and Linking Devices

[Table 7](#) lists the available DeviceNet bridge and linking devices that can be used with the DeviceNet network.

Table 7 - DeviceNet Communication Modules and Capabilities

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

Connections Over DeviceNet Networks

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

Data Highway Plus (DH+) Network Communication

Applies to these controllers:

ControlLogix 5580

For DH+ network communication, you have two module options for use in the ControlLogix chassis. [Table 8](#) lists the DH+ modules and capabilities.

Table 8 - DH+ Modules and Capabilities

RIO Module	Is used to
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> Function as a remote I/O (RIO) scanner. Support 32 logical rack connections or 16 block transfer connections per channel. Establish connections between controllers and I/O adapters. Distribute control so that each controller has its own I/O. Use for standard communications only.
1756-DHRIOXT	<ul style="list-style-type: none"> Performs the same functions as a 1756-DHRIO module. Operates in extreme environments with -25...70 °C (-13...158 °F) temperatures. Use for standard communications only.

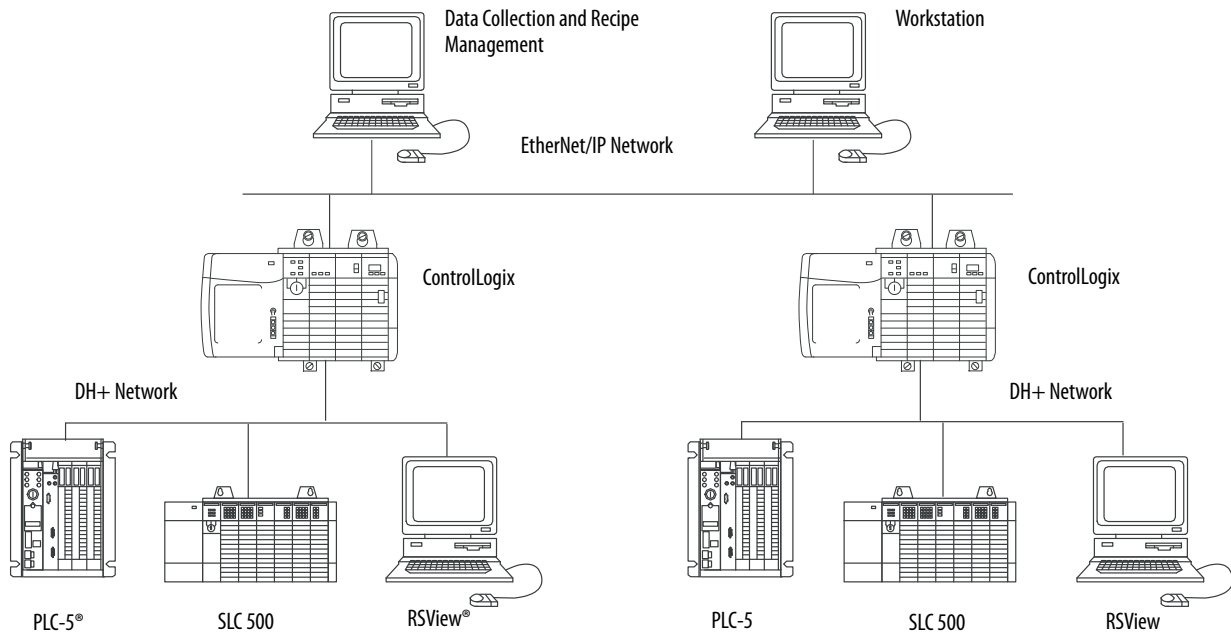
For DH+ network communication, use a 1756-DHRIO or 1756-DHRIOXT module in the ControlLogix chassis to exchange information between these controllers:

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

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

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

Figure 12 - ControlLogix DH+ Network Communication Example



Communicate Over a DH+ Network

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

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

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

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

Universal Remote I/O (RIO) Communication

Applies to these controllers:
ControlLogix 5580

For universal remote I/O communication, you have three module options for use in the ControlLogix chassis. [Table 9](#) lists the RIO modules and capabilities.

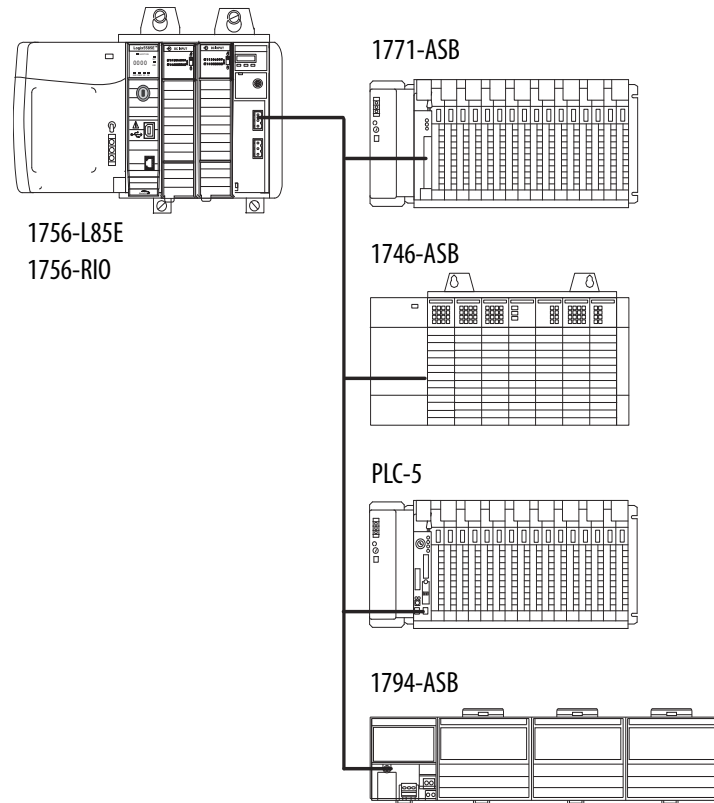
Table 9 - RIO Modules and Capabilities

RIO Module	Is used to
1756-RIO, 1756-RIOK	<ul style="list-style-type: none"> Function as an RIO scanner and adapter. Support connections to 32 racks in any combination of rack size or block transfers. Update data to the ControlLogix controller by using scheduled connections. Use for standard communications only.
1756-DHRIO, 1756-DHRIOK	<ul style="list-style-type: none"> Function as an RIO scanner. Support 32 logical rack connections or 16 block transfer connections per channel. Establish connections between controllers and I/O adapters. Distribute control so that each controller has its own I/O. Use for standard communications only.
1756-DHRIOXT	<ul style="list-style-type: none"> Performs the same functions as a 1756-DHRIO module. Operates in extreme environments with -25...+70 °C (-13...+158 °F) temperatures. Use for standard communications only.

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

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

Figure 13 - ControlLogix Universal Remote I/O Communication Example



Communicate Over a Universal Remote I/O Network

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

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

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

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

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

- All devices that are connected to a remote I/O network must communicate by using the same communication rate. These rates are available for remote I/O:
 - 57.6 Kbps
 - 115.2 Kbps
 - 230.4 Kbps
- You must assign unique partial and full racks to each channel used in Remote I/O Scanner mode.

Both channels of a 1756-DHRIO or 1756-DHRIOXT module cannot scan the same partial or full rack address. Both module channels can communicate to 00...37 octal or 40...77 octal, but each channel can communicate only with one address at a time in whichever of these two ranges it falls.

Foundation Fieldbus Communication

Applies to these controllers:

ControlLogix 5580

Foundation Fieldbus is an open interoperable fieldbus that is designed for process control instrumentation. The Foundation Fieldbus devices that are described in [Table 10](#) can be connected to the ControlLogix controller via another network as shown in the following example.

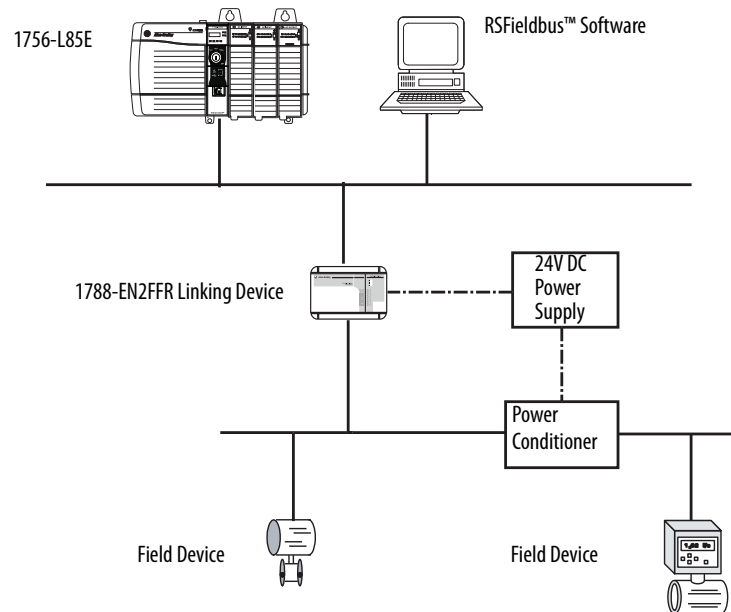
Table 10 - Foundation Fieldbus Devices and Capabilities

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

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

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

Figure 14 - Foundation Fieldbus Example



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

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

HART Communication

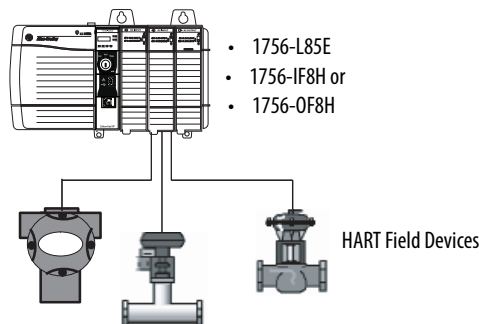
Applies to these controllers:
 ControlLogix 5580

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

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

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

Figure 15 - HART Protocol Example



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

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

Connect to a Controller

Topic	Page
Set the IP Address	51
Duplicate IP Address Detection	52
DNS Addressing	53
Update Controller Firmware	55

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

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

Set the IP Address

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

- The controllers ship without an IP address.
- The controller is DHCP-enabled. That is, the controller is configured to obtain an IP address via a DHCP server.

If there is no DHCP server or the DHCP server is not configured to set the IP address, you must set the IP Address manually.

Requirements

To set the IP address, have the following:

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

Other Methods to Set the IP Address

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

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

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

Duplicate IP Address Detection

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

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

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

- Network (NET) status indicator is solid red.
- The 4-character display indicates the conflict.

The display scrolls: <IP_address_of_this_module> Duplicate IP
<Mac_address_of_duplicate_node_detected>

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

Duplicate IP Address Resolution

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

Duplicate IP Address Detection Conditions	Resolution Process
<ul style="list-style-type: none"> Both devices support duplicate IP address detection. Second device is added to the network after the first device is operating on the network. 	<ol style="list-style-type: none"> The device that began operation first uses the IP address and continues to operate without interruption. The device that begins operation second detects the duplication and enters Conflict mode. To assign a new IP address to the controller and leave Conflict mode, set the Network IP Address with the BootP DHCP EtherNet/IP Commissioning Tool. See the EtherNet/IP Network Device User Manual, publication ENET-UM006.
<ul style="list-style-type: none"> Both devices support duplicate IP address detection Both devices were powered up at approximately the same time. 	<p>Both EtherNet/IP devices enter Conflict mode. To resolve this conflict, follow these steps:</p> <ol style="list-style-type: none"> Assign a new IP address to the controller. Set the Network IP Address with the BootP DHCP EtherNet/IP Commissioning Tool. See the EtherNet/IP Network Device User Manual, publication ENET-UM006. Cycle power to the other device.
One device supports duplicate IP address detection and a second device does not	<ol style="list-style-type: none"> 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. The device that supports duplicate IP address detection detects the duplication and enters Conflict mode. To assign a new IP address to the controller and leave Conflict mode, set the Network IP Address with the BootP DHCP EtherNet/IP Commissioning Tool. See the EtherNet/IP Network Device User Manual, publication ENET-UM006.

DNS Addressing

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

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

To use DNS addressing, follow these steps.

- Assign a host name to the controller.

A network administrator can assign a host name. Valid host names must be IEC-1131-3 compliant.

- Configure the controller parameters.
- 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.

- In the Logix Designer application, add the controller to the I/O configuration tree.

IMPORTANT If a child module resides in the same domain as its parent module, type the host name. If the domain of the child module differs from the domain of its parent module, type the host name and the domain name (hostname.domainname)

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

Update Controller Firmware

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

To update your controller firmware, complete these tasks:

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

Firmware Upgrade Guidelines for Safety Controllers

IMPORTANT Safety Consideration

You cannot update a controller that is safety locked.

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

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

- All major and minor firmware releases for GuardLogix controller systems are certified for use in safety applications. As part of the certification process, Rockwell Automation tests the safety-related firmware functions (for example the CIP Safety™ communication subsystems, embedded safety instruction execution, and safety-related diagnostic functions). The firmware release notes identify changes to safety-related functions.
- Perform an impact analysis of the planned firmware upgrade.
 - Review of the firmware release notes for changes in safety-related functionality.
 - Review of hardware and firmware compatibility in the Product Compatibility and Download site to identify potential compatibility conflicts.
 - Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system as described in the 'Edit Your Safety Application' section in the safety reference manual for your controller.
- You must remove and re-generate the safety signature as part of the firmware upgrade process. Use the online and offline edit process described in the safety reference manual for your controller.

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

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

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

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 identified during the impact analysis and determine what additional testing is necessary.
3. Perform the online and offline edit process described in the safety reference manual for your controller. You can restrict the 'Test the Application' block to the testing identified by the hazard and risk assessment.

Determine Required Controller Firmware

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

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

IMPORTANT Safety Consideration

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

Obtain Controller Firmware

You can obtain controller firmware in these ways:

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

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

We recommend that you check the Product Compatibility and Download Center (PCDC) to determine if later revisions of the controller firmware are available. For more information, see the next bullet.

- From the Rockwell Automation Product Compatibility and Download Center (PCDC). You can check for available revisions of controller firmware, and download controller firmware, associated files, and product release notes.

ControlFLASH Plus™ software version 2.00.00 and later provides integration with PCDC for an enhanced experience while you browse for firmware revisions, downloads, release notes, and access to important notices.

To visit PCDC, go to <http://compatibility.rockwellautomation.com/Pages/home.aspx>.

Use ControlFLASH Plus or ControlFLASH Software to Update Firmware

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

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

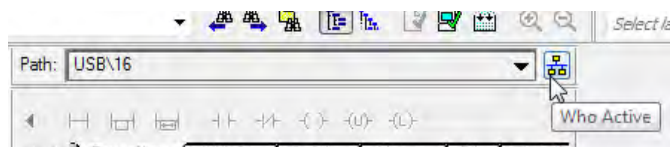
Use AutoFlash to Update Firmware

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

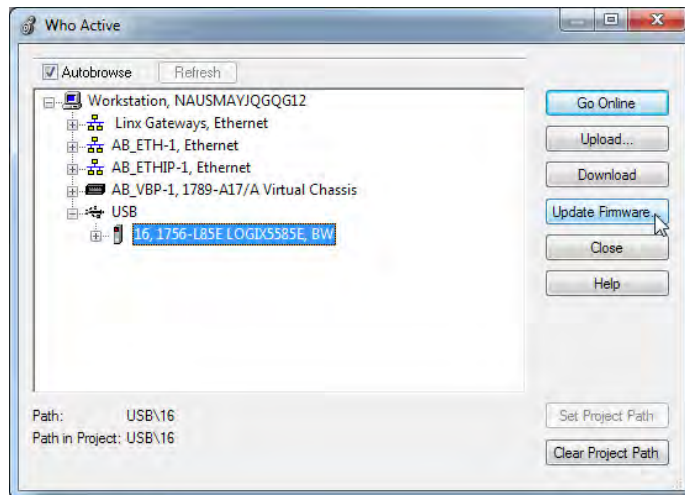


ATTENTION: If the Secure Digital Card is locked and set to load on power-up, then this update can be overwritten by firmware on the SD card.

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

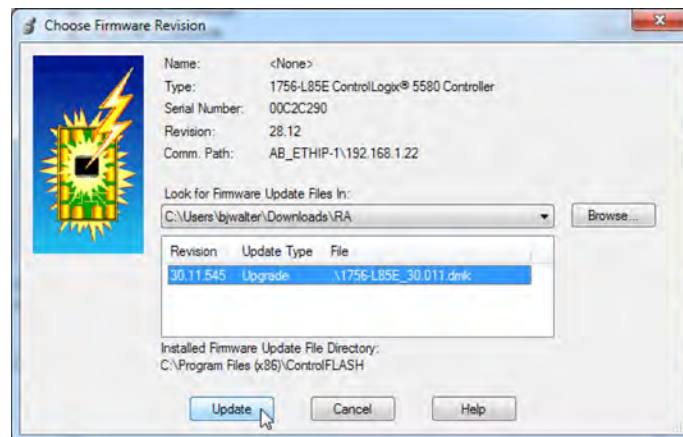


4. On the Who Active dialog box, select your controller under the communication driver you want to use, and click Update Firmware.

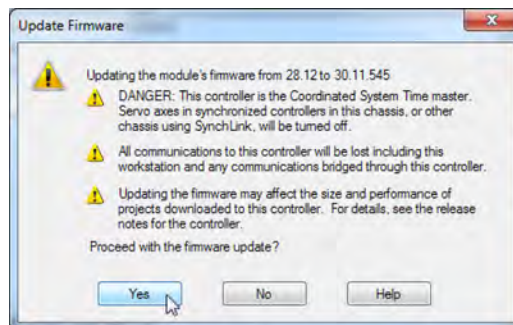


5. On the Choose Firmware Revision dialog, browse to the location of the firmware files (C:\Program Files (x86)\ControlFLASH).

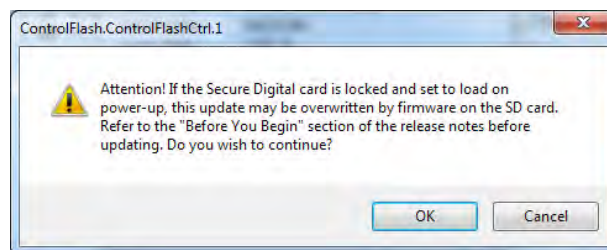
6. Select the firmware revision, and click Update.



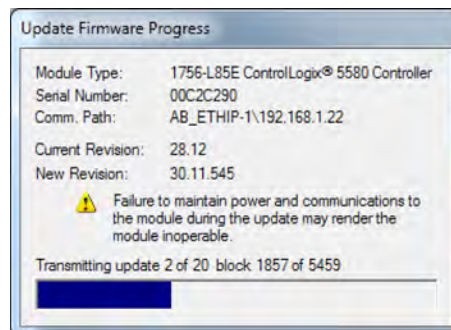
7. On the Confirmation dialog, click Yes.



8. On the ControlFLASH Attention dialog, click OK.



The firmware update begins.



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

Notes:

Start Using the Controller

Topic	Page
Create a Logix Designer Application Project	61
Additional Configuration for a GuardLogix Controller	62
Go Online with the Controller	71
Download to the Controller	77
Upload from the Controller	80
Choose the Controller Operation Mode	83
Reset Button	86

Create a Logix Designer Application Project

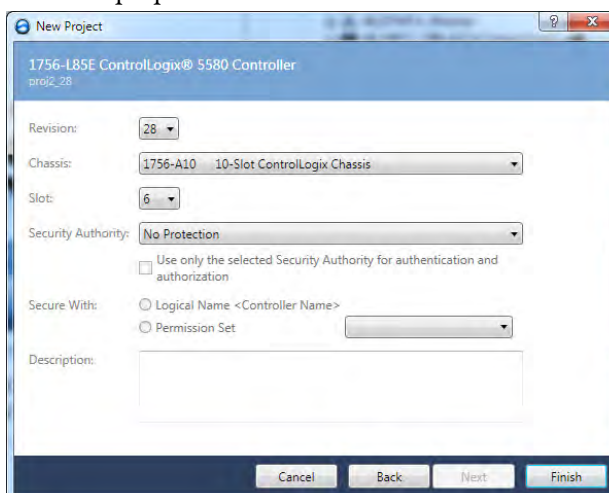
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

1. Create a new project and select the controller.
2. Define the properties of the controller.



- Choose the major revision of firmware for the controller.
- Choose the chassis size.
- Choose the slot for the controller.
- Choose a security authority option.

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

- Enter a description of the project.

Additional Configuration for a GuardLogix Controller

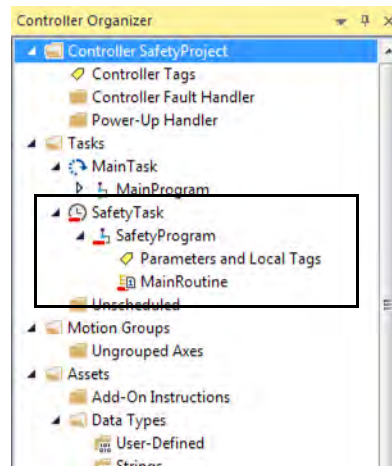
Applies to these controllers:

GuardLogix 5580

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

For a GuardLogix controller, the Logix Designer application creates a safety task and a safety program. A main Ladder Diagram safety routine called MainRoutine is also created within the safety program.

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



Set the Safety Level for a GuardLogix Controller

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

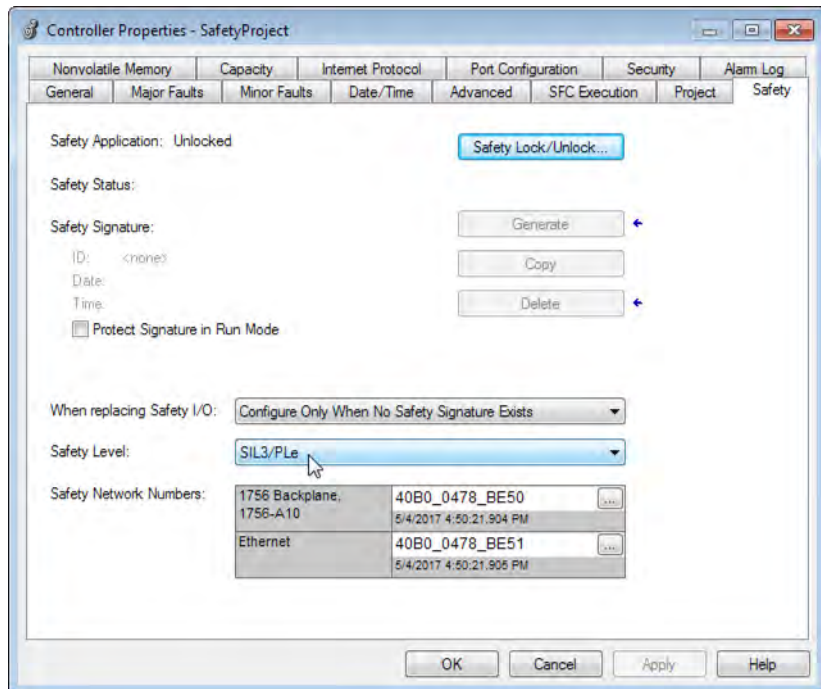
- The safety level required for an application is based on a required risk assessment performed by the customer.
- The safety level achieved is determined by conformance to Safety Integrity Level (SIL) and Performance Level (PL) requirements and safety application requirements. See the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

You must specify the safety level:

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

Perform these steps to set the Safety Level:

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



4. Click Apply.
5. Click OK.

Passwords for Safety-locking and Unlocking

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

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

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

For information on how to set passwords, see [Set Passwords for Safety-locking and Unlocking on page 191](#).

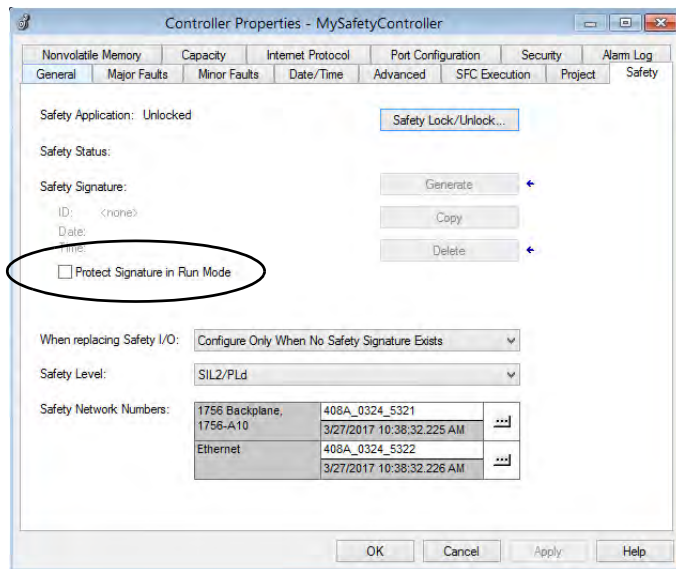
Protect the Safety Signature in Run Mode

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

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

Follow these steps to protect the safety signature:

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



Assign the Safety Network Number (SNN)

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

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

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

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

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

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

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

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

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

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

- [Automatic Assignment of Time-based SNN on page 66](#)
- [Manual Assignment of SNN on page 67](#)

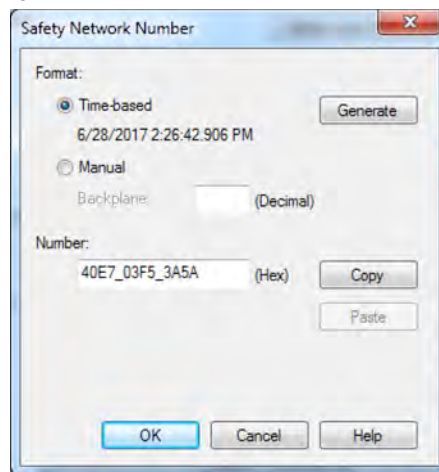
Automatic Assignment of Time-based SNN

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

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

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

Figure 16 - Time-based Format



Manual Assignment of SNN

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

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

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

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

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

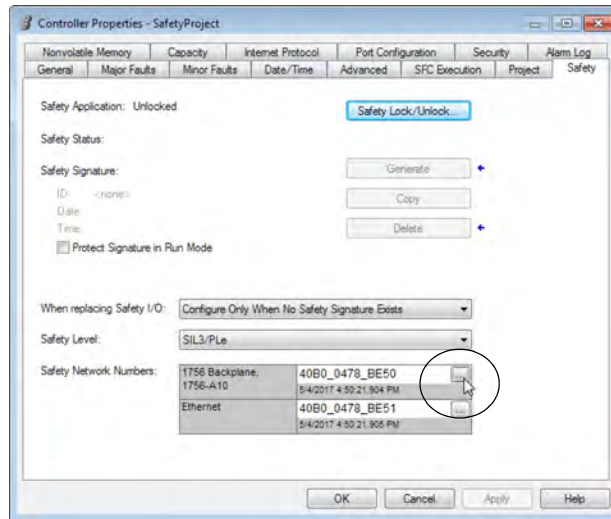
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

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

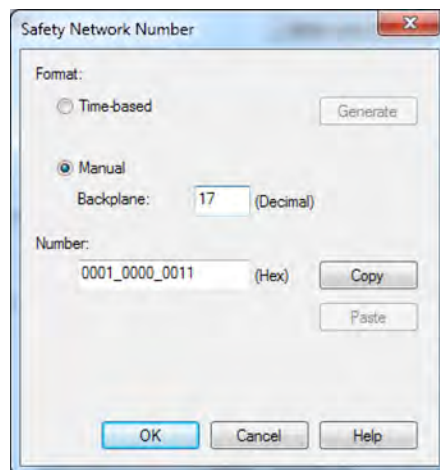
If there are duplicate unique node references, as the system user, you are responsible for proving that an unsafe condition cannot result.

Follow these steps to change the controller SNNs to a manual assignment:

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



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



6. Click OK.

You can allow the Logix Designer application to automatically assign an SNN, or you can assign the SNN manually.

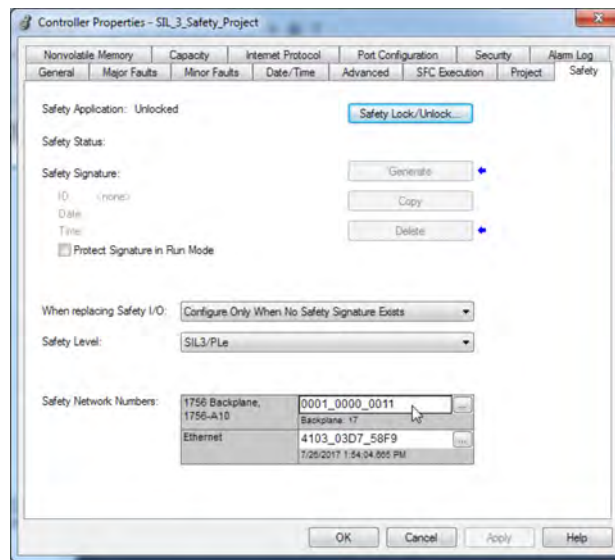
Copy and Paste a Safety Controller Safety Network Number

If you must apply a Safety Network Number (SNN) to other safety controllers, you can copy and paste the SNN. There are multiple ways to copy and paste safety controller SNNs.


Copy a Safety Controller SNN

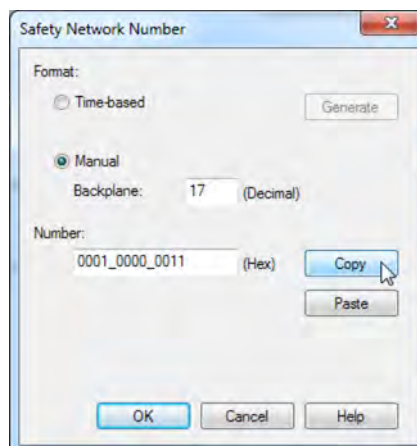
From the Controller Properties Safety Tab:

1. On the Safety tab, click in the SNN field that you want to copy.
2. Press Ctrl-C to copy the SNN.



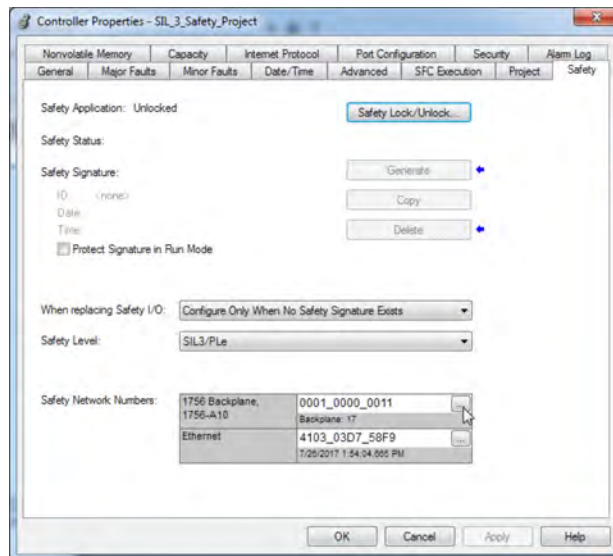
From the Safety Network Number dialog:


1. On the Controller Properties dialog, click the Safety tab.
2. Click  to the right of the safety network number to open the Safety Network Number dialog.
3. On the Safety Network Number dialog, either click Copy, or click in the SNN field and Press Ctrl-C.

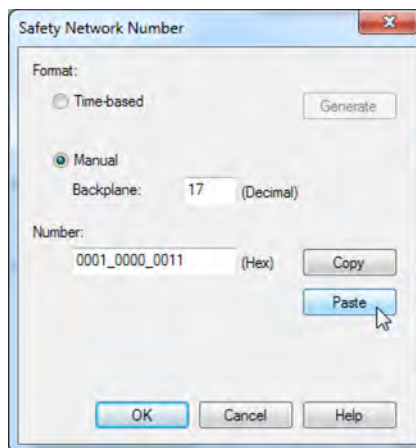


Paste a Safety Controller SNN

1. On the Controller Properties dialog, click the Safety tab.



2. Click  to the right of the safety network number to open the Safety Network Number dialog.
3. On the Safety Network Number dialog, either click Paste, or click in the SNN field and Press Ctrl-V.



4. Click OK.
5. On the Controller Properties Safety tab, click OK.

Go Online with the Controller

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

Applies to these controllers:

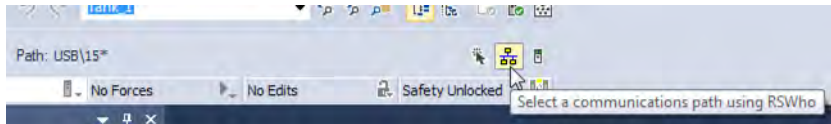
ControlLogix 5580

GuardLogix 5580

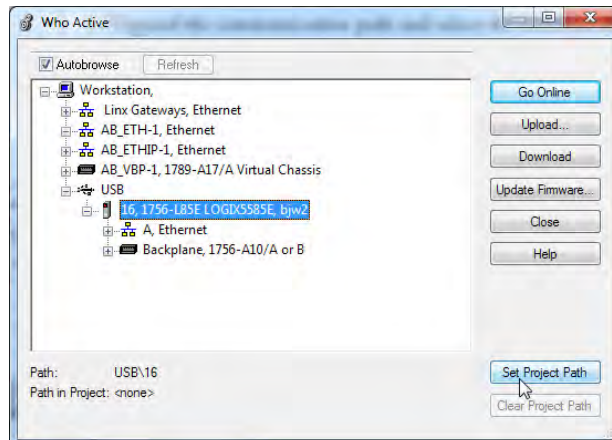
TIP For this section, the USB port was chosen as the communication path. Other paths through the embedded Ethernet port or via the backplane are also possible.

Use RSWho

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



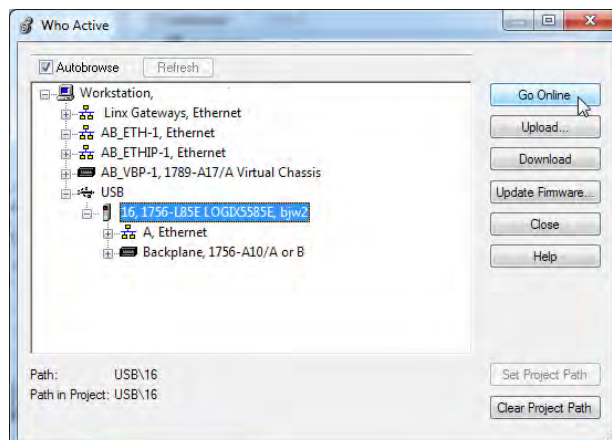
3. Expand the communication path and select the controller.



4. If you want to store the path in the project file, click Set Project Path.

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

5. After choosing the communication path, click Go Online in the Who Active dialog box.



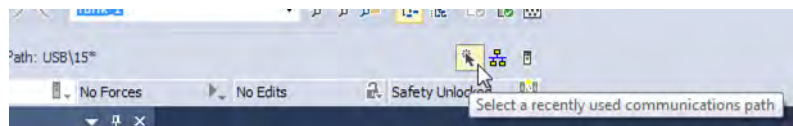
Go Online will use the highlighted node in the Who Active tree, regardless of the setting for Path in Project. For more information on the Who Active dialog box, see the Logix Designer Online Help.

See [Additional Considerations for Going Online with a GuardLogix Controller on page 73.](#)

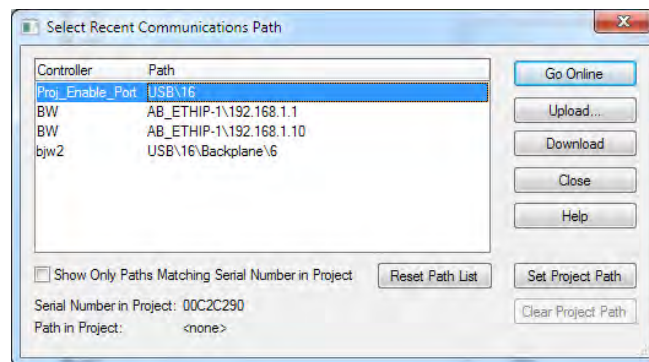
Use a Recent Communication Path

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

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



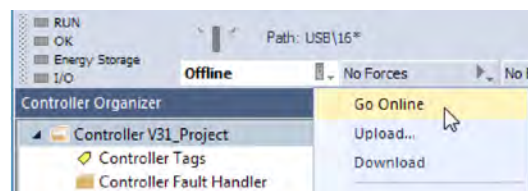
2. On the Select Recent Communications Path dialog box, choose the path.



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

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

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



See [Additional Considerations for Going Online with a GuardLogix Controller on page 73.](#)

Additional Considerations for Going Online with a GuardLogix Controller

Applies to these controllers:

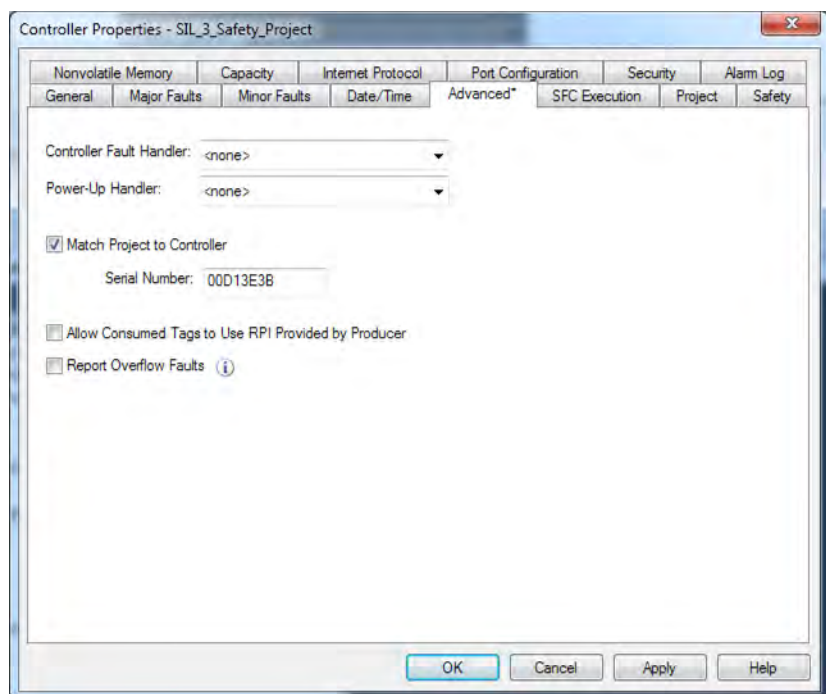
GuardLogix 5580

The Logix Designer application determines whether you can go online with a target controller based on whether the offline project is new or whether changes occurred in the offline project. If the project is new, you must first download the project to the controller. If changes occurred to the project, you are prompted to upload or download. If no changes occurred, you can go online to monitor the execution of the project.

A number of factors affect these processes, including Project to Controller Match feature, the safety status and faults, the existence of a safety signature, the safety-lock/-unlock status of the project and the controller, and the configured safety level disagreeing with the presence or absence of a partner in the chassis.

Match Project to Controller

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



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

Firmware Revision Matching

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

IMPORTANT To update the firmware of the controller, first install a firmware upgrade kit. An upgrade kit ships on a supplemental DVD along with the Studio 5000® environment.

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

Safety Status/Faults

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

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

Safety Signature and Safety-locked and -unlocked Status

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

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

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

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

The existence of a safety signature, and the controller's safety-lock status, determines whether or not a download can proceed.

Table 11 - Effect of Safety-lock and safety signature on Download Operation

Safety-lock Status	Safety Signature Status	Download Functionality
Controller safety-unlocked	safety signature in the offline project matches the safety signature in the controller.	All standard project components are downloaded. Safety tags are reinitialized to the values they had when the safety signature was created. Safety lock status matches the status in the offline project.
	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.
Controller safety-locked	safety signatures match.	If the offline project and the controller are safety-locked, all standard project components are downloaded and safety tags are reinitialized to the values they had when the safety signature was created. 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 GuardLogix Controller

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

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

Table 12 - Connect to the Controller with a Safety Project

If the software indicates	Then
Unable to connect to controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller, select another project file, or choose the Update project serial number checkbox and choose Go Online... to connect to the controller and update the offline project serial number to match the controller.
Unable to connect to controller. The revision of the offline project and the controller's firmware are not compatible.	Choose one of the following options: <ul style="list-style-type: none"> • Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection. IMPORTANT: The online project is deleted. • To preserve the online project, cancel the online process and install a version of the Studio 5000 environment that is compatible with the firmware revision of your controller.
You need to upload or download to go online by using the open project.	Choose one of the following options: <ul style="list-style-type: none"> • Upload to update the offline project. • Download to update the controller project. • Choose File to select another offline project.
Unable to connect in a manner that preserves safety signature. The firmware minor revision on the controller is not compatible with safety signature in offline project.	<ul style="list-style-type: none"> • To preserve the safety signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller. • To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. IMPORTANT: The safety system requires revalidation.
Unable to connect to controller. Incompatible safety signature cannot be deleted while project is safety-locked.	Cancel the online process. You must safety-unlock the offline project before attempting to go online.

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

Download to the Controller

Applies to these controllers:

ControlLogix 5580

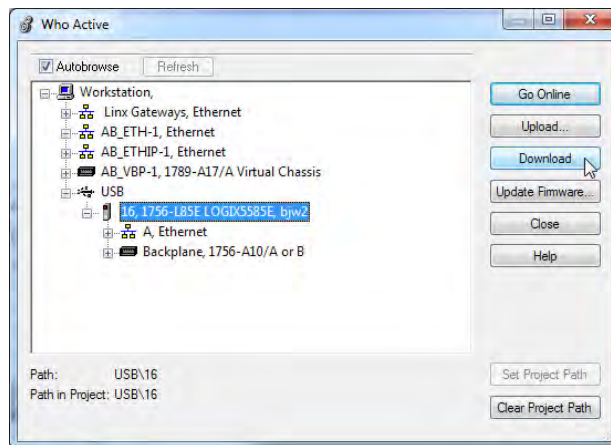
GuardLogix 5580

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

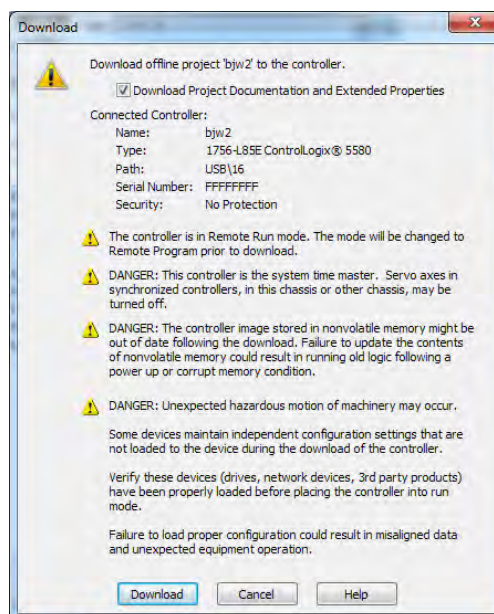
Use Who Active

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

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



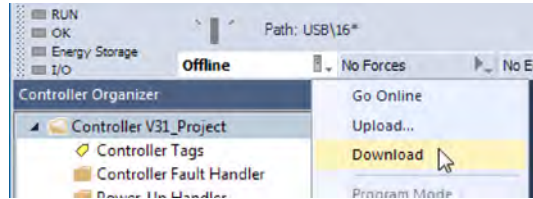
2. After reading the warnings in the Download dialog box, click Download.



Use the Controller Status Menu

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

Figure 17 - Download Via the Controller Status Menu



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

Additional Considerations for Download to a GuardLogix Controller

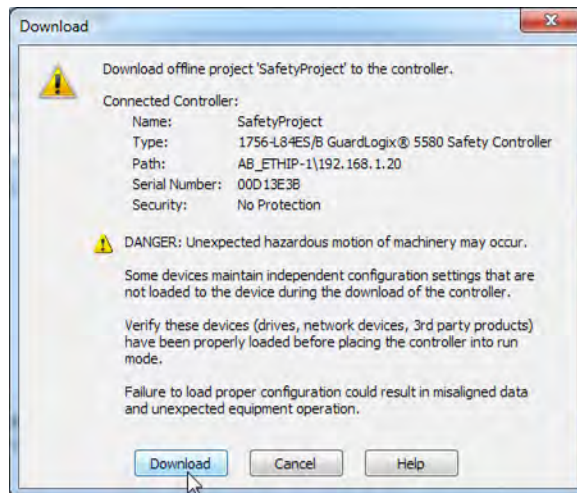
Applies to these controllers:

GuardLogix 5580

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

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

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



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

If the software indicates:	Then:
Unable to download to the controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller or verify that this is the correct controller. If it is the correct controller, check the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number.
Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible.	Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.
Unable to download a SIL 2 application, Safety Partner is Present.	Remove the safety partner.
Unable to download to controller. The safety partner is missing or unavailable.	Cancel the download process. Install a compatible safety partner before attempting to download.
Unable to download to controller. The firmware revision of the safety partner is not compatible with the primary controller.	Update the firmware revision of the safety partner. Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.
Unable to download to controller. Safety partnership has not been established.	Cancel this download process and attempt a new download.
Unable to download to controller. Incompatible safety signature cannot be deleted while the project is safety-locked.	Cancel the download. To download the project, you must safety-unlock the offline project, delete the safety signature, and download the project. IMPORTANT: The safety system requires revalidation.
Cannot download in a manner that preserves the safety signature. Controller's firmware minor revision is not compatible with safety signature in offline project.	<ul style="list-style-type: none"> • If the firmware minor revision is incompatible, to preserve the safety signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project. • To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. IMPORTANT: The safety system requires revalidation.
Unable to download to controller. Controller is locked. Controller and offline project safety signatures do not match.	Choose Unlock. The Safety Unlock for Download dialog box appears. If the Delete Signature checkbox is selected and you choose Unlock, click Yes to confirm the deletion.
Downloading safety signature...	The safety signature is present in the offline project and is downloading.
Reloading safety signature...	The safety signature is present in the offline project and is not downloaded, because a matching signature exists in the controller and is reloaded from there.

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

Upload from the Controller

Applies to these controllers:

ControlLogix 5580

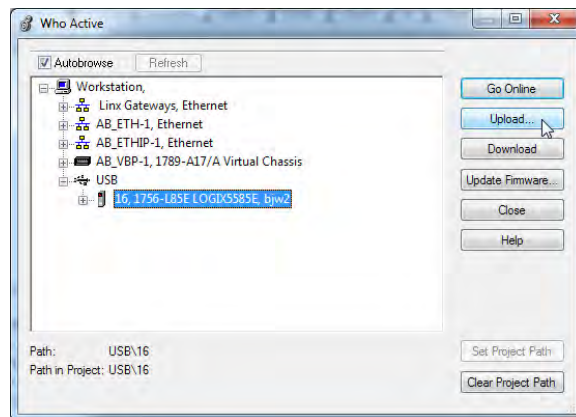
GuardLogix 5580

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

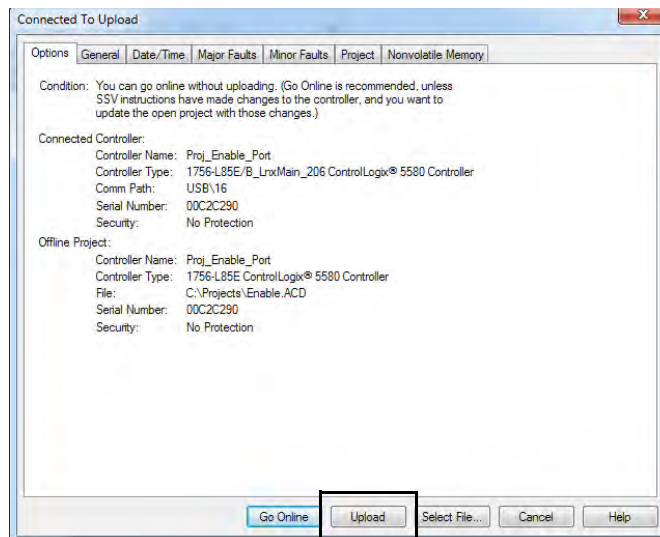
Use Who Active

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

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



2. On the Connected to Upload dialog box, verify that the project is the one you want to upload.
3. Click Upload.



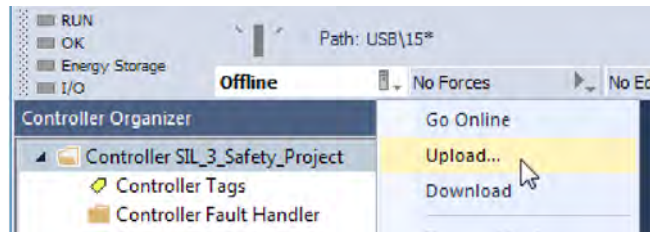
For more information on the Connected To upload dialog box, see the Logix Designer Online Help.

Use the Controller Status Menu

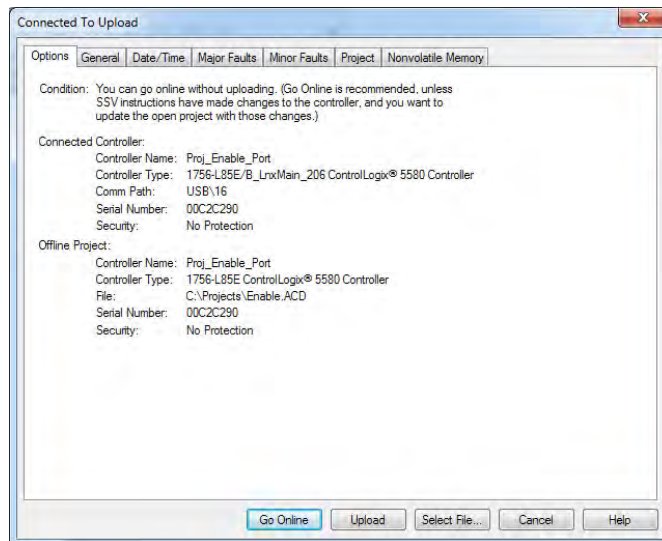
After you have chosen a communication path in the Logix Designer application, you can use the Controller Status menu to upload from the controller.

1. From the Controller Status menu, choose Upload.

Figure 18 - Upload Via the Controller Status Menu



2. On the Connected to Upload dialog box, verify that the project is the one you want to upload.
3. Click Upload.



Additional Considerations for Upload from a GuardLogix Controller

Applies to these controllers:
GuardLogix 5580

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

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

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

Upload Behavior:	Response:
If the project to controller match is enabled, the Logix Designer application checks whether the serial number of the open project and the serial number of the controller match.	<ul style="list-style-type: none"> • Connect to the correct controller or verify that this is the correct controller. • Select a new project to upload into or select another project by choosing Select File. • If it is the correct controller, select the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number.
The Logix Designer application checks whether the open project matches the controller project.	<ul style="list-style-type: none"> • If the projects do not match, you must select a matching file or cancel the upload process. • If the projects match, the software checks for changes in the offline (open) project.
The Logix Designer application checks for changes in the offline project.	<ul style="list-style-type: none"> • If there are no changes in the offline project, you can go online without uploading. Click Go Online. • If there are changes in the open project that are not present in the controller, you can choose to upload the project, cancel the upload, or select another file.
Uploading safety signature...	This message appears during the upload only if a safety signature matching the one in the controller does not exist in the offline project.


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

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

Choose the Controller Operation Mode

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

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

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

Use the keyswitch to Change the Operation Mode

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

When the keyswitch on the controller is set to RUN mode, features like online editing, program downloads, and firmware updates are prohibited. See [Choose the Controller Operation Mode on page 83](#) for a complete list of prohibited features.

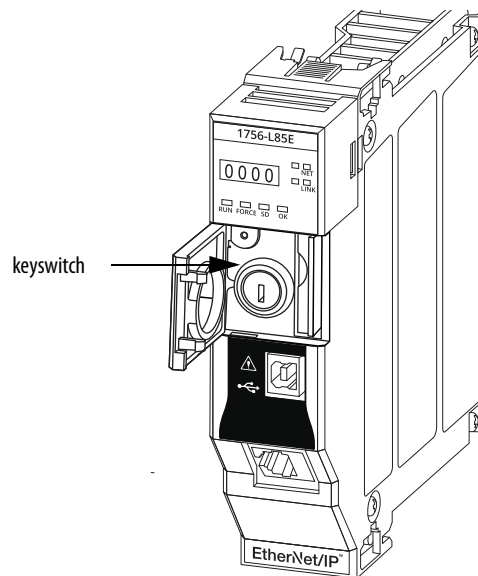
The physical keyswitch can complement other authorization and authentication methods that similarly control user-access to the controller, such as the FactoryTalk® Security service.

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

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

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

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



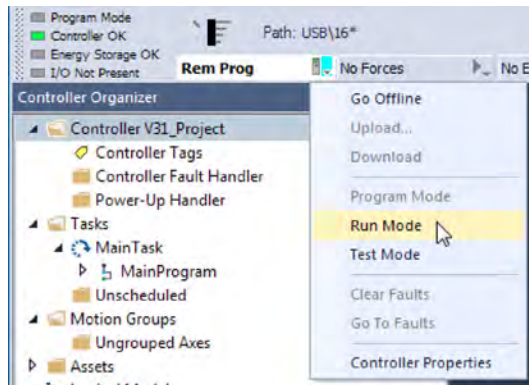
Use the Logix Designer Application to Change the Operation Mode

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

The Controller Status menu lets you specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

Figure 19 - Operation Mode



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

Reset Button

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

You can reset the ControlLogix® and GuardLogix controllers, and the 1756-L8SP Safety Partner, with the reset button. The reset button is only read during a power-up or restart. If you press the reset button at another time, it has no effect.

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

A controller has two stages of reset:

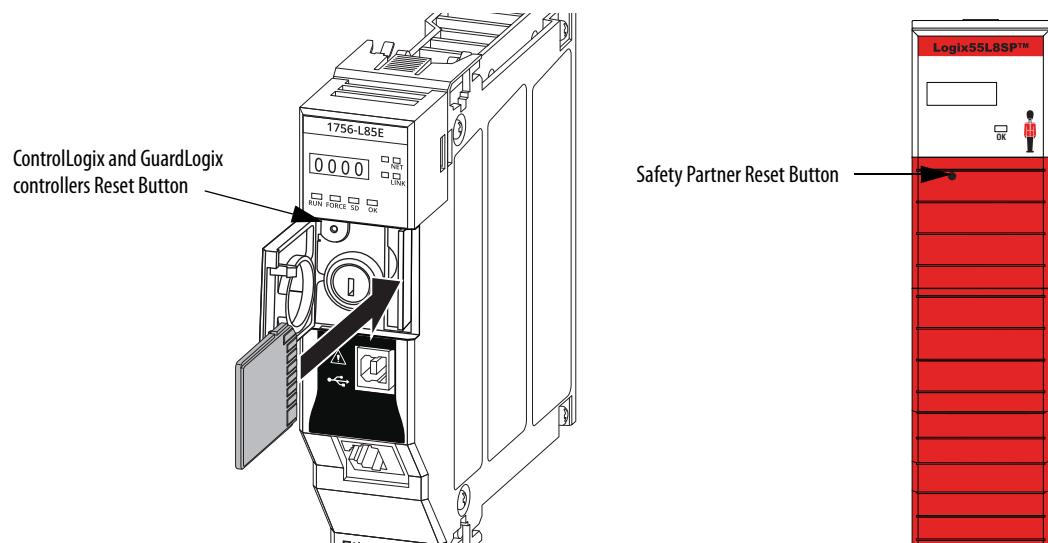
- A Stage 1 reset clears the application program and memory, but retains the IP address and all network settings. A stage 1 reset occurs only if the controller contains a user application. See [Stage 1 Reset on page 87](#).
- A Stage 2 reset returns the controller to out-of box settings (including firmware), and clears all network settings. A stage 2 reset occurs only if the controller does not contain a user application, and the current controller firmware is not a 1.x version. See [Stage 2 Reset on page 88](#).

The Safety Partner reset returns the safety partner to out-of box settings (including firmware). See [Safety Partner Reset on page 89](#).

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



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



Stage 1 Reset

The stage 1 reset:

- Clears the application program.
- Retains the network settings for the embedded Ethernet port.
- Retains APR (motion position info) information.
- Retains all PTP configuration (Time Synchronization) parameters.
- Retains Wall Clock Time within the energy retention capability of the module.
- Creates a timestamped entry in the Controller Log that a Stage 1 Reset event has occurred.
- Resets the controller to begin the controller start up process.
- Prevents the controller from loading firmware or software from the SD card on this first start up after the reset, regardless of the setting on the SD card, and without modifying the SD card contents (the write-protect setting is irrelevant). An SD card will reload (if configured to do so) on subsequent powerup situations.
- Enables the Ethernet Port, if it was previously disabled.

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

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

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

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

- Download the project from the Logix Designer application - For more information, see [Download to the Controller on page 77](#)
- 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:

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

Follow these steps to perform a Stage 2 reset:

1. Power down the controller.
2. Remove the key from the keyswitch.
3. Open the front door on the controller.
4. Remove the SD card.
5. Use a small tool with a diameter of a paper clip, to press and hold the reset button. The button is recessed behind the panel.
6. While holding in the reset button, power up the controller.
7. Continue to hold the reset button while the 4-character display cycles through DFLT, 4, 3, 2, 1, Factory Default.
8. After Factory Default appears, release the reset button.
9. On your workstation, delete all of the files on the SD card.
10. Power down the controller.
11. Reinstall the SD card.
12. Powerup the controller.
13. Verify that the controller is at firmware revision 1.x, and the controller is set to DHCP.

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

- Configure the Ethernet ports, set the desired EtherNet/IP mode, and set the controller IP address configuration. For more information, see [Connect to a Controller on page 51](#).
- Update the firmware revision - For more information, see [Update Controller Firmware on page 55](#).
- Download a Logix Designer application project to the controller in one of these ways:
 - Download the project from the Logix Designer application - For more information, see [Download to the Controller on page 77](#).
 - Cycle power on the controller to load a project from the SD card. This option works only if the project stored on the SD card is configured to load the project on powerup.

Safety Partner Reset

Follow these steps to perform a safety partner reset:

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

Notes:

Use the Secure Digital Card

Topic	Page
Considerations for Storing and Loading a Safety Project	93
Store to the SD Card	94
Load from the SD Card	98
Other Secure Digital Card Tasks	100

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers ship with a Secure Digital (SD) card installed. We recommend that you leave the SD card installed, so if a fault occurs, diagnostic data is automatically written to the card. Rockwell Automation can then use the data to help investigate the cause of the fault.

We recommend that you use the SD cards available from Rockwell Automation:

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

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

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

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

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

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

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

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

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

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

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

Considerations for Storing and Loading a Safety Project

Applies to these controllers:

GuardLogix 5580

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

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

If no application project exists in the controller, you can save only the firmware of the safety controller if a valid partnership exists. A firmware-only load does not clear a Safety Task Inoperable condition.

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

- Safety tags are stored with the value they had when the signature was first created.
- Standard tags are stored with their current values.
- The current safety signature is saved.

When you store a safety application project on an SD card, Rockwell Automation recommends you select Program (Remote Only) as the Load mode, that is, the mode that the controller enters after a project is loaded from the SD card.

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

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

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

Store to the SD Card

Applies to these controllers:

ControlLogix 5580

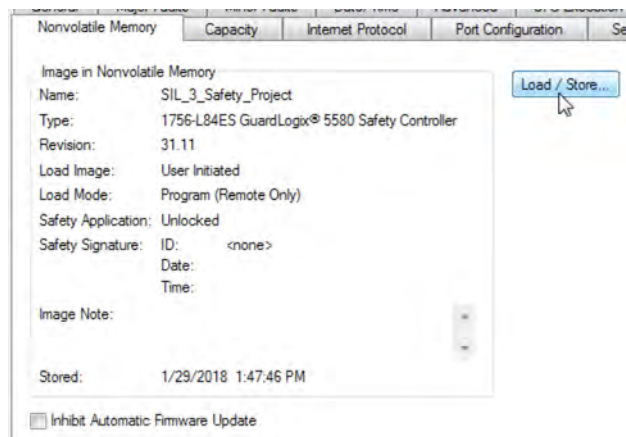
GuardLogix 5580

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

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

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

1. Make sure that the controller is online in Program mode or Remote Program mode.
2. Right-click the controller name and choose Properties.
3. On the Nonvolatile Memory tab, click Load/Store.



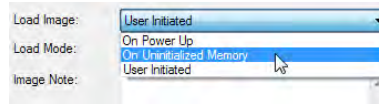
TIP If Load/Store is dimmed (unavailable), verify the following:

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

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

 Nonvolatile memory not present.

4. Change the Load Image properties according to your application requirements.



This table describes the Load Image options.

Table 13 - Load Image Options

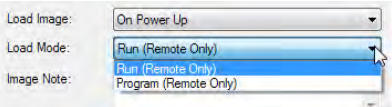
If you want to load the project	Then select this Load Image option	Notes	Safety Considerations
Whenever you turn on or cycle power	On Power Up	<ul style="list-style-type: none"> During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory. The controller loads the stored project and firmware at every powerup regardless of the firmware or application project on the controller. You can always use the Studio 5000 Logix Designer® application to load the project. 	<ul style="list-style-type: none"> For a safety application, On Power Up loads whether or not the controller is safety-locked or there is a safety signature.
Whenever there is no project in the controller and you turn on or cycle chassis power	On Uninitialized Memory	<ul style="list-style-type: none"> If the project has been cleared from memory, this option loads the project back into the controller on power up. The controller updates the firmware on the controller, if required. The application project stored in nonvolatile memory is also loaded and the controller enters the selected mode, either Program or Run. You can always use the Logix Designer application to load the project. 	<ul style="list-style-type: none"> The controller also updates the firmware on the safety partner, if required.
Only through the Logix Designer application	User Initiated	<ul style="list-style-type: none"> If the controller type as well as the major and minor revisions of the project in nonvolatile memory match the controller type and major and minor revisions of the controller, you can initiate a load. 	<ul style="list-style-type: none"> You can initiate a load, regardless of the Safety Task status. You can load a project to a safety-locked controller only when the safety signature of the project stored in nonvolatile memory matches the project on the controller. If the signatures do not match or the controller is safety-locked without a safety signature, you are prompted to first unlock the controller. IMPORTANT: When you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety signature are set to the values contained in nonvolatile memory once the load is complete. If the firmware on the primary controller matches the revision in nonvolatile memory, the safety partner firmware is updated, if required, the application stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the Program mode.

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

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

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

- Change the Load Mode properties according to your application requirements.

If you want the controller to go to this mode after loading	Then choose	Menu Items
Program	Program (remote only)	
Run	Run (remote only)	

IMPORTANT Safety Consideration

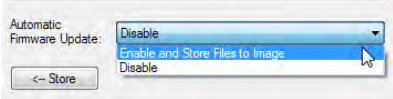
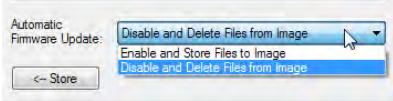
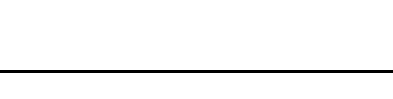
Rockwell Automation recommends that you use Program (Remote Only), when you set the Load Mode for a safety application project.

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

IMPORTANT Safety Consideration

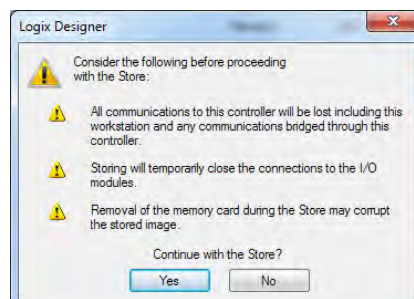
Some Safety I/O devices do not support the Firmware Supervisor feature. For example, Safety I/O devices on DeviceNet® networks and POINT Guard I/O™ modules do not support the Firmware Supervisor feature.

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

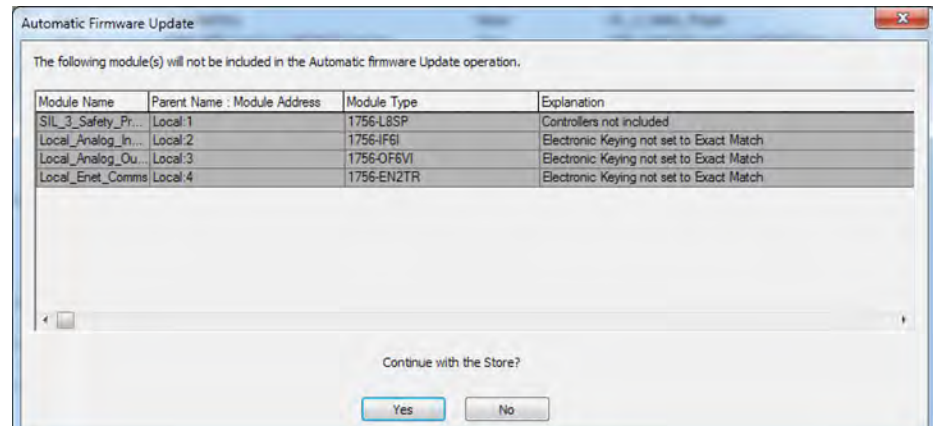
Setting	Description	Menu Items
Disable	Disables any automatic firmware updates. This item only appears in the menu when you initially save the image.	
Enable and Store Files to Image	Enables automatic firmware updates for I/O devices in the configuration tree of the controller. Saves I/O device firmware and controller firmware to the image. Only I/O devices that are configured for Exact Match Keying will participate in the Automatic Firmware Update process. ⁽¹⁾	
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 image. This item only appears in the menu on subsequent saves of the image.	

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

- Click Store.
- Click Yes in the confirmation dialog box that appears.



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



IMPORTANT Do not remove the SD card while the controller is reading from, or writing to, the card. If you remove the card during either activity, the data on the card or controller can become corrupt. Additionally, the controller firmware at the time when the card is removed can become corrupted. Leave the card in the controller until the OK status indicator turns solid green.

9. On the Automatic Firmware Update dialog box, click Yes.

The project is saved to the SD card as indicated by the controller status indicators.

These indications show the store status

While the store is **in progress**, the following occurs:

- OK indicator is flashing green
- SD indicator is flashing green
- Saving... Do Not Remove SD Card is shown on the status display
- A dialog box in the Logix Designer application indicates that the store is in progress
- Controller Resets
- SAVE is shown on the status display

When the store is **complete**, the following occurs:

- The controller resets.

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

Load from the SD Card

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

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

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

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

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

Controller Power-up

This table shows what happens at power up when you insert an SD card that contains an image into a controller.

Image Setting	Controller is in out-of-box condition (v1.x firmware)	Firmware > 1.x and internal non-volatile memory is not valid ⁽²⁾	Firmware > 1.x and internal non-volatile memory is valid ⁽²⁾
User Initiated	Loads Firmware Only ⁽¹⁾	Does Nothing	Does Nothing
On Power Up	Loads both Firmware and Application	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application 	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application
On Uninitialized Memory	Loads both Firmware and Application ⁽¹⁾	<ul style="list-style-type: none"> • Loads Firmware if there is a revision mismatch • Loads Application 	Does Nothing

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

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

User-initiated Action

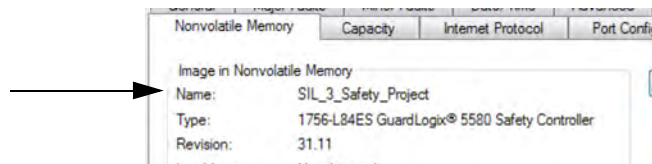
IMPORTANT For an out-of-box controller that uses firmware revision 1.xx, you must manually update the controller to the required firmware revision before you can load a project on the controller.

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

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

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

1. Open the Controller Properties, and click the Nonvolatile Memory tab.
2. On the Nonvolatile Memory tab, verify that the project listed next to Name: is the project that you want to load.

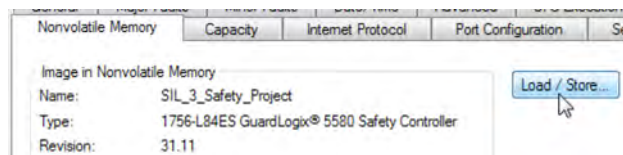


TIP If no project is stored on the SD card, a message in the lower-left corner of the Nonvolatile Memory tab indicates that an image (or project) is not available as shown here.

 No image in the nonvolatile memory.

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

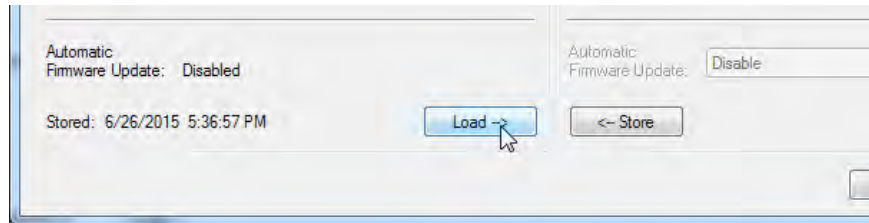
3. Click Load/Store.



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

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

4. Click Load.



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

Table 14 - These indications show the load status

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

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

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

Other Secure Digital Card Tasks

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

You can perform these tasks with the SD card:

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

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

Manage Controller Communication

Topic	Page
Connection Overview	101
Nodes on an EtherNet/IP Network	102
Controller Communication Interaction with Control Data	104
Produce and Consume (Interlock) Data	105
Send and Receive Messages	107
Socket Interface	108
Simple Network Management Protocol (SNMP)	112

Connection Overview

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

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

Nodes on an EtherNet/IP Network

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

When configuring your control system, you must account for the number of EtherNet/IP™ nodes you include in the I/O configuration tree in your project. [Table 15](#) shows the maximum number of EtherNet/IP nodes supported for each controller.

With firmware revision 29 and later, the Ethernet Nodes field on the Controllers Properties Capacity tab keeps a running count as you add EtherNet/IP nodes to the I/O configuration tree. See [Figure 20 on page 103](#).

Table 15 - Maximum Number of Ethernet/IP Nodes Supported

System	Cat. No. ^{(1) (2)}	Version 28	Version 29	Version 30	Version 31 or later
ControlLogix®	1756-L81E, 1756-L81EK, 1756-L81E-NSE, 1756-L81EXT, 1756-L81EP	—	60	100	100
	1756-L82E, 1756-L82EK, 1756-L82E-NSE, 1756-L82EXT	—	80	175	175
	1756-L83E, 1756-L83EK, 1756-L83E-NSE, 1756-L83EXT, 1756-L83EP	100	100	250	250
	1756-L84E, 1756-L84EK, 1756-L84E-NSE, 1756-L84EXT	—	150	250	250
	1756-L85E, 1756-L85EK, 1756-L85E-NSE, 1756-L85EXT, 1756-L85EP	300	300	300	300
GuardLogix®	1756-L81ES, 1756-L81ESK	—	—	—	100
	1756-L82ES, 1756-L82ESK	—	—	—	175
	1756-L83ES, 1756-L83ESK	—	—	—	250
	1756-L84ES, 1756-L84ES, 1756-L84ESK	—	—	—	250

(1) This table also applies to conformal coated catalog numbers. Controller catalog numbers followed by a “K” indicate a conformal coated model.

(2) ControlLogix NSE controllers, ControlLogix-XT controllers, and ControlLogix Process controllers are available with version 33 or later.

IMPORTANT EtherNet/IP communication modules in the local chassis with the controller do not count as nodes, but EtherNet/IP devices connected to the communication modules do count as nodes. See [Figure 20 on page 103](#).

Devices Included in the Node Count

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

- Remote communication adapters
- Remote controllers.
- Devices with an embedded EtherNet/IP port, such as I/O modules, drives, and linking devices
- EtherNet/IP devices connected to a communication module in the local chassis, even though the communication module in the local chassis does not count as a node. See [Figure 20 on page 103](#).
- HMI devices that are included in the I/O configuration section, for example, PanelView™ Plus terminals.
- Third-party devices that are directly connected to the EtherNet/IP network.

Devices Excluded from the Node Count

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

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

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

This example shows four nodes in the I/O tree.

Figure 20 - EtherNet/IP Nodes Example

The screenshot displays the I/O Configuration tree on the left and the Controller Properties dialog box on the right. The I/O tree shows a hierarchy of modules under 'I/O Configuration'. Arrows point to specific modules with labels:

- Not a node. Module is in local chassis. (points to 1756-IB16 Local_Input_1)
- Node (points to 1734-AEN2TR Remote_Comm_1)
- Not a node. Module is in local chassis. (points to 1756-EN2T Local_Comm_2)
- Node (points to 2097-V32PR0/A Drive_2)
- Node (points to 1756-L85E V31_Test)
- Node (points to 2097-V33PR5-LM Main)

The Controller Properties dialog box shows the Capacity tab. A table titled 'Ethernet Nodes' is highlighted:

Ethernet Nodes	
Recommended Maximum:	300 nodes
Used:	4 nodes

Controller Communication Interaction with Control Data

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

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

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

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

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

[Table 16](#) highlights the controllers behavior.

Table 16 - ControlLogix 5580 and GuardLogix 5580 Controller Behavior

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

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

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

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

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

Table 17 shows two data elements added to a structure for data integrity checking: Start Data and End Data. We recommend that the controller validates the Start Data value and the End Data value match before the controller acts on My_Recipe1.

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

Table 17 - 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

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

Produce and Consume (Interlock) Data

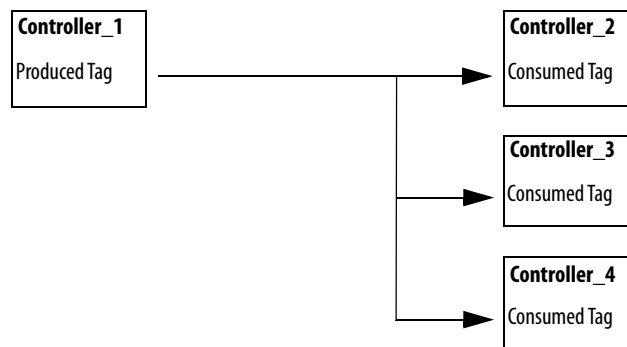
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers let you produce (transmit) and consume (receive) controller-scoped tags. ControlLogix 5580 controllers and GuardLogix 5580 controllers produce the same standard tag through both the Ethernet port and the backplane, and consumer counts apply to the total consumers from both ports.

Figure 21 - Illustration of Produced and Consumed Tags



[Table 18](#) describes the system-shared tags.

Table 18 - Produced and Consumed Tag Definitions

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

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

Produced and consumed tags use connections of the controller and the communication modules being used. For information on Produced/Consumed Safety Tags for GuardLogix 5580 controllers, see [Produced/Consumed Safety Tags on page 177](#).

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

Table 19 - ControlNet Connections

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

Requested Packet Interval (RPI) of Multicast Tags

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

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

Send and Receive Messages

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

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

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

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

Each message uses one connection out of the controller, regardless of how many devices are in the message path.

Table 20 - Message Types

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

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

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

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

Determine Whether to Cache Message Connections

When you configure a MSG instruction, you can choose whether to cache the connection. Use [Table 21](#) to determine options for caching connections.

Table 21 - Options for Caching Connections

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

TIP Cashed connections transfer data faster than uncashed connections. The controllers can cache 256 messages and trigger 256 messages simultaneously.

Socket Interface

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controller can use socket interfaces to communicate with Ethernet devices that do not support the EtherNet/IP application protocol. The socket interface is implemented via the Socket Object. The controller communicates with the Socket Object via MSG instructions. MSG instructions that configure and operate the socket interface must be configured as Unconnected, and use the Message to Self path. To communicate with another device, you must understand the application protocol of the other device.

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

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

Simple Network Management Protocol (SNMP)

SNMP enables the controller to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. SNMP is disabled on the controller by default.

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

Use a CIP Generic MSG to Enable SNMP on the Controller

1. Add a MSG instruction to your program.

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

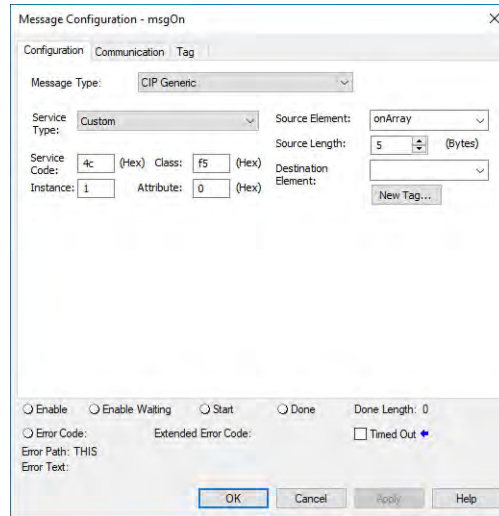
2. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Custom
 - Service Code - 4c
 - Instance - 1
 - Class - f5
 - Attribute - 0
 - Source Element - Controller tag of USINT[5] data type.

In this example, the controller tag is named onArray and must match the following graphic.

IMPORTANT The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP will not be enabled.

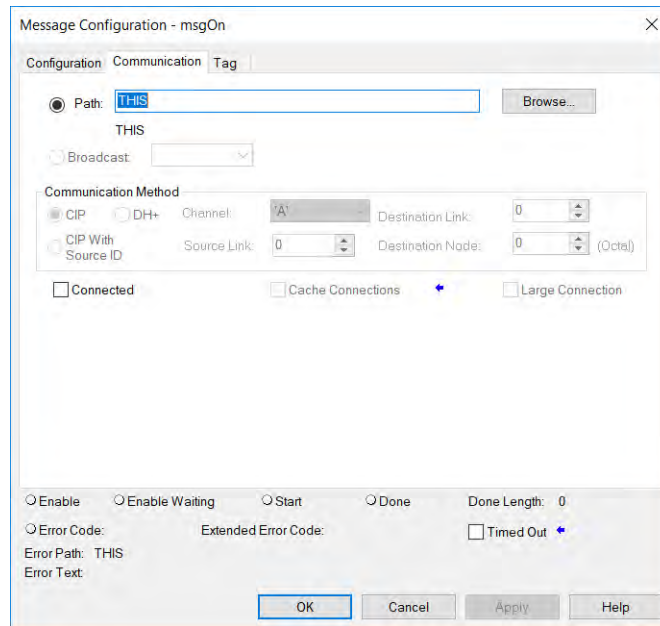
Name	Value	Style	Data Type
onArray	{...}	Decimal	USINT[5]
onArray[0]	1	Decimal	USINT
onArray[1]	161	Decimal	USINT
onArray[2]	0	Decimal	USINT
onArray[3]	17	Decimal	USINT
onArray[4]	1	Decimal	USINT

– Source Length - 5



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

IMPORTANT Messages to THIS must be unconnected messages.



Use a CIP Generic MSG to Disable SNMP on the Controller

1. Add a MSG instruction to your program.

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

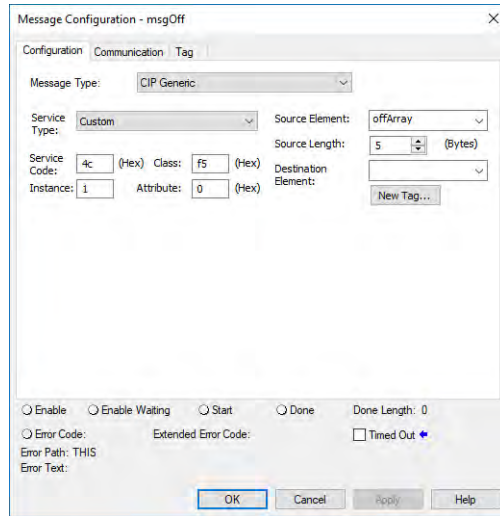
2. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Custom
 - Service Code - 4c
 - Instance - 1
 - Class - f5
 - Attribute - 0
 - Source Element - Controller tag of USINT[5] data type.

In this example, the controller tag is named offArray and must match the following graphic.

IMPORTANT The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, SNMP will not be disabled.

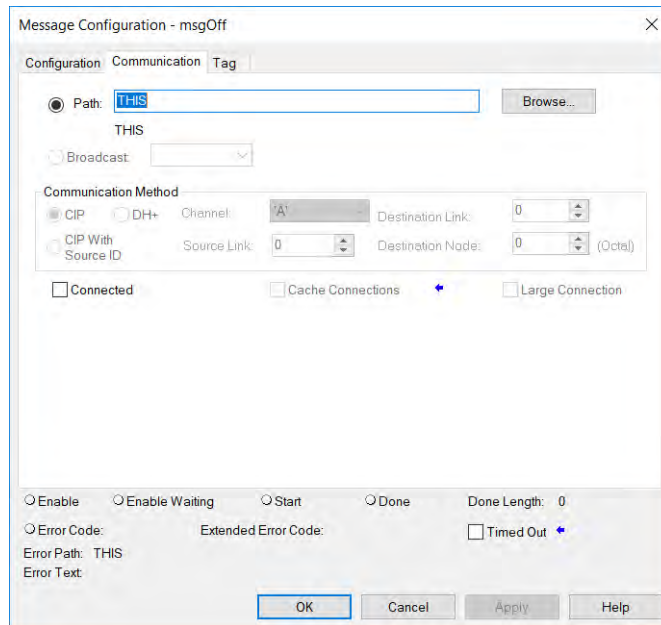
offArray	[...] Decimal	USINT[5]
▸ offArray[0]	1 Decimal	USINT
▸ offArray[1]	161 Decimal	USINT
▸ offArray[2]	0 Decimal	USINT
▸ offArray[3]	17 Decimal	USINT
▸ offArray[4]	0 Decimal	USINT

– Source Length - 5



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

IMPORTANT Messages to THIS must be unconnected messages.



Standard I/O Modules

Topic	Page
Selecting ControlLogix I/O Modules	113
Local I/O Modules	115
Remote I/O Modules	120
Add to the I/O Configuration While Online	127
Determine When Data is Updated	129

Selecting ControlLogix I/O Modules

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

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

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

Electronic Keying

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

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

The following Electronic Keying options are available.

Keying Option	Description
Compatible Module	<p>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:</p> <ul style="list-style-type: none"> • Same catalog number • Same or higher Major Revision • Minor Revision as follows: <ul style="list-style-type: none"> – If the Major Revision is the same, the Minor Revision must be the same or higher. – If the Major Revision is higher, the Minor Revision can be any number.
Disable Keying	<p>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.</p> <p>ATTENTION: Be cautious when using Disable Keying; if used incorrectly, this option can lead to personal injury or death, property damage, or economic loss.</p> <p>We strongly recommend that you do not use Disable Keying.</p> <p>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.</p>
Exact Match	<p>Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.</p>

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.

More Information

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

Local I/O Modules

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

[Table 22](#) lists the available ControlLogix chassis and the number of slots available with each.

Table 22 - ControlLogix and ControlLogix-XT™ Chassis and Slots

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

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

Add Local I/O to the I/O Configuration

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

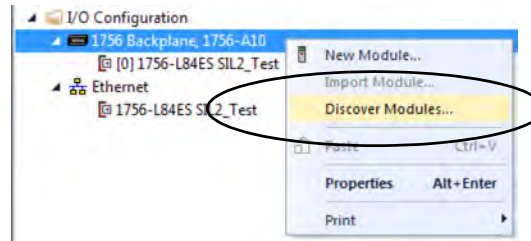
There are two methods to add local I/O modules to the project:

- [Discover Modules on page 116](#)
- [New Module on page 118](#)

Discover Modules

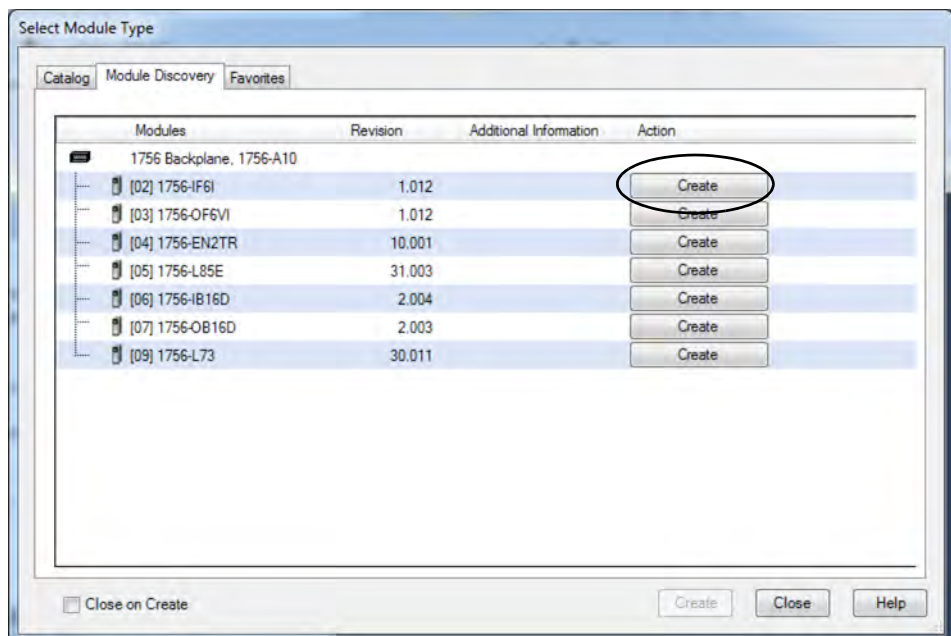
To use Discover Modules to add a local I/O module, complete these steps.

1. Go online with your Studio 500 Logix Designer® application.
2. Right-click the 1756 Backplane, and choose Discover Modules.

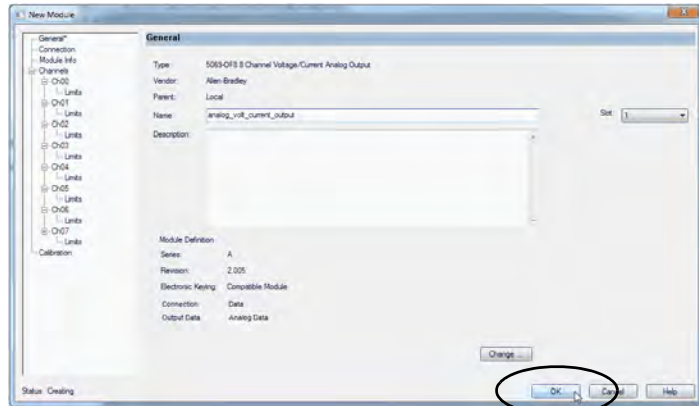


The Logix Designer application automatically detects available modules that are installed in the system.

3. At the Select Module Type window, click Create to add a discovered module to your project.

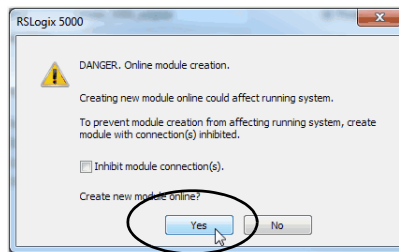


- At the New Module window, configure the module properties and click OK.



- At the warning dialog box, click Yes.

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



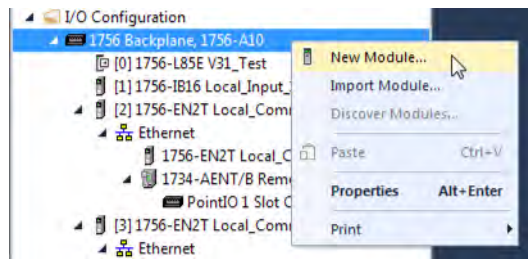
- Close the Select Module Type dialog box.

To add additional local I/O modules, complete one of the following:

- If you cleared the Close on Create checkbox when you created the first I/O module, repeat steps [3...6](#).
- If you did not clear the Close on Create checkbox when you created the first I/O module, repeat steps [2...6](#).

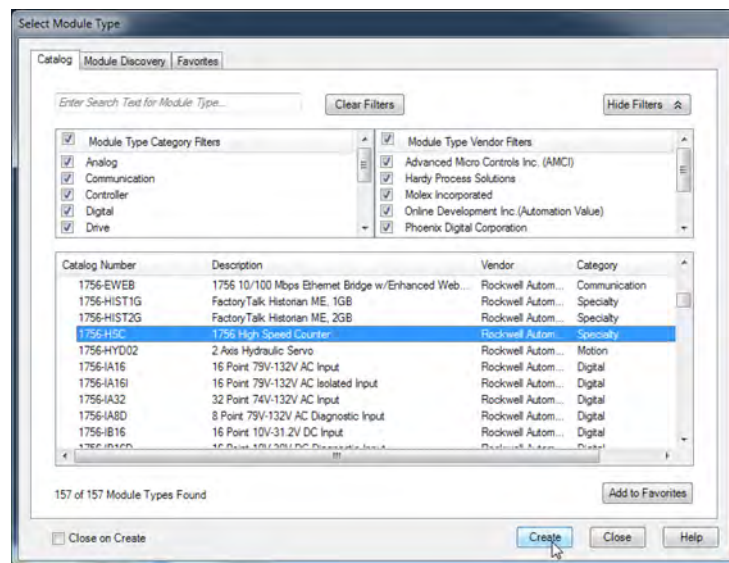
New Module

1. Right-click the backplane, and choose New Module.



2. Select the I/O module and click Create.

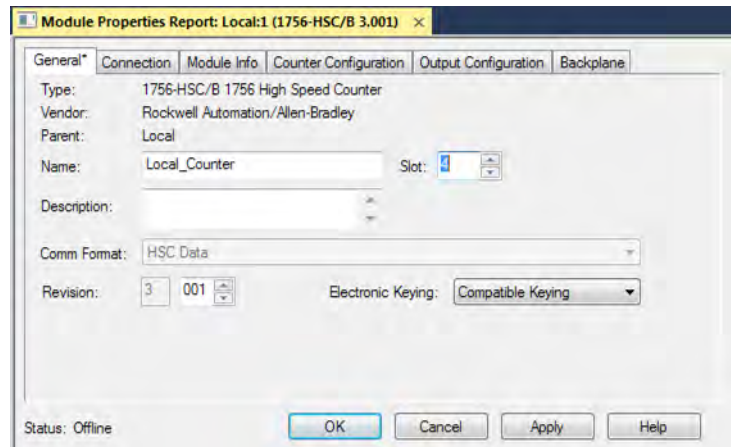
TIP Use the filters to reduce the list of modules to choose from.



The New Module dialog box appears.

3. Configure the module and click OK.

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



To add additional local I/O modules, complete one of the following:

- If you cleared the Close on Create checkbox when you created the first I/O module, repeat steps [2...3](#).
- If you did not clear the Close on Create checkbox when you created the first I/O module, repeat steps [1...3](#).

See the [Additional Resources](#) section in the preface for more information if you are designing your ControlLogix System for any of the following modules:

- Analog I/O
- Configurable flowmeter
- Digital I/O
- HART analog I/O
- High-speed analog I/O
- High-speed counter
- Low-speed counter
- Programmable limit switch

Remote I/O Modules

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

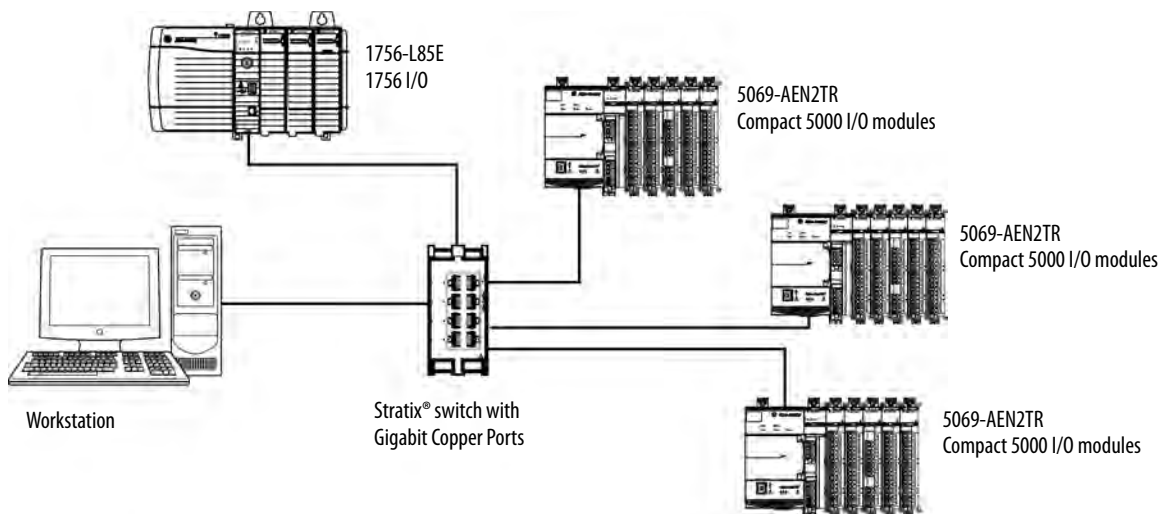
- Compact 5000™ I/O modules in a remote bank using a 5069-AEN2TR or similar adapter
- 1756 I/O in a remote chassis via a Network Bridge Module
- Distributed I/O families such as POINT I/O™ or Block I/O™
- On-Machine™ I/O families such as ArmorPOINT® or ArmorBlock® I/O

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

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

For more information about the network configurations that can be used to connect remote I/O, see [Communication Networks on page 35](#).

Figure 22 - ControlLogix 5580 Controller and Remote I/O on a 1 Gbps EtherNet/IP Network

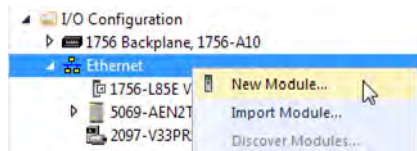


Add Remote I/O to the Ethernet Port on the Controller

If you are adding remote I/O, you can add the I/O modules to the Ethernet port of the controller. To add remote I/O to the I/O Configuration folder in the Logix Designer application, complete these steps.

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

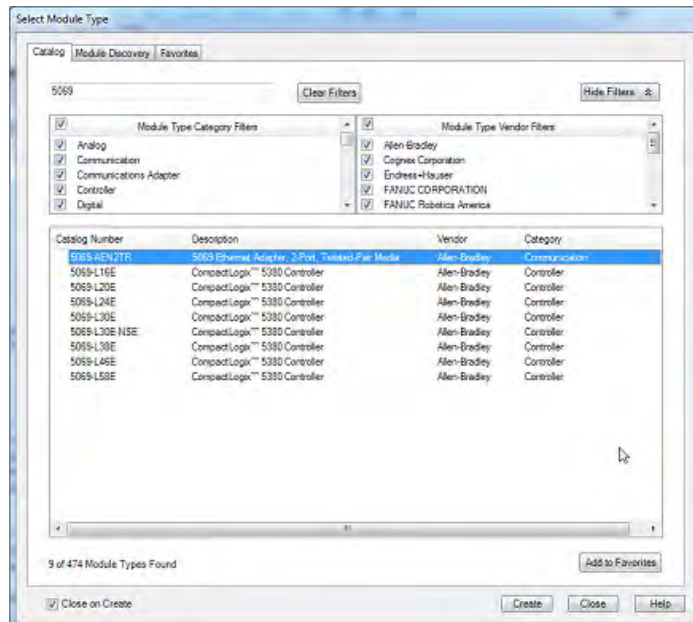
1. In the I/O Configuration tree, right-click Ethernet and choose New Module.



2. Select the remote communication module or EtherNet/IP device.

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

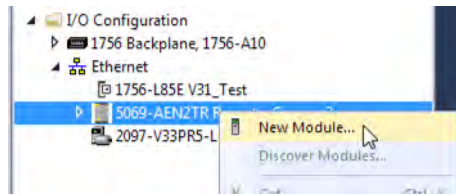
For some modules, the Select Major Revision dialog box can appear. If the dialog box appears, choose the major revision of the module and click OK.



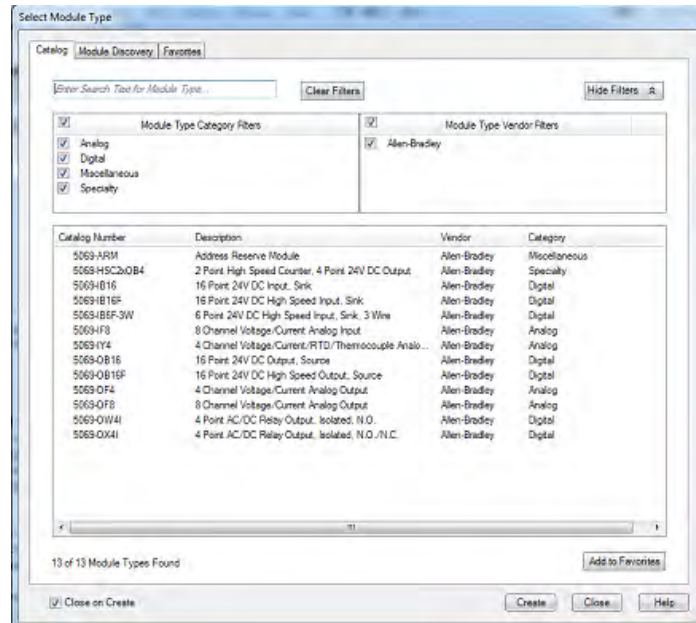
3. Make sure Close on Create is checked.
4. Click Create.
5. Specify the communication module properties according to your network configuration.

For more information about the communication module and network properties, see the [Additional Resources](#) section in the Preface.

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



- Select the I/O module that you want to add and click OK.

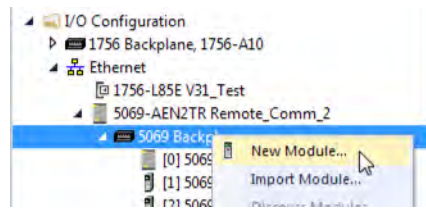


- Make sure Close on Create is checked.
- Click Create.
- Specify the Module Properties according to your module and application.

See the [Additional Resources](#) section in the Preface for more information about the module configuration properties for any of the following modules:

- Analog I/O
- Configurable flowmeter
- Digital I/O
- HART analog I/O
- High-speed analog I/O
- High-speed counter
- Low-speed counter
- Programmable limit switch

11. Add any other I/O modules that you are using in the remote chassis.

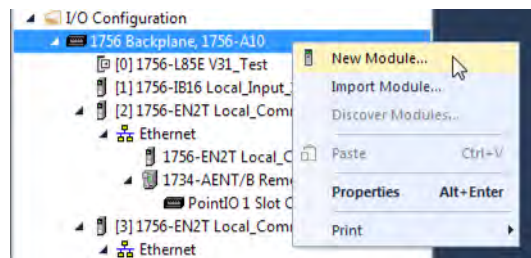


12. Complete steps 1...11 until your remote I/O network and I/O modules are configured.

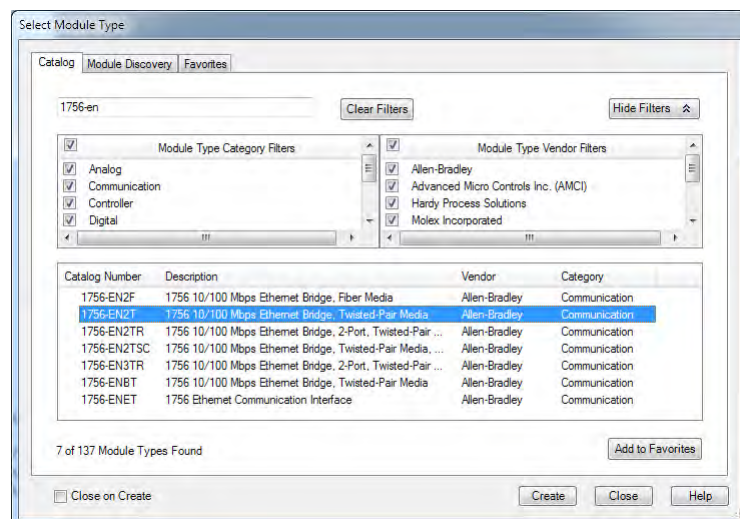
Add Remote I/O to a Local Communication Module

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

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



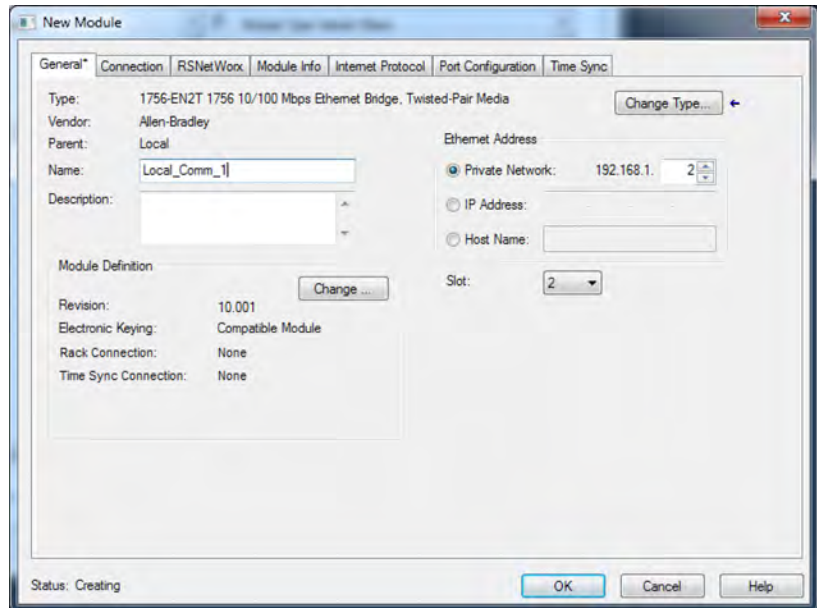
2. Select a communication module.



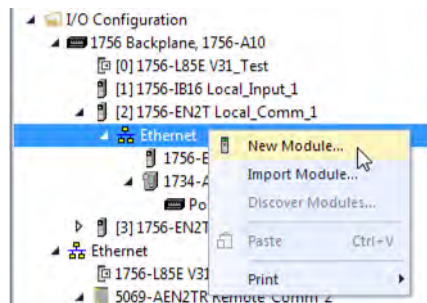
3. Click Create.

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

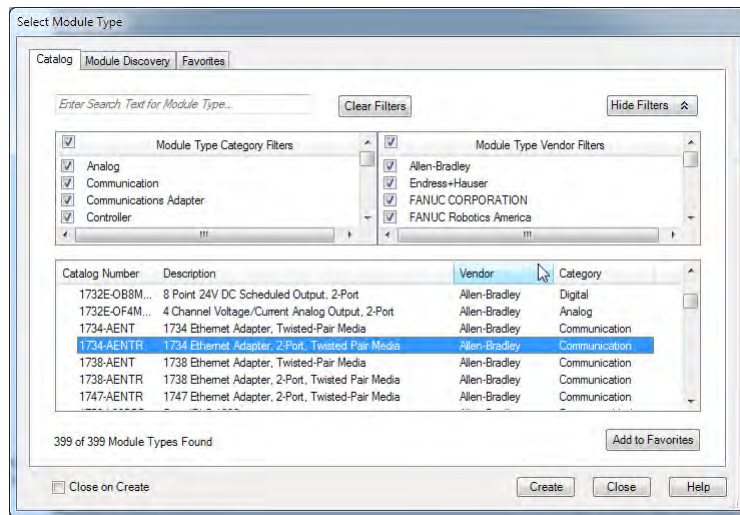
For more information about the communication module and network properties, see the [Additional Resources](#) section in the Preface.



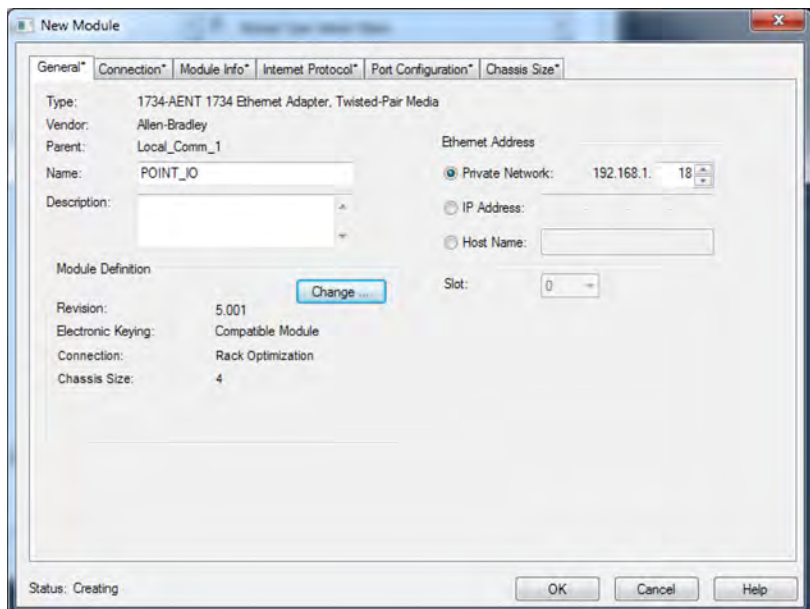
- Click OK.
- Click Close on the Select Module Type dialog box.
- Right-click the communication network under the communication module, and choose New Module.



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

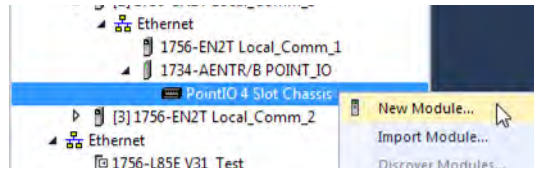


- Click Create.
- Specify the module and connection properties according to your network configuration.



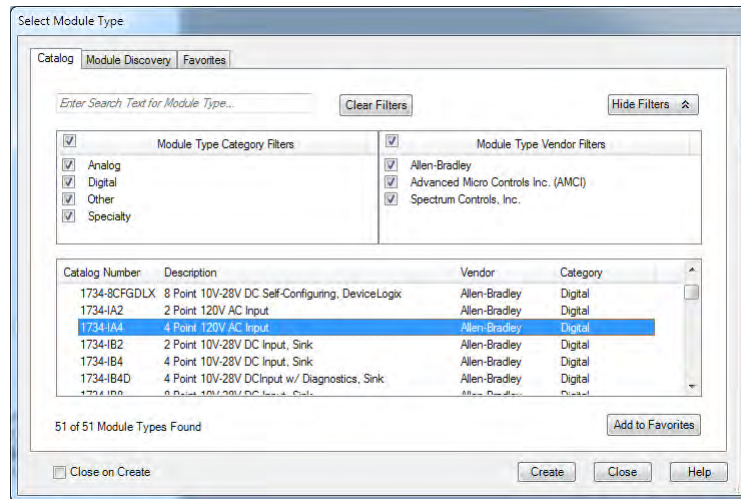
- Click OK.
- Click Close on the Select Module Type dialog box.

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

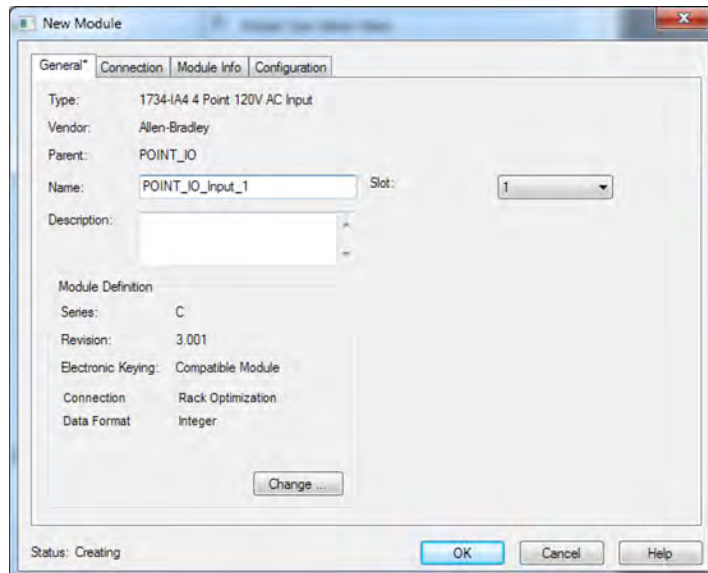


- Select the I/O module that you want to add, and click Create.

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



- Specify the Module Properties according to your module and application. For more information about the module configuration properties, see the user manual for the I/O module you are adding.



- Add any other I/O modules that you are using in this bus.
- Complete steps 1...16 until your remote I/O network and I/O modules are configured.

Add to the I/O Configuration While Online

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

IMPORTANT To add I/O modules when the controller is online, the controller keyswitch must be in the REM or PROG position.

The I/O modules must already be installed in the system. You cannot install the I/O modules when the system is powered.

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

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

To see a list of the available AOP files, go to:

<https://download.rockwellautomation.com/esd/download.aspx?downloadid=addonprofiles>

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

For information on the number of nodes you can have for an EtherNet/IP network, see [Nodes on an EtherNet/IP Network on page 102](#).

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 and Devices that Can be Added While Online

You can add these modules and devices to the I/O configuration while online with Logix Designer, version 28.00.00 or later.

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

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

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

Determine When Data is Updated

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

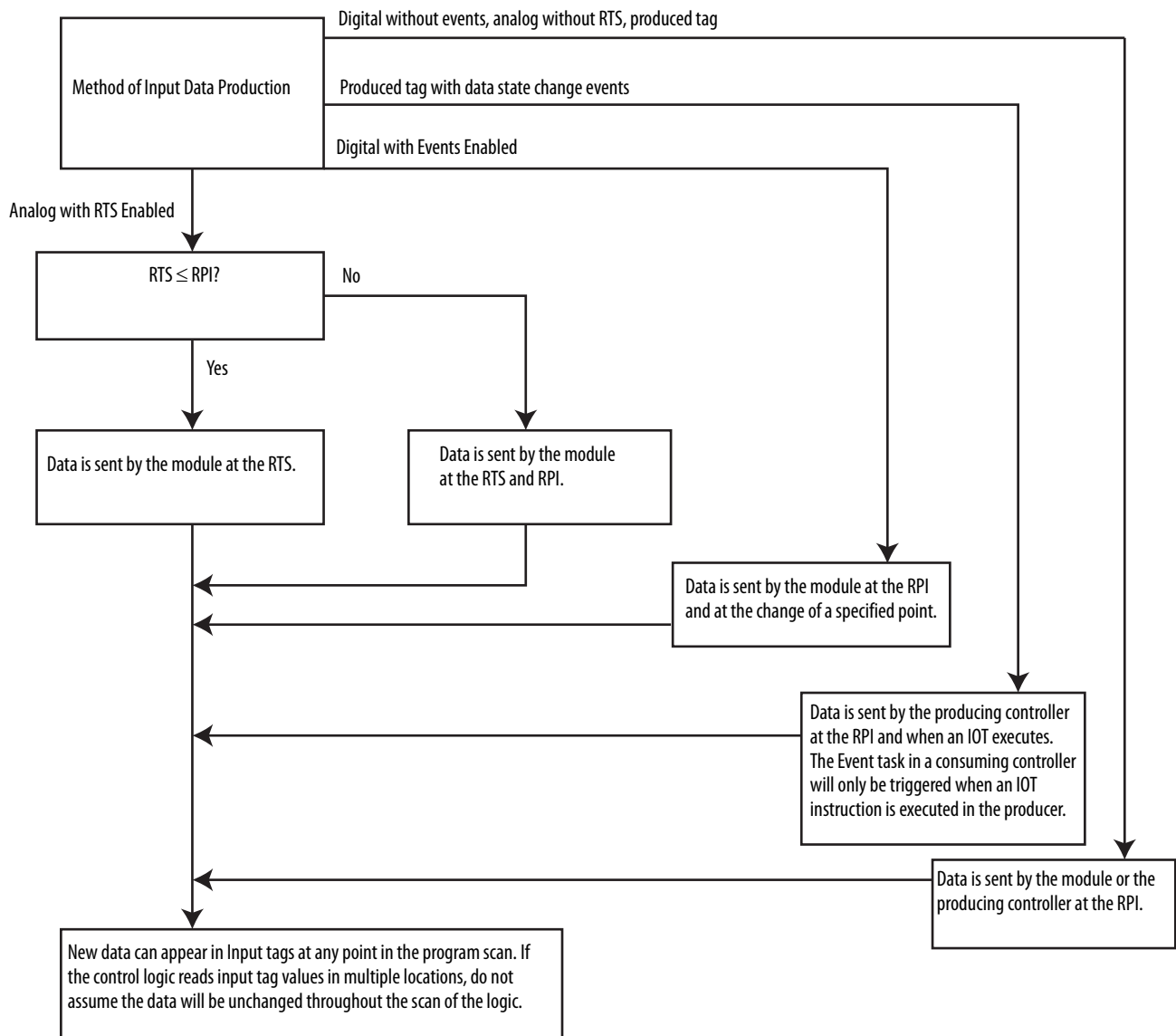
ControlLogix controllers update data asynchronously with the execution of logic. See these flowcharts to determine when a controller, input module, or bridge sends data:

- [Input Data Update Flowchart](#) on this page
- [Output Data Update Flowchart on page 130](#)

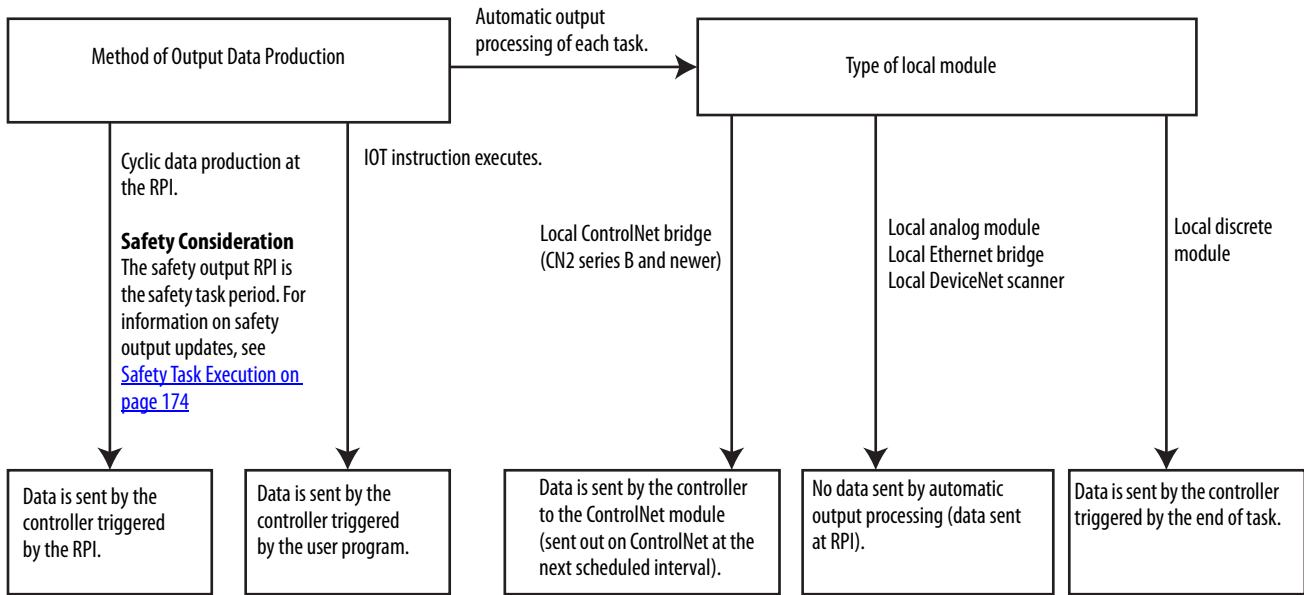
Input Data Update Flowchart

IMPORTANT Safety Consideration

GuardLogix® standard inputs are updated just like ControlLogix standard inputs, but GuardLogix safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution. See [Safety Task Execution on page 174](#).



Output Data Update Flowchart



Safety I/O Devices

Topic	Page
Add Safety I/O Devices	131
Configure Safety I/O Devices	132
Using Network Address Translation (NAT) with CIP Safety Devices	134
Set the SNN of a Safety I/O Device	136
Connection Reaction Time Limit	140
Safety I/O Device Signature	141
I/O Device Address Format	144
Monitor Safety I/O Device Status	144
Replace a Safety I/O Device	145
Reset Safety I/O Device to Out-of-box Condition	143

Add Safety I/O Devices

Applies to these controllers:

GuardLogix 5580

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

- Node address for DeviceNet® networks
- IP address for EtherNet/IP™ networks
- Safety network number (SNN). To set the SNN, see page [136](#).
- Configuration signature. See page [141](#) for information on when the configuration signature is set automatically and when you need to set it.
- Reaction time limit. To set the reaction time limit, see page [140](#).
- Safety input, output, and test parameters complete the module configuration.

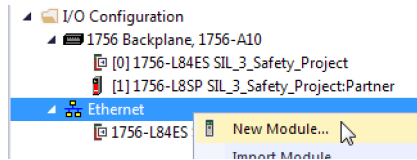
IMPORTANT You cannot add Safety I/O Devices while online with the controller.

Configure Safety I/O Devices

Add the safety I/O device to the communication module under the I/O Configuration folder of the controller project.

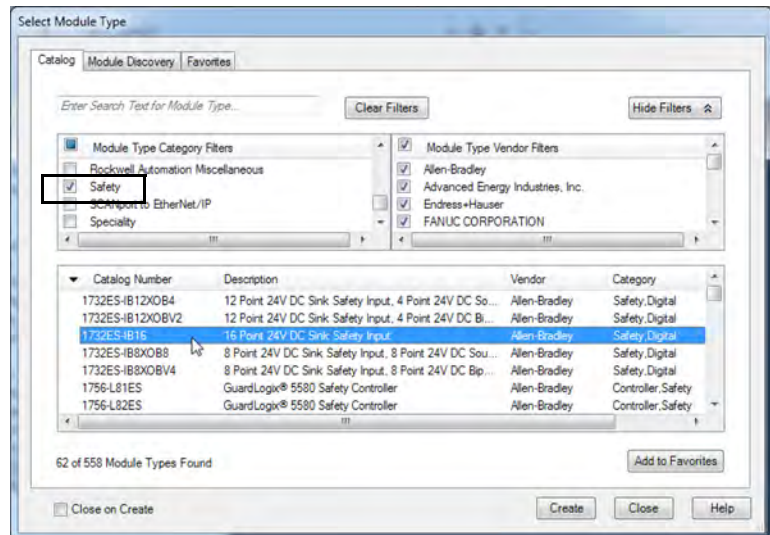
TIP Some safety I/O devices support both standard and safety data. The Module Definition defines what data is available.

1. Right-click the network, and choose New Module.

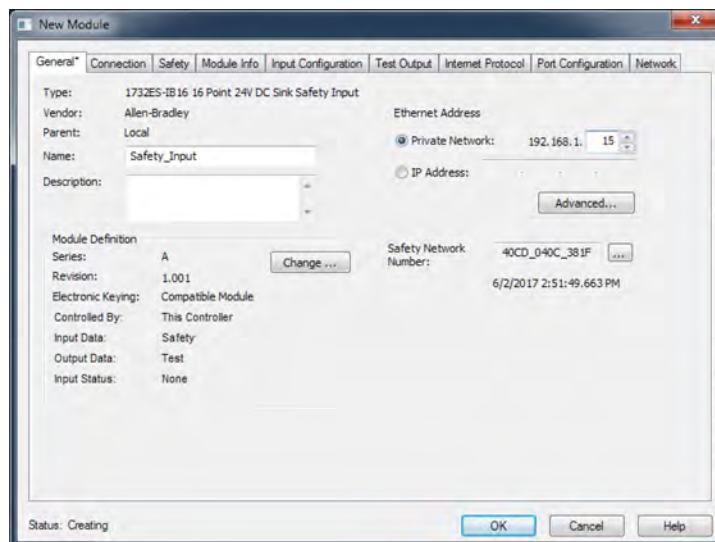


2. From the Catalog tab, select the safety I/O device.

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



3. Click Create.
4. Type a name for the new device.




5. To modify the Module Definition settings, click Change (if required).

IMPORTANT For safety I/O devices, do not use Disable Keying. See [Electronic Keying on page 114](#).

6. Enter the node address for DeviceNet networks, or the IP address for EtherNet/IP networks.

Only unused node numbers are included in the pull-down menu.

If your network uses network address translation (NAT), see [Using Network Address Translation \(NAT\) with CIP Safety Devices on page 134](#).

7. To modify the Safety Network Number, click the  button.

See page [136](#) for details.

8. Set the Connection Reaction Time Limit by using the Safety tab.

See page [140](#) for details.

9. To complete configuration of the safety I/O device, refer to the user documentation and the Studio 5000 Logix Designer® application's online help.

Using Network Address Translation (NAT) with CIP Safety Devices

Applies to these controllers:

GuardLogix 5580

NAT translates one IP address to another IP address via a NAT-configured router or switch. The router or switch translates the source and destination addresses within data packets as traffic passes between subnets.

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

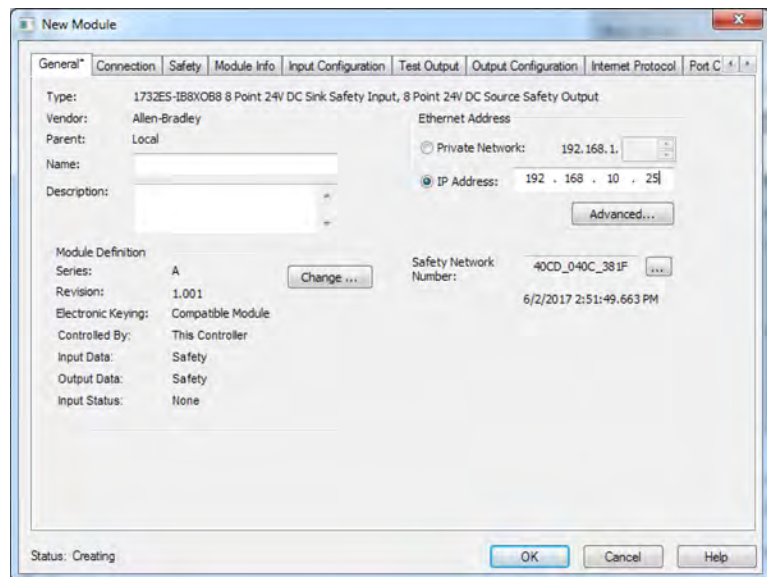
This section only applies to safety users where the controller and the devices it talks to are on separate sides of the NAT-configured router or switch.

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

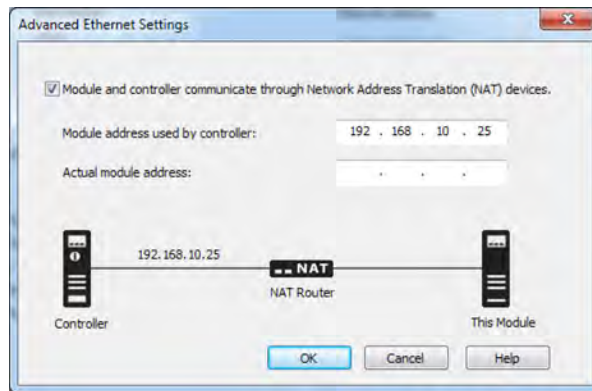
If you are using NAT to communicate with a CIP Safety device, follow these steps to set the IP address.

1. In the IP Address field, type the IP address that the controller will use.

This is usually the IP address on the public network when using NAT.



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



3. Check the checkbox to indicate that this module and the controller communicate through NAT devices.
4. Type the Actual module address.

TIP If you configured the IP address using the rotary switches, this is the address you set on the device. Alternately, the Actual module address is the same address shown on the device's Internet Protocol tab.

5. Click OK.

Set the SNN of a Safety I/O Device

A time-based Safety Network Number (SNN) is automatically assigned when you add the first safety I/O device on the network. This does not apply to the controller backplane or Ethernet port since the controller counts as a device on the network.

When subsequent safety devices are added to the same network, they are assigned the same SNN as defined in the lowest address on that CIP Safety network, or the controller itself in the case of ports attached to the controller.


For most applications, the automatic, time-based SNN is sufficient.

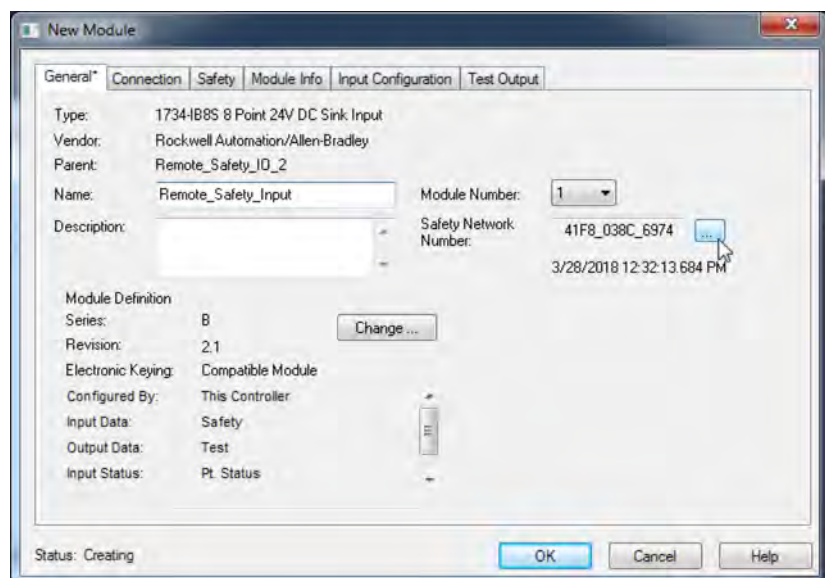
If your application requires you to manually assign the SNN of safety I/O devices, you only have to assign the SNN of the first safety I/O device you add in a remote network or backplane. Logix Designer then assigns the SNN of the first device to any additional devices that you add to that same remote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

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

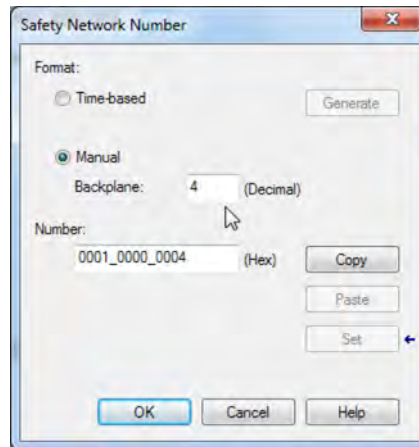
Change a Safety I/O Device SNN

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

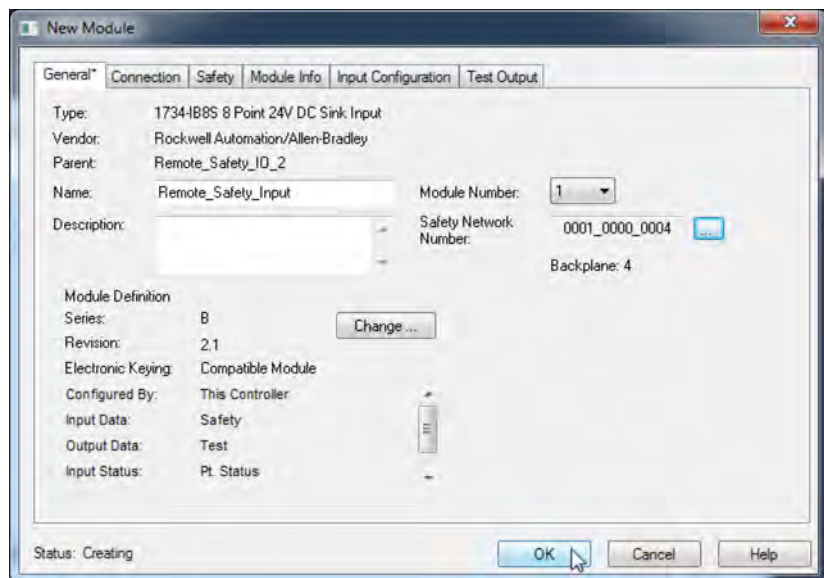
1. Right-click the remote EtherNet/IP communication module in the I/O Configuration tree, and select New Module.
2. Select your safety I/O device, and click Create.
3. On the New Module configuration dialog, click  to the right of the safety network number.



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



6. Click OK.
7. On the New Module configuration dialog, click OK.



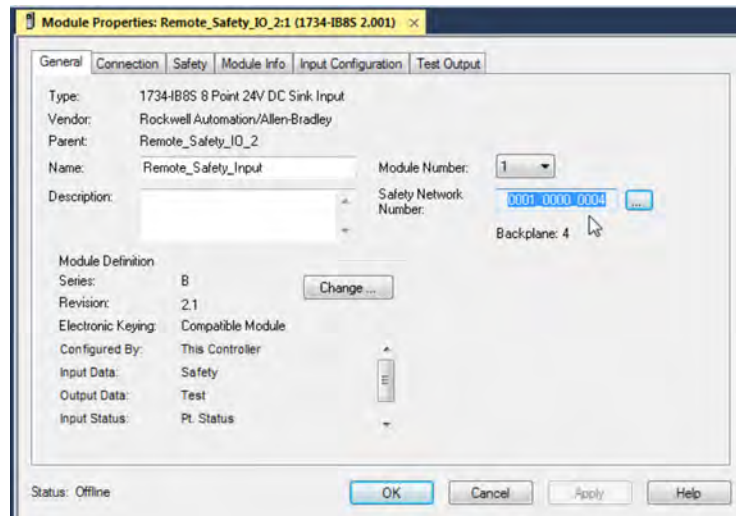
Copy and Paste a Safety I/O Device SNN

If you must apply a SNN to other safety I/O devices, you can copy and paste the SNN. There are multiple ways to copy and paste safety I/O device SNNs.


Copy a Safety I/O Device SNN

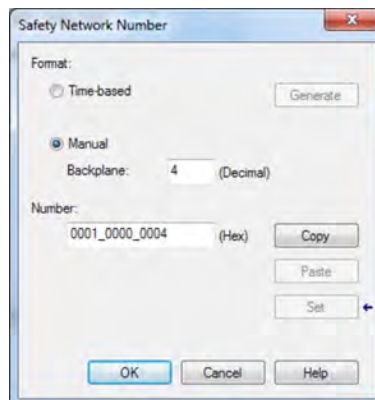
From the Module Properties General Tab:

1. On the General tab, select and highlight the SNN.
2. Press Ctrl-C to copy the SNN.




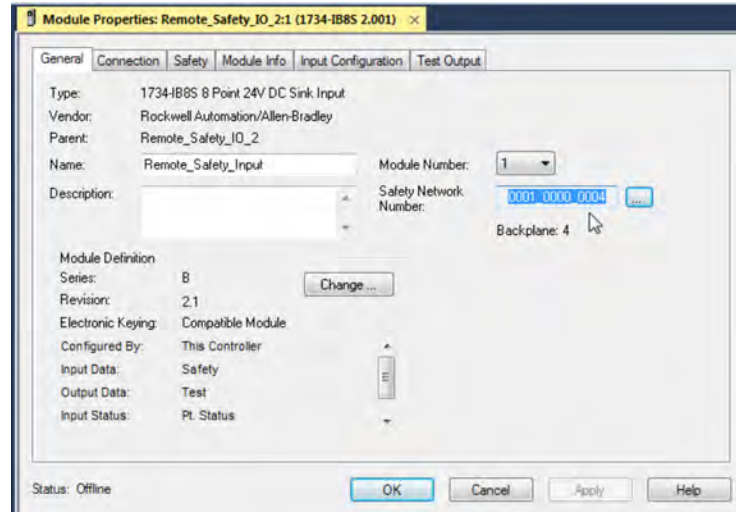
From the Safety Network Number dialog:

1. On the Module Properties General Tab, click  to the right of the safety network number to open the Safety Network Number dialog.
2. On the Safety Network Number dialog, either click Copy, or click in the SNN field and Press Ctrl-C.

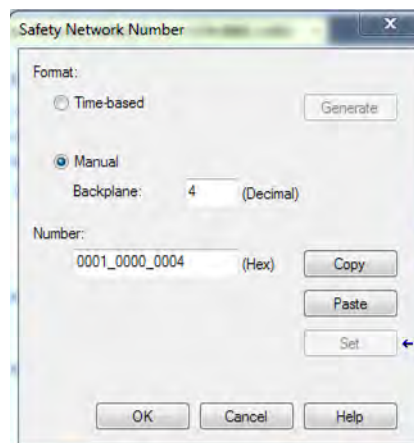


Paste a Safety I/O Device SNN

1. On the Module Properties General tab, click  to the right of the safety network number to open the Safety Network Number dialog.



2. On the Safety Network Number dialog, either click Paste, or click in the SNN field and Press Ctrl-V.



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

Connection Reaction Time Limit

The Connection Reaction Time Limit (CRTL) is defined by these three values.

Value	Default	Description
Requested Packet Interval (RPI)	10 ms (Input RPI)	How often the input and output packets are placed on the wire (network).
Timeout Multiplier	2	The Timeout Multiplier is essentially the number of retries before timing out.
Network Delay Multiplier	200	The Network Delay Multiplier accounts for any known delays on the wire. When these delays occur, timeouts can be avoided using this parameter.

If you adjust these values, then you can adjust the connection reaction time limit. 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, especially large banks of POINT Guard I/O™ Safety modules, the default connection reaction time limit can result in connection loss to the safety I/O modules. In these cases, it may be necessary to increase the values from their defaults. Make sure the new connection reaction time limit is used in the safety reaction time calculations.

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

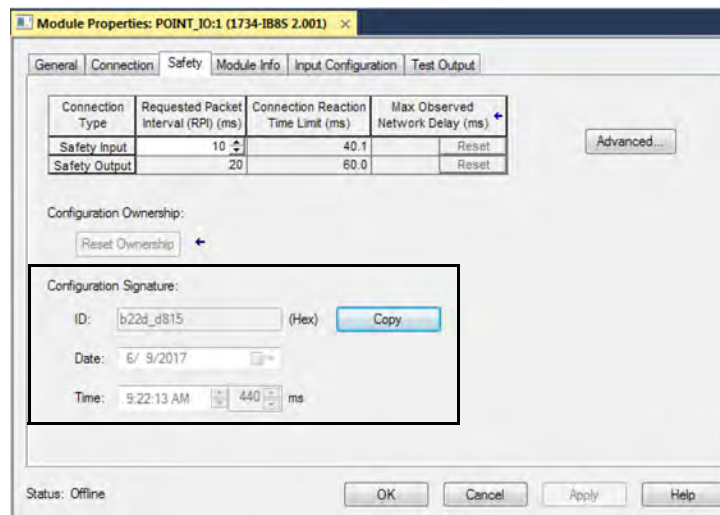
Safety I/O Device Signature

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

Configuration via the Logix Designer Application

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

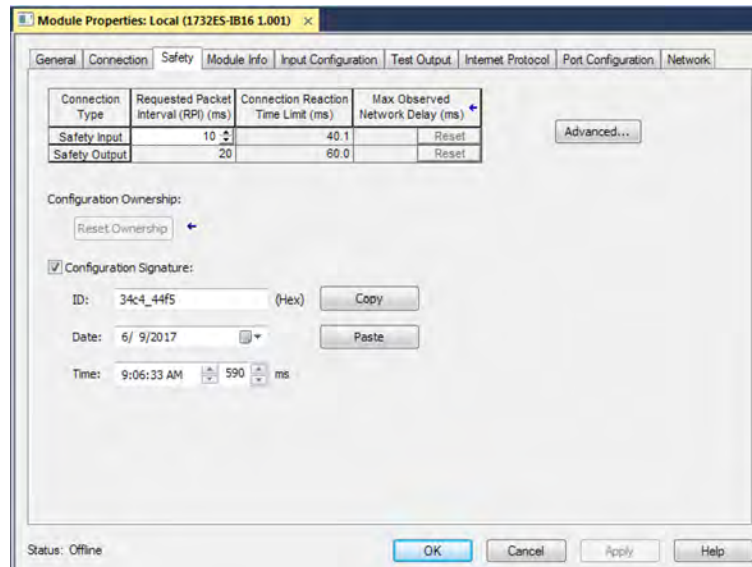
Figure 23 - View and Copy the Configuration Signature



Different Configuration Owner (data-only connection)

When the I/O device configuration is owned by another controller, you need to copy the module configuration signature from its owner's project and paste it into the Safety tab of the Module Properties dialog box.

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



Reset Safety I/O Device to Out-of-box Condition

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

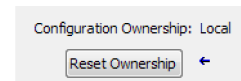
When the controller project is online, the Safety tab of the Module Properties dialog box displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the safety network number (SNN), and node address or slot number of the configuration owner. Communication error is displayed if the module read fails.

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

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

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

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



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

I/O Device Address Format

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

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

A Safety I/O module address follows this example.

EXAMPLE Modulename.Type.Member

Table 23 - Safety I/O Device Address Format

Where	Is	
Modulename	The name of the safety I/O device	
Type	Type of data	Input: I Output: O
Member	Specific data from the I/O device	
	Input-only module	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:I.Input Members
	Output-only module	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:O.Output Members
	Combination I/O	Modulename:I.RunMode ⁽¹⁾ Modulename:I.ConnectionFaulted ⁽¹⁾ Modulename:I.Input Members Modulename:O.Output Members

(1) This member is required.

Table 24 - More Resources

Resource	Description
Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004	Provides information on addressing standard I/O devices

Monitor Safety I/O Device Status

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

Replace a Safety I/O Device

This chapter provides information on replacing safety I/O devices when they are connected to GuardLogix® controllers.

Configuration Ownership

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

- When the opened project owns the configuration, Local is displayed.
- When a second device owns the configuration, Remote is displayed, along with the safety network number (SNN), and node address or slot number of the configuration owner.
- If the module read fails, Communication error is displayed.

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

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

Replacement Configuration

You can use the Logix Designer application to replace a safety I/O device on an Ethernet network.

To replace a Guard I/O module on a DeviceNet network, your choice depends on the type of module.

Table 25 - Software

If you are using a	Use	See
Safety I/O device on EtherNet/IP network.	The Logix Designer application	Below
1791DS Guard I/O module with a 1756-DNB adapter	The Logix Designer application	Below

- If you are relying on a portion of the CIP Safety system to maintain SIL 2/PLD or SIL 3/PLe behavior during device replacement and functional testing, the Configure Always feature cannot be used.

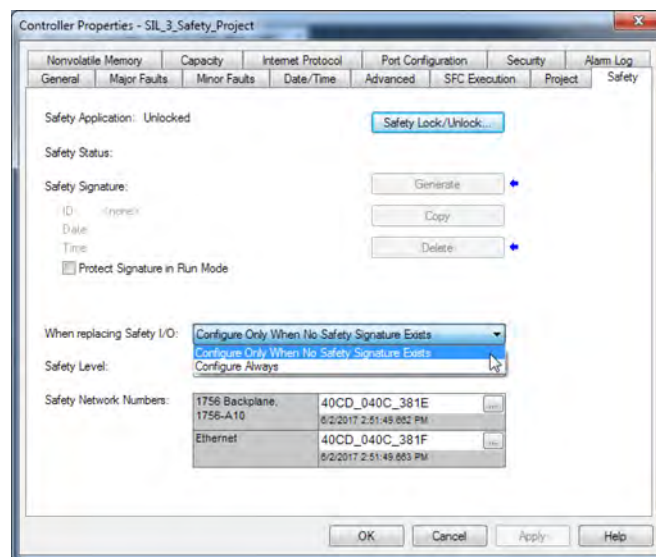
Go to [Replacement with ‘Configure Only When No Safety Signature Exists’ Enabled on page 147.](#)

- If the entire routable CIP Safety control system is not being relied on to maintain SIL 2/PLD or SIL 3/PLe behavior during the replacement and functional testing of a device, the Configure Always feature can be used.

Go to [Replacement with ‘Configure Always’ Enabled on page 152.](#)

Safety I/O device replacement is configured on the Safety tab of the GuardLogix 5380 controller.

Figure 24 - Safety I/O Device Replacement



Replacement with 'Configure Only When No Safety Signature Exists' Enabled


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

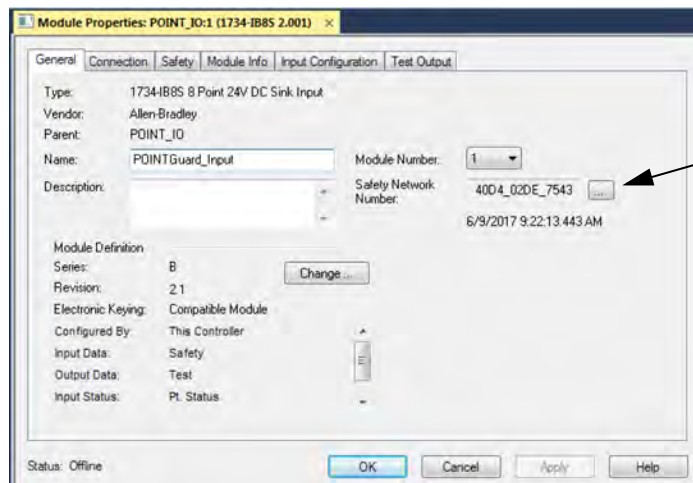
If the project is configured as 'Configure Only When No Safety Signature Exists', follow the appropriate steps in [Table 26](#) to replace a safety I/O device based on your scenario. After you complete the steps, the DeviceID matches the original, enabling the safety controller to download the proper device configuration, and re-establish the safety connection.

Table 26 - Replacing a Module

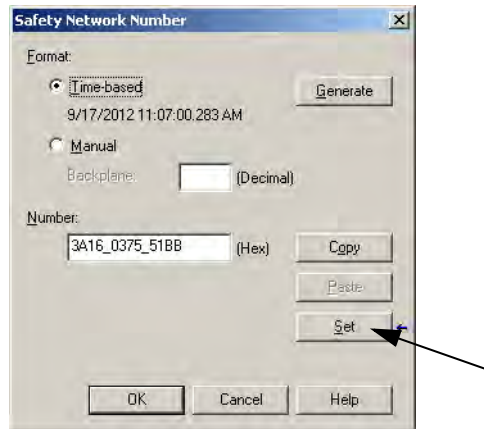
GuardLogix® Safety Signature Exists	Replacement Module Condition	Action Required
No	No SNN (Out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (Out-of-box)	See Scenario 1 - Replacement Device is Out-of-box and Safety Signature Exists on page 147.
Yes	Different SNN from original safety task configuration	See Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists on page 149.
No		See Scenario 3 - Replacement Device SNN is Different from Original and No Safety Signature Exists on page 151.

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

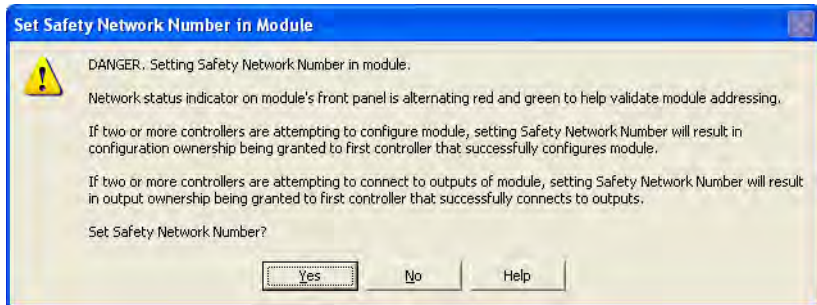
1. Remove the old I/O device and install the new device.
2. Right-click the replacement safety I/O device and choose Properties.
3. Click  to the right of the safety network number to open the Safety Network Number dialog box.



4. Click Set.



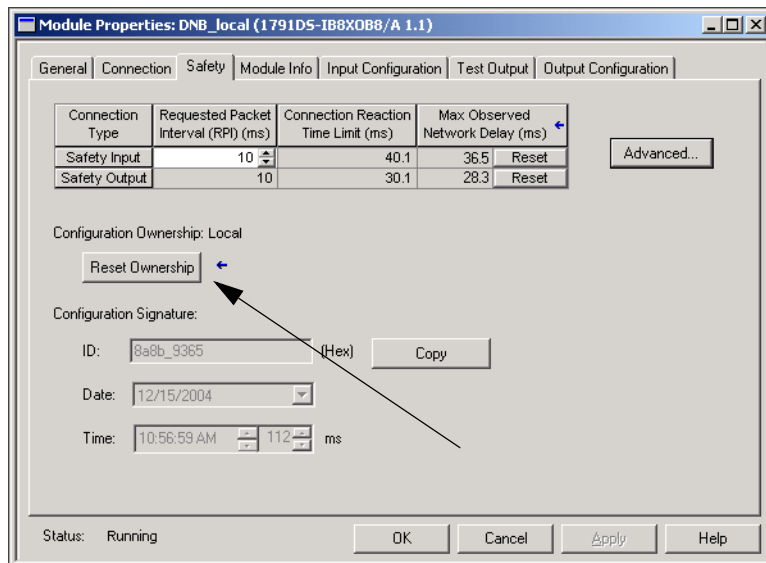
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.




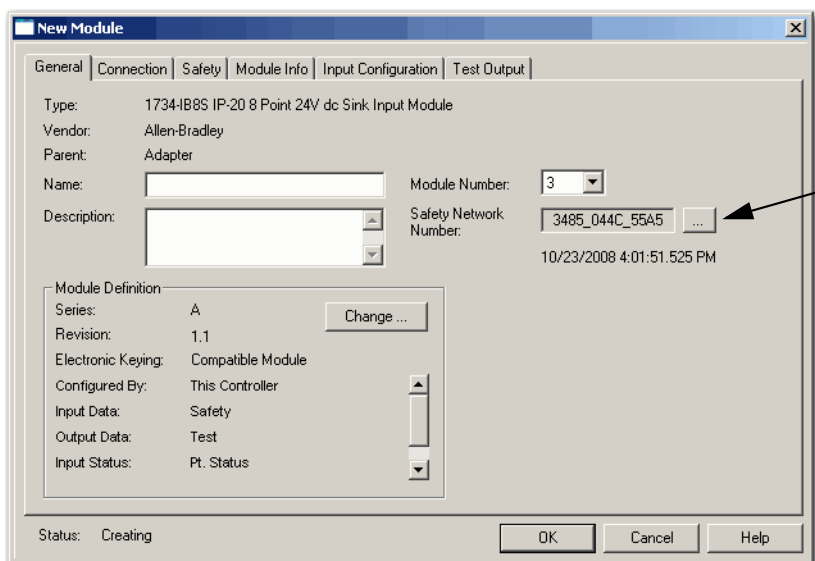
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

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

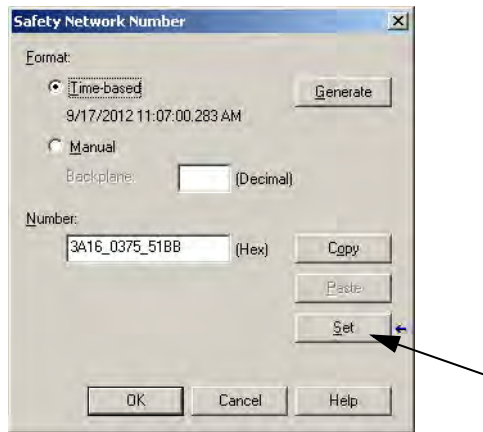
1. Remove the old I/O device and install the new device.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.
4. Click Reset Ownership.



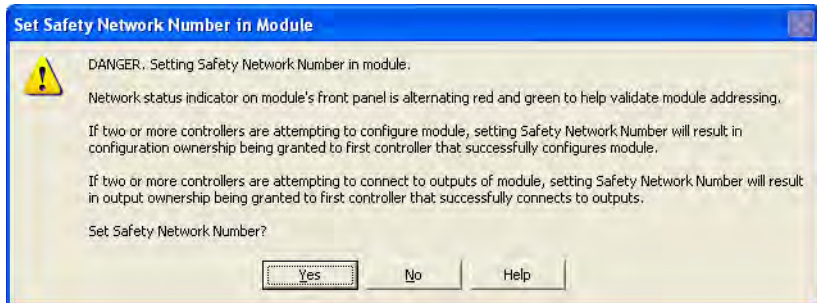
5. Click OK.
6. Right-click the device and choose Properties.
7. Click  to the right of the safety network number to open the Safety Network Number dialog box.



8. Click Set.



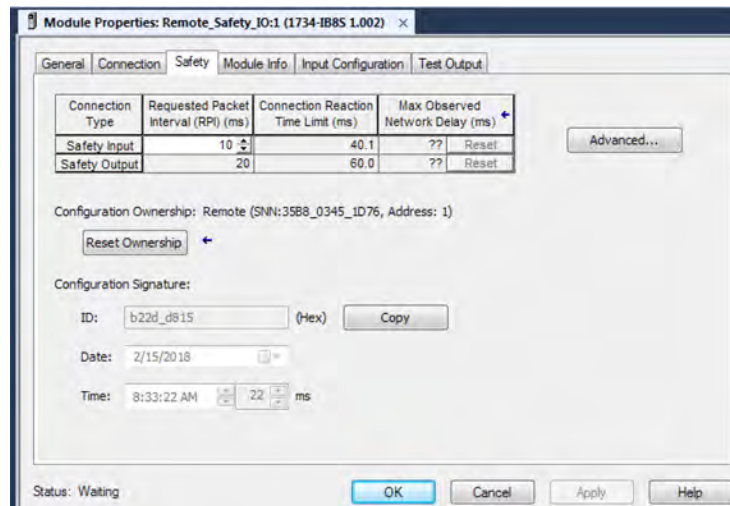
9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.



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

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

1. Remove the old I/O device and install the new device.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.



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

Replacement with 'Configure Always' Enabled



ATTENTION: Enable the 'Configure Always' feature only if the entire CIP Safety Control System is **not** being relied on to maintain SIL 2/PLD or SIL 3/PLD behavior during the replacement and functional testing of a device.

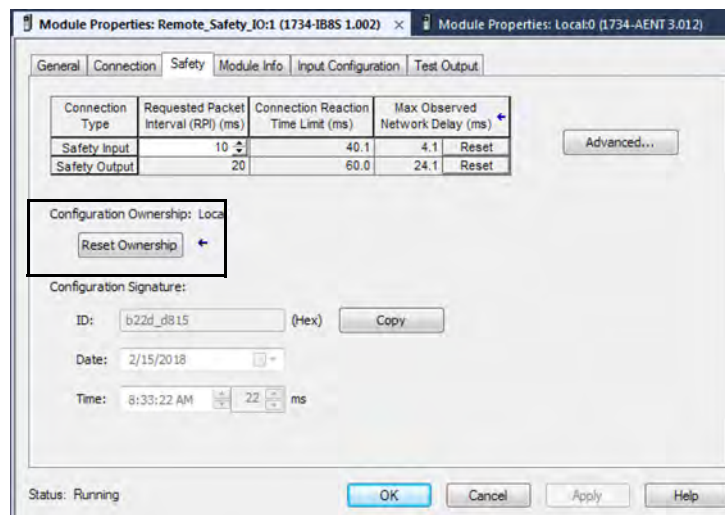
Do not place devices that are in the out-of-box condition on a CIP Safety network when the Configure Always feature is enabled, except while following this replacement procedure.

When the 'Configure Always' feature is enabled in the controller project, the controller automatically checks for and connects to a replacement device that meets all of the following requirements:

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

If the project is configured for 'Configure Always', follow the appropriate steps to replace a safety I/O device.

1. Remove the old I/O device and install the new device.
 - a. If the device is in out-of-box condition, go to step 6. No action is needed for the GuardLogix controller to take ownership of the device.
 - b. If an SNN mismatch error occurs, go to the next step to reset the device to out-of-box condition.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.
4. Click Reset Ownership.



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

Develop Standard Applications

Topic	Page
Elements of a Control Application	153
Tasks	155
Programs	157
Routines	160
Parameters and Local Tags	161
Programming Languages	162
Add-On Instructions	163
Extended Properties	164
Access the Module Object from an Add-On Instruction	165
Monitor Controller Status	166
Monitor I/O Connections	167

Elements of a Control Application

Applies to these controllers:

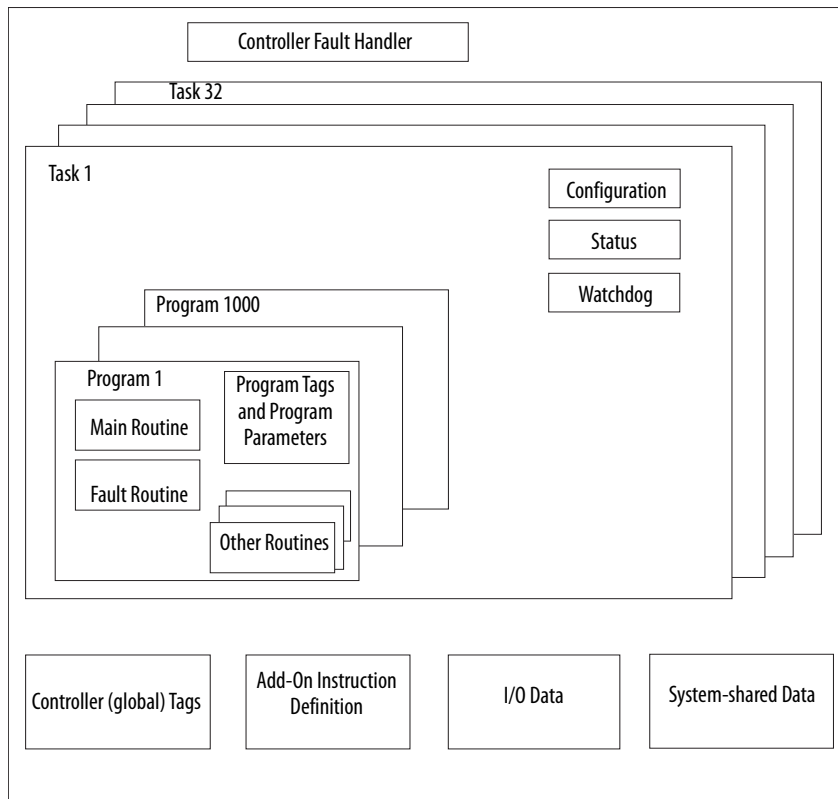
ControlLogix 5580

GuardLogix 5580

A control application consists of several elements that require planning for efficient application execution. Application elements include the following:

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

Figure 25 - 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 26 - Task Within a Control Application

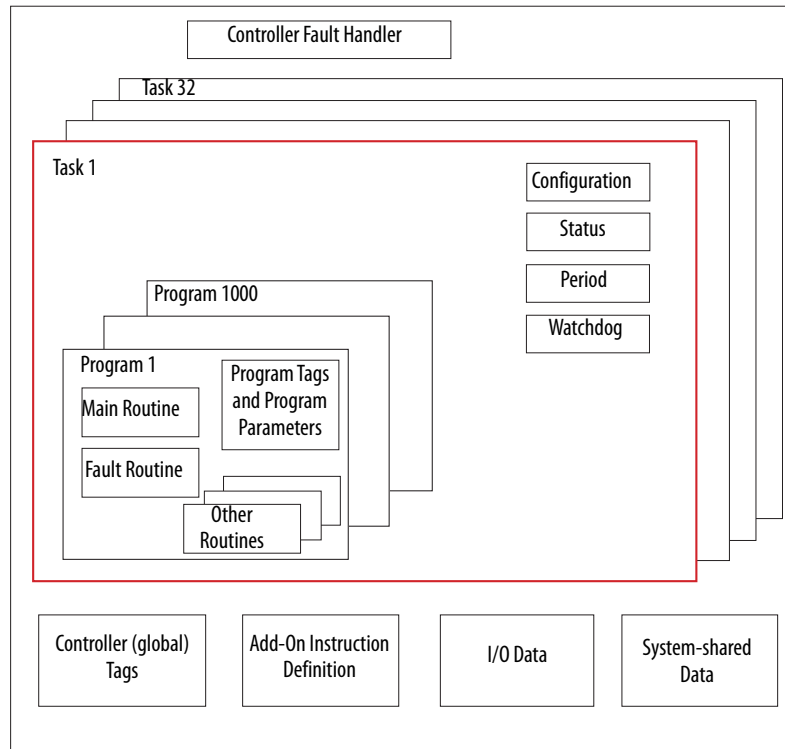
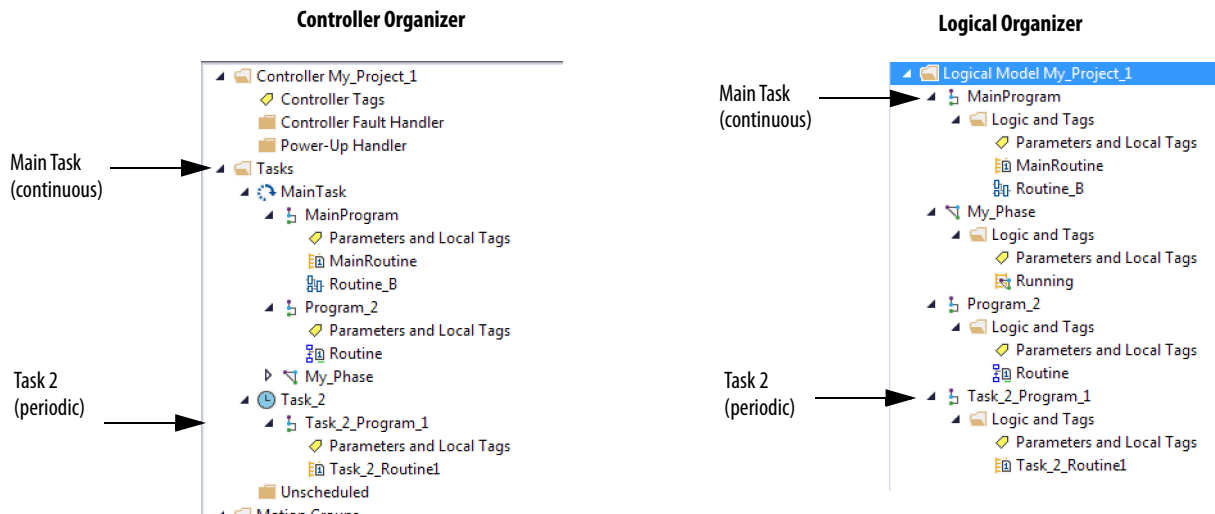
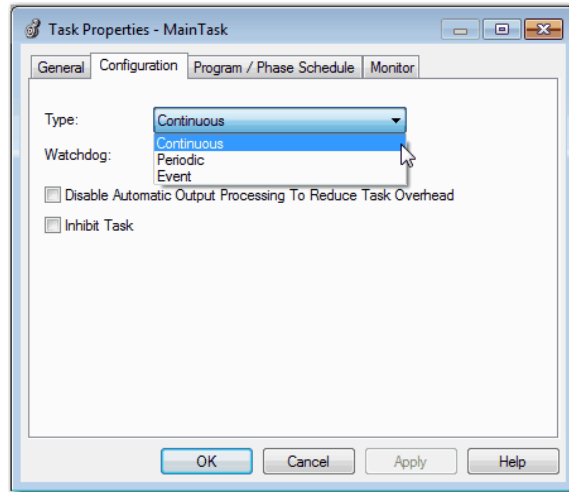


Figure 27 - Tasks



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

Figure 28 - Configuring the Task Type



[Table 27](#) explains the types of tasks you can configure.

Table 27 - Task Types and Execution Frequency

Task Type	Task Execution	Description
Continuous	Constant	The continuous task runs in the background. Any CPU time that is not allocated to other operations (such as motion and other tasks) is used to execute the programs in the continuous task. <ul style="list-style-type: none"> • The continuous task runs constantly. When the continuous task completes a full scan, it restarts immediately. • A project does not require a continuous task. If used, there can be only one continuous task.
Periodic	At a set interval, such as each 100 ms	A periodic task performs a function at an interval. <ul style="list-style-type: none"> • Whenever the time for the periodic task expires, the task interrupts any lower priority tasks, executes once, and returns control to where the previous task left off. • You can configure the time period from 0.1...2,000,000.00 ms. The default is 10 ms. It is also controller and configuration dependent.
Event	Immediately when an event occurs	An event task performs a function when an event (trigger) occurs. The trigger for the event task can be the following: <ul style="list-style-type: none"> • Module input data change of state • A consumed tag trigger • An EVENT instruction • An axis trigger • A motion event trigger You can configure an optional timeout interval for missed event triggers, which causes the event tasks to execute even in the absence of the trigger. Set the Check the Execute Task If No Event Occurs Within <timeout period> check box for task.

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

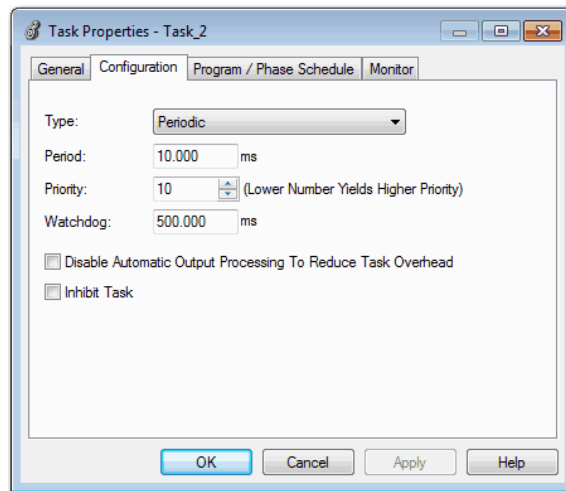
A task can have up to 1000 programs, each with its own executable routines and program-scoped tags. Once a task is triggered (activated), the programs that are assigned to the task execute in the order in which they are grouped. Programs can appear only once in the Controller Organizer and multiple tasks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

Task Priority

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

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

Figure 29 - Configure Task Priority



Programs

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

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

Each program contains the following:

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

Figure 30 - Program Within a Control Application

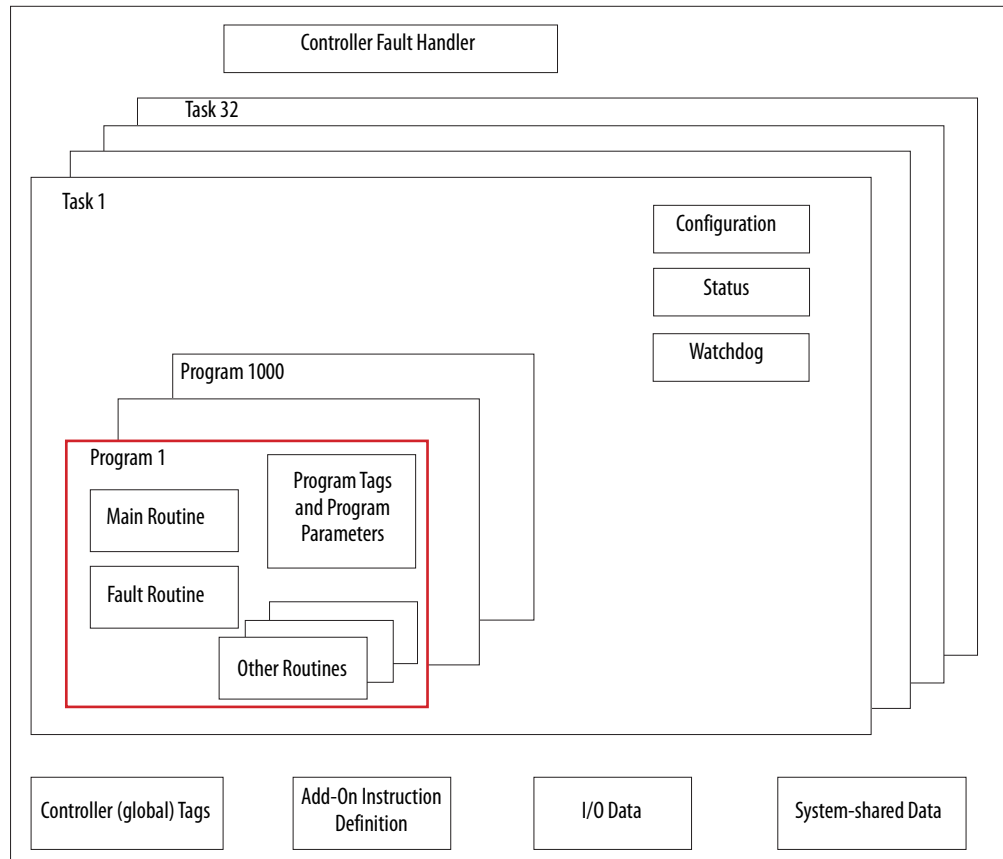
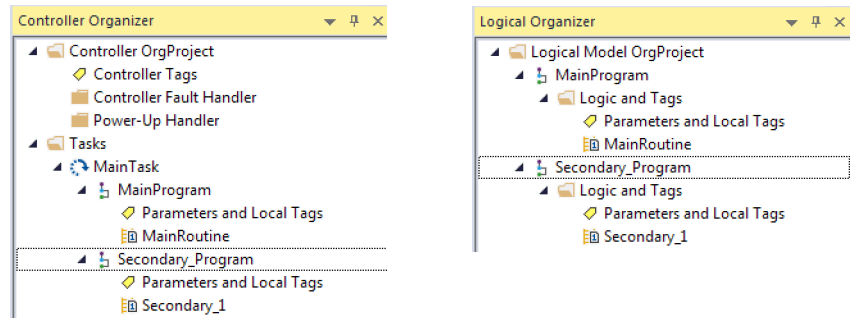


Figure 31 - Programs



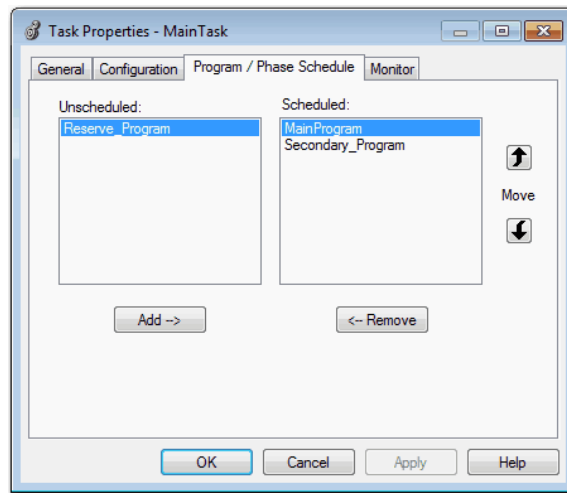
Scheduled and Unscheduled Programs

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

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

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

Figure 32 - Scheduling an Unscheduled Program



Routines

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

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

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

Figure 33 - Routines in a Control Application

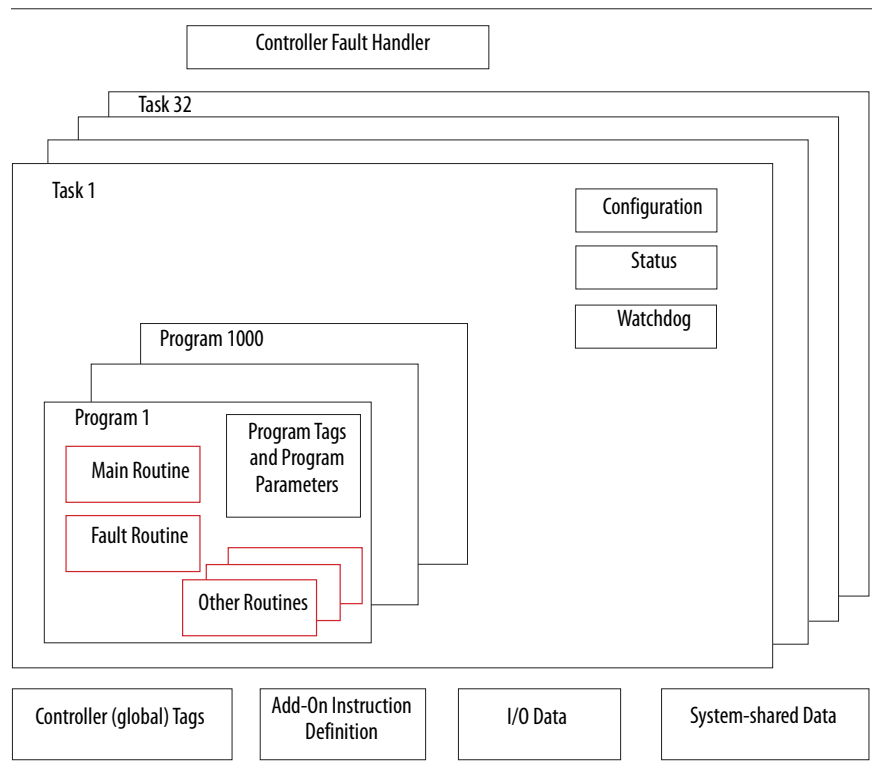
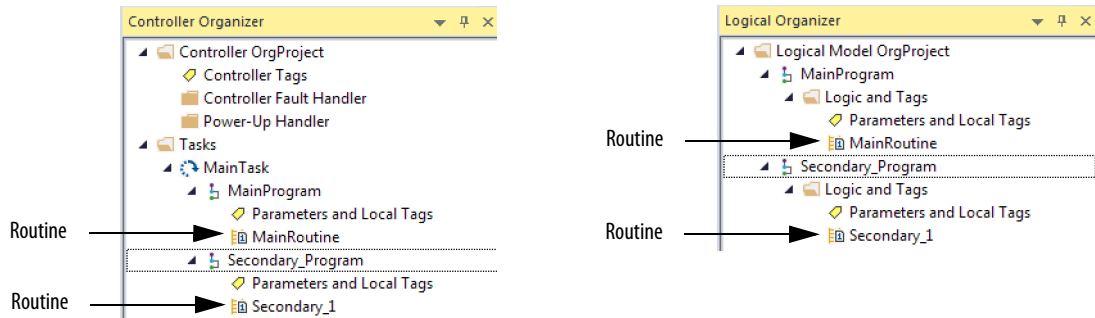


Figure 34 - Routines



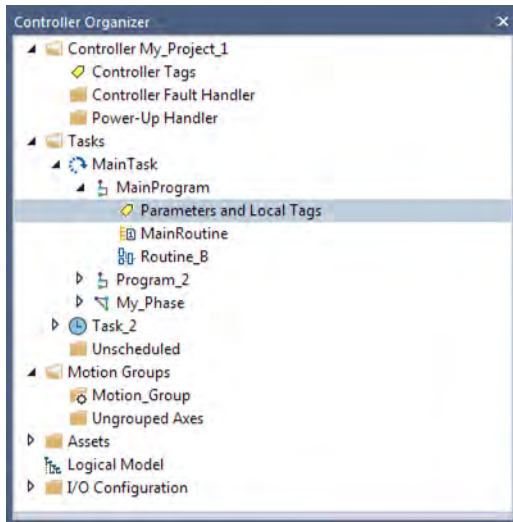
Parameters and Local Tags

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

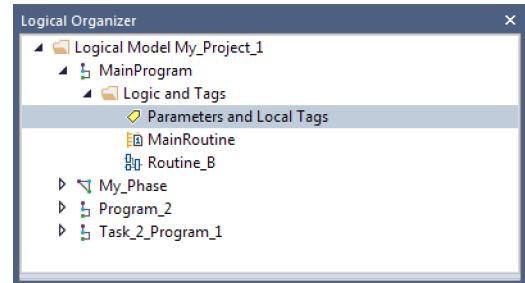
- Organize your data to mirror your machinery.
- Document your application as you develop it.

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

Controller Organizer —Main Program Parameters and Local Tags



Logical Organizer —Main Program Parameters and Local Tags



Program Parameters and Local Tags Window

Name	Usage	Value	Style	Data Type	Description	Constant	Alias For
ADD_01	Local	{...}		FBD_MATH		<input type="checkbox"/>	
ADD_02	Local	{...}		FBD_MATH		<input type="checkbox"/>	
Disabled	Local	0 Decimal		BOOL		<input type="checkbox"/>	
Motor_Starter_01	Local	{...}		Motor_Starter	Starts the motor.	<input type="checkbox"/>	

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

Program Parameters

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

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

There are several guidelines for creating and configuring parameters and local tags for optimal task and program execution:

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

Programming Languages

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

Language	Is best used in programs with
Ladder Diagram (LD)	Continuous or parallel execution of multiple operations (not sequenced)
	Boolean or bit-based operations
	Complex logical operations
	Message and communication processing
	Machine interlocking
	Operations that service or maintenance personnel have to interpret to troubleshoot the machine or process
	IMPORTANT: Ladder Diagram is the only programming language that can be used with the Safety Task on GuardLogix 5580 controllers.
Function Block Diagram (FBD)	Continuous process and drive control
	Loop control
	Calculations in circuit flow
Sequential Function Chart (SFC)	High-level management of multiple operations
	Repetitive sequence of operations
	Batch process
	Motion control that uses structured text
	State machine operations
Structured Text (ST)	Complex mathematical operations
	Specialized array or table loop processing
	ASCII string handling or protocol processing

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

Add-On Instructions

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

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

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

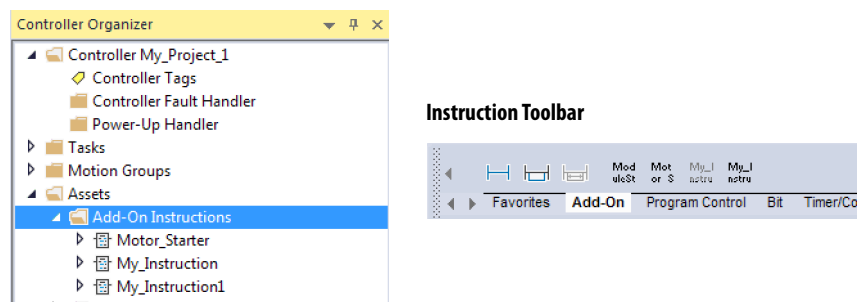
You can use Add-On Instructions across multiple projects. You can define your instructions, obtain them from somebody else, or copy them from another project. [Table 28](#) explains some of the capabilities and advantages of use Add-On Instructions.

Table 28 - Add-On Instruction Capabilities

Capability	Description
Save Time	With Add-On Instructions, you can combine your most commonly used logic into sets of reusable instructions. You save time when you create instructions for your projects and share them with others. Add-On Instructions increase project consistency because commonly used algorithms all work in the same manner, regardless of who implements the project.
Use Standard Editors	You create Add-On Instructions by using one of three editors: <ul style="list-style-type: none"> • Ladder Diagram • Function Block Diagram • Structured Text
Export/Import Add-On Instructions	You can export/import Add-On Instructions to other projects and copy and paste them from one project to another. Give each instruction a unique, descriptive name to make it easier to manage and reuse your collection of Add-On Instructions.
Use Context Views	Context views let you visualize the logic of an instruction for instant, simplified online troubleshooting of your Add-On Instructions.
Document the Instruction	When you create an instruction, you enter information for the description fields. Each instruction definition includes revision, change history, and description information. The description text also becomes the help topic for the instruction. You can also generate a signature for the AOI, and include the AOI in a tracking group.
Apply Source Protection	When you create Add-On Instructions, you can limit users of your instructions to read-only access, or you can bar access to the internal logic or local parameters that are used by the instructions. This source protection lets you stop unwanted changes to your instructions and helps protect your intellectual property. You can pre-compile and encrypt your AOI for better Intellectual property protection. Using this feature has less of a performance impact than the Logix-designer source protection

Once defined in a project, Add-On Instructions behave similarly to the built-in instructions in the controllers. With Studio 5000 Logix Designer application version 31 and greater, Add-On Instructions appear under the Assets folder in the organizer. They also appear on the instruction tool bar for easy access along with internal instructions.

Figure 35 - Add-On Instructions (Studio 5000 Logix Designer Application Version 31 Example)



Extended Properties

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

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

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

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

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

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

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

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

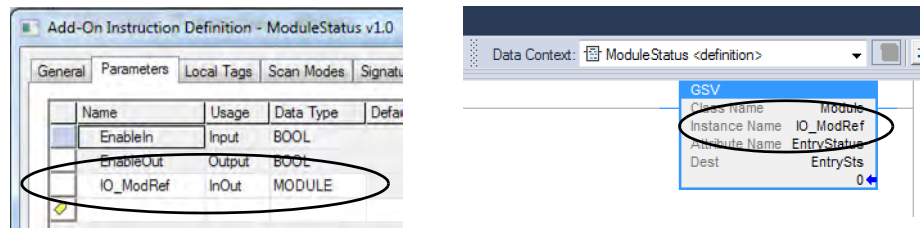
For more information on Extended Properties, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication [1756-PM004](#).

Access the Module Object from an Add-On Instruction

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

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

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



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

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

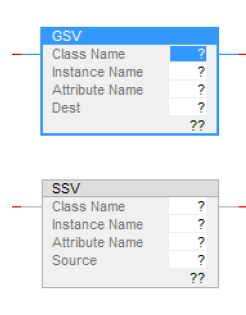
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Monitor Controller Status

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

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

Figure 36 - GSV and SSV Instructions for Monitoring and Setting Attributes



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

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

The GSV and SSV instructions monitor and set many objects and attributes. See the online help for the GSV and SSV instructions.


Monitor I/O Connections

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

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

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

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

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

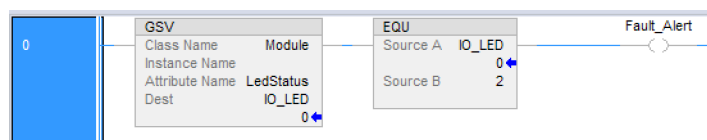
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#).

Determine If I/O Communication Has Timed Out

This example can be used with the ControlLogix 5580 or GuardLogix 5580 controllers, and help determine if controller communication has timed out:

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

Figure 37 - GSV Used to Identify I/O Timeout



IMPORTANT Safety Consideration

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

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

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

For Safety I/O modules, see [Monitor Safety Connections on page 198](#).

Automatic Handling of I/O Module Connection Faults

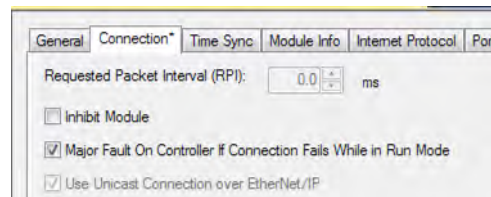
Depending on your application, you may want an I/O connection error to cause the Controller Fault Handler to execute. To do so, set the module property that causes a major fault to result from an I/O connection error. The major fault causes the execution of the Controller Fault Handler.



ATTENTION: You cannot program Safety I/O module connections or safety produce/consume connections to automatically cause a major fault on the controller. See [Develop Safety Applications on page 171](#).

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 38 - 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 [167](#) 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.

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

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

Sample Controller Projects

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

Figure 39 - Opening Sample Projects



Notes:

Develop Safety Applications

Topic	Page
Safety Task	172
Safety Programs	174
Safety Routines	174
Safety Add-On Instructions	175
Produced/Consumed Safety Tags	177
Safety Tag Mapping	186
Safety Application Protection	189
Programming Restrictions	194
Monitor Safety Status	195
Safety Faults	201
Develop a Fault Routine for Safety Applications	204
Use GSV/SSV Instructions in a Safety Application	205

Applies to these controllers:

GuardLogix 5580

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

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

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

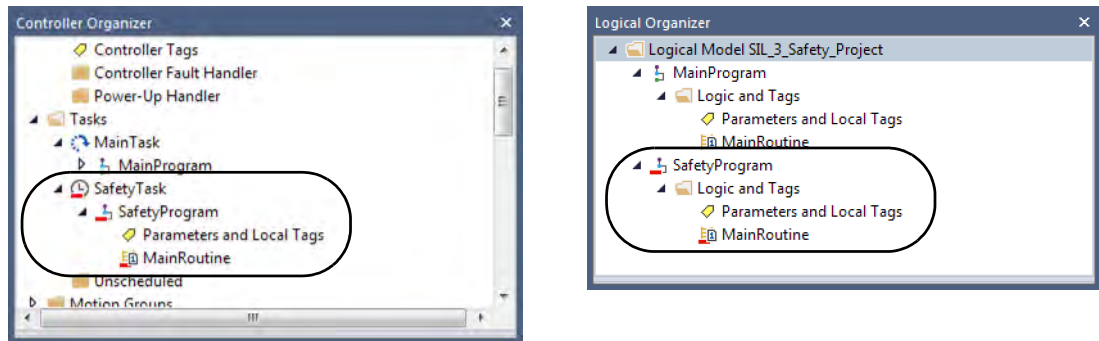


ATTENTION: Performing an on-line modification (to logic, data, or configuration) can affect the Safety Function(s) of the system if the modification is performed while the application is running. A modification should only be attempted if absolutely necessary. Also, if the modification is not performed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

Safety Task

When you create a safety controller project, the Studio 5000 Logix Designer® application automatically creates a safety task with a safety program and a main (safety) routine.

Figure 40 - Safety Task in the Controller Organizer and Logical organizer



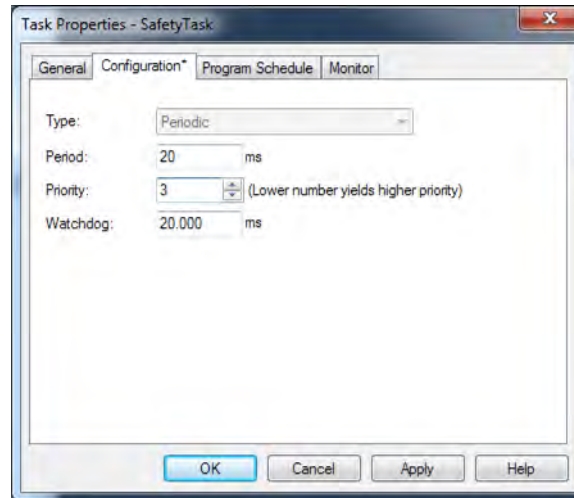
Within the safety task, you can use multiple safety programs, composed of multiple safety routines. The GuardLogix® 5580 controllers supports one safety task. The safety task cannot be deleted.

You cannot schedule standard programs or execute standard routines within the safety task.

Safety Task Period

The safety task is a periodic timed task. You set the task priority and watchdog time via the Task Properties - Safety Task dialog box. To open the dialog box, right-click the Safety Task and choose Properties.

Figure 41 - Configure the Safety Task Period



To get the most consistent safety task execution time, and to minimize safety task watchdog faults, we recommend running the safety task as the highest priority user task.

You specify the safety task period (in ms) and the safety task watchdog (in ms). The safety task period is the elapsed time between successive starting times for the safety task. The safety task watchdog is the maximum time allowed from the start of safety task execution to its completion.

The safety task period is limited to a maximum of 500 ms and cannot be modified online. Be sure that the safety task has enough time to finish logic execution before it is triggered again. If a safety task watchdog timeout occurs, a nonrecoverable safety fault is generated in the safety controller.

The safety task period directly affects system reaction time.

For information on calculating system reaction time, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication [1756-RM012](#).

Safety Task Execution

The safety task executes in the same manner as a standard periodic task, with the following exceptions:

- For a SIL 3/PLe application, the safety task does not begin executing until the primary controller and safety partner establish their control partnership. Standard tasks begin executing as soon as the controller transitions to Run mode.
- All safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution. See page 186 for information on safety tag mapping.
- Safety output packets (produced tags and output modules) are generated at the conclusion of safety task execution.
- When the controller does not have a safety signature and is not safety locked, the safety task can be held off until a communications update completes.

Safety Programs

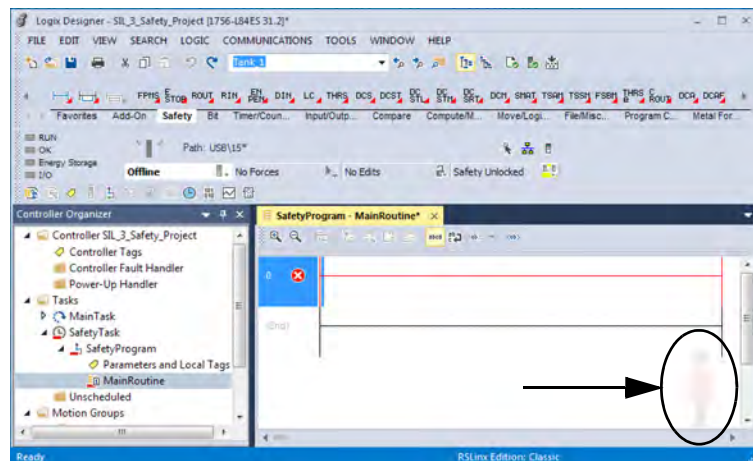
Safety programs have all attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines. One safety routine must be designated as the main routine, and another safety routine can be designated as the fault routine.

Safety programs cannot contain standard routines or standard tags.

Safety Routines

Safety routines have all the attributes of standard routines, except that they exist only in a safety program. Only ladder diagram is supported for safety routines.

TIP A watermark feature visually distinguishes a safety routine from a standard routine.



Safety Add-On Instructions

You can create safety Add-On Instructions to be used in Safety applications. Safety Add On Instructions feature a safety instruction signature for use in safety-related applications up to and including SIL 2-rated applications.

For more information, see the Logix 5000 Controllers Add On Instructions Programming Manual, publication [1756-PM010](#).

Safety Tags

Safety tags have all the attributes of standard tags with the addition of mechanisms 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

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 [Safety Tag Mapping on page 186](#).

The Logix Designer application can write to safety tags directly via the Tag Monitor when the GuardLogix 5580 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 may 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 types or arrays composed of the two types above

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 safety controller. Program-scoped safety tags can be read by external communication devices, but only local safety routines can write to them. These are routines that reside within the safety program.

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:

- More than one program in the project
- To produce or consume data
- In safety tag mapping

See [Safety Tag Mapping on page 186](#) for more information.

Controller-scoped safety tags can be read, but not written to, by standard routines.

Program Parameters

For program parameters, a safety parameter cannot be connected with or bound to a standard parameter or controller-scoped tag.

For information on program parameters, see [Program Parameters on page 162](#).

Produced/Consumed Safety Tags

To transfer safety data between GuardLogix controllers, you use produced and consumed safety tags.

Tags 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 reserved for the status of the connection. This member is a predefined data type called CONNECTION_STATUS.

Table 29 - Produced and Consumed Connections

Tag	Connection Description
Produced	GuardLogix 5580 controllers can produce (send) safety tags to other GuardLogix controllers. <ul style="list-style-type: none"> • GuardLogix 5580 controllers only support unicast produced tags. • GuardLogix 5580 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 a single connection for each consumer. • The consuming controller needs to be at firmware revision 19 or later. Unicast was not added to safety produced/consumed tags until firmware revision 19.
Consumed	GuardLogix 5580 controllers can consume (receive) safety tags from other GuardLogix controllers in these configurations: <ul style="list-style-type: none"> • 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 GuardLogix 5580 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 properly 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, as described below.

Configure the SNN for a Peer Safety Controller Connection

The peer safety controller is subject to the same configuration requirements as the local safety controller. The peer safety controller must also have a safety network number (SNN).

The safety application that is downloaded into the peer safety controller configures SNN values for each CIP Safety™ port on the controller.

Table 30 - SNN and Controller Placement

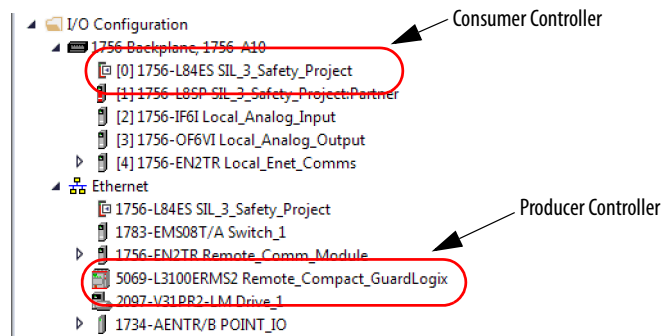
Peer Safety Controller Location	SNN
Placed in the local chassis	The user application on the peer controller generates an SNN value for the local backplane port of the controller.
Placed in another chassis	The controller must have a unique SNN.

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


If the automatically assigned SNN of the producer controller does not match the SNN the controller actually uses, you can follow these steps to copy and paste the SNN.

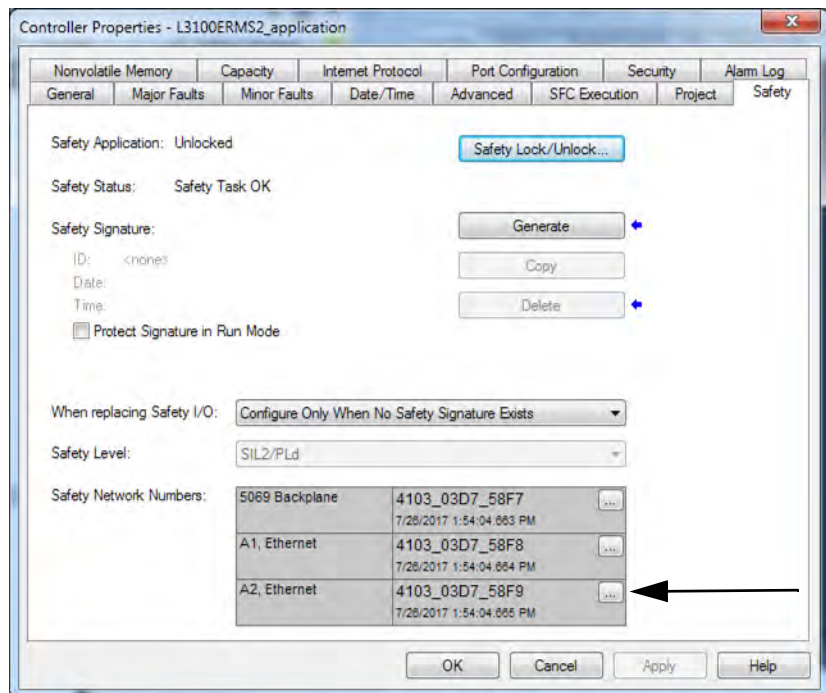
TIP Setting the correct SNNs of the controller as described in [Assign the Safety Network Number \(SNN\) on page 65](#) usually results in the producer controller being assigned the correct SNN. In these cases you need not perform this procedure.

1. Add the producer controller to the consumer controller’s I/O tree.

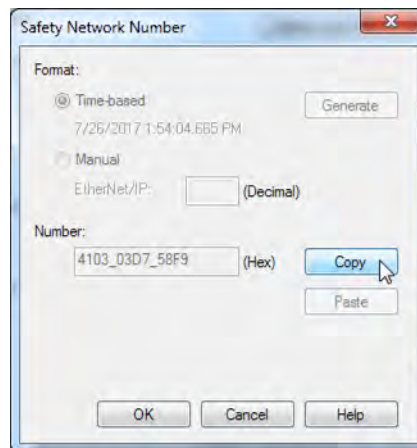


2. In the producer controller’s project, right-click the producer controller and choose Controller Properties.

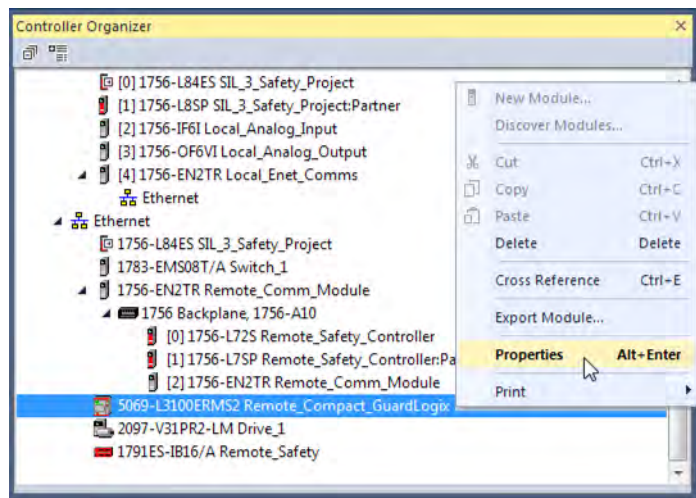
- On the Safety tab, click the  next to the port (Ethernet or Backplane) that communicates with the consumer controller. This opens the Safety Network Number dialog box.




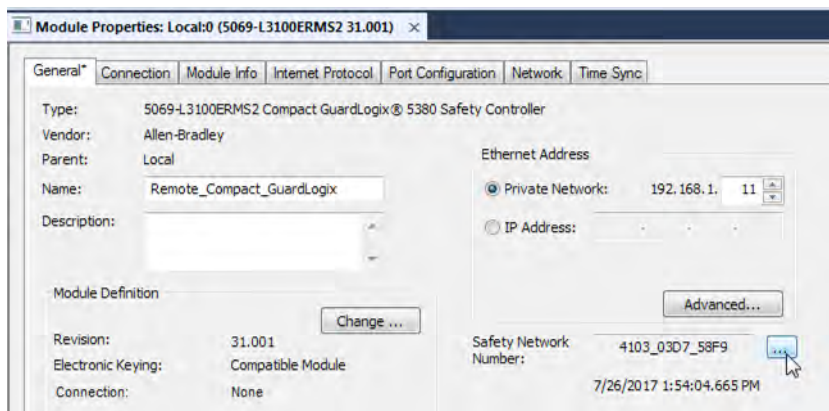
- Copy the producer controller's SNN.



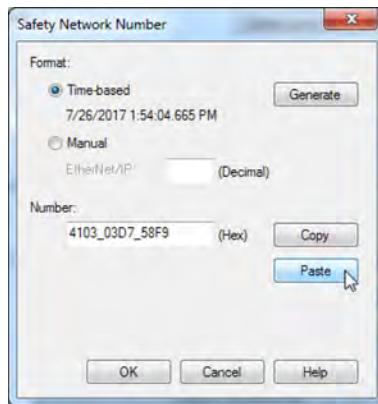
- In the I/O tree of the consumer controller's project, right-click on the module that represents the producing controller, and choose Module Properties.



- On the Module Properties General tab, click  to open the Safety Network Number dialog.

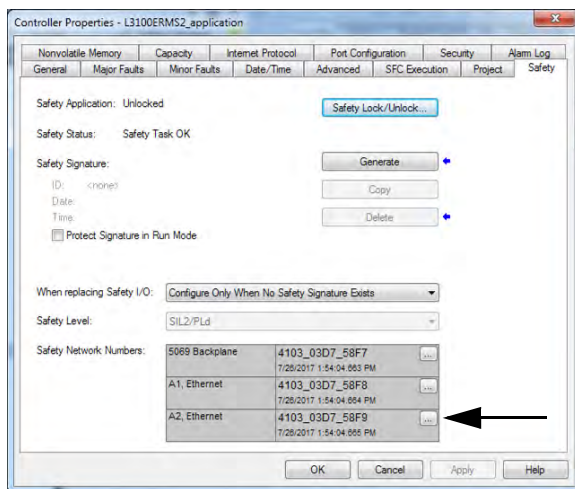


- Paste the producer controller's SNN into the SNN field and click OK.

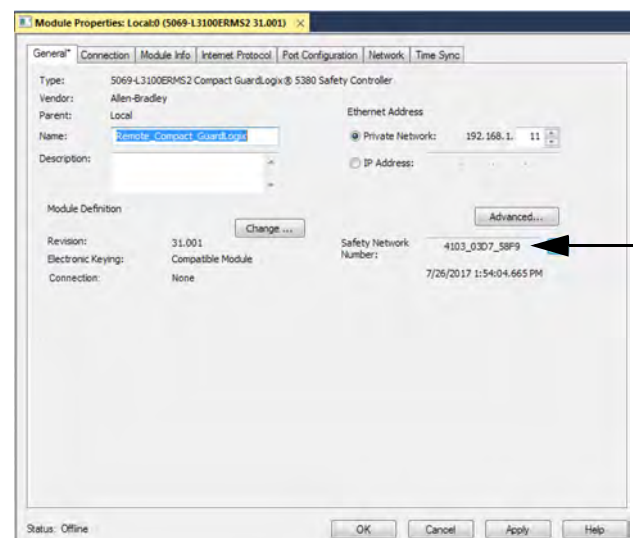


The safety network numbers match.

Producer Controller Properties Dialog Box in Producer Project



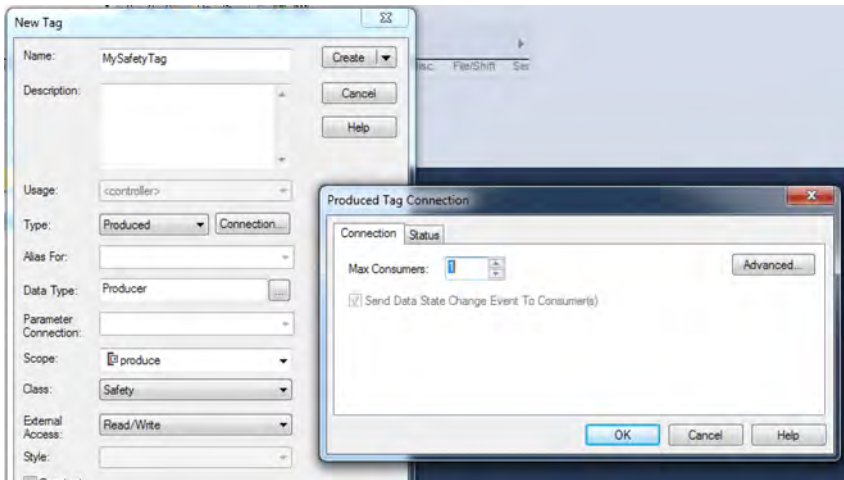
Module Properties Dialog Box in Consumer Project



Produce a Safety Tag

Complete these steps to produce a safety tag.

1. In the producing controllers project, create a user-defined data type defining 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 choose New Tag.
3. Set the type as Produced, the class as Safety, and the Data Type to the user-defined type you created in step 1.
4. Click Connection and enter the max limit on the number of consumers (1 through 15).



5. Click OK.
6. Click Create.

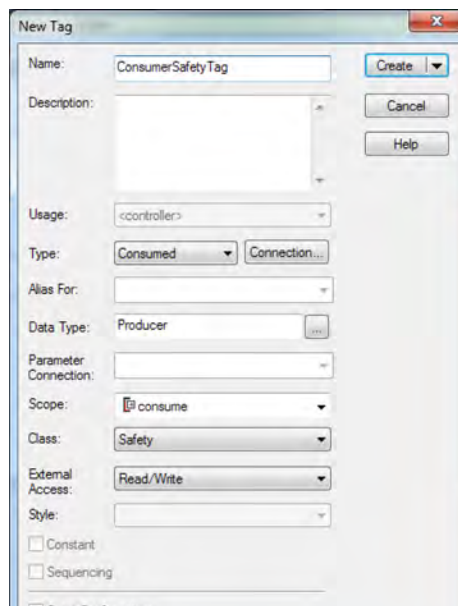
Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

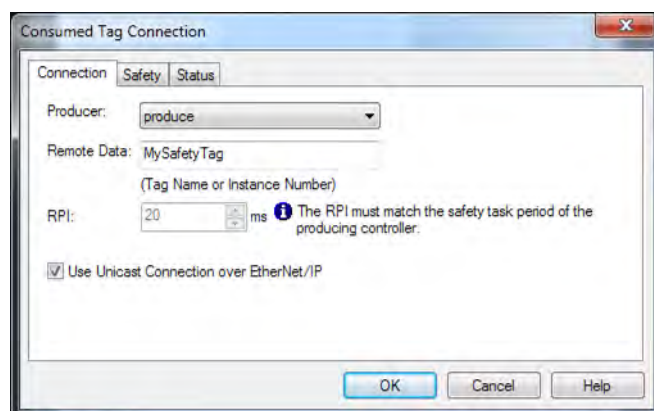
1. In the consumer controller's project, create a user-defined data type identical to the one created in the producer project (the names of the user-defined data types must match).

TIP The user-defined type can be copied from the producer project and pasted into the consumer project.

2. Right-click Controller Tags and choose New Tag.
3. Set the Type as Consumed, the Class as Safety, and the Data Type to the user-defined data type you created in step 1.



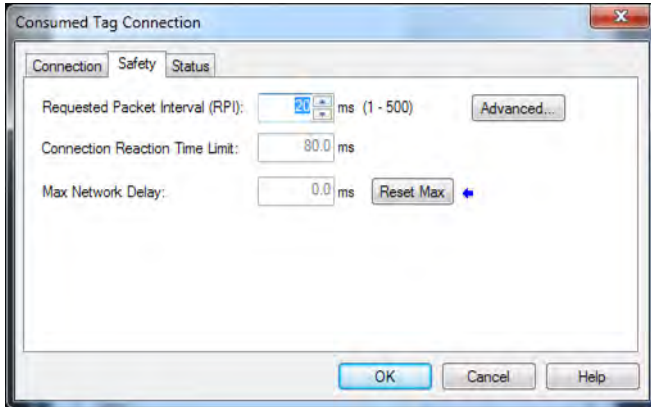
4. Click Connection to open the Consumed Tag Connection dialog box.



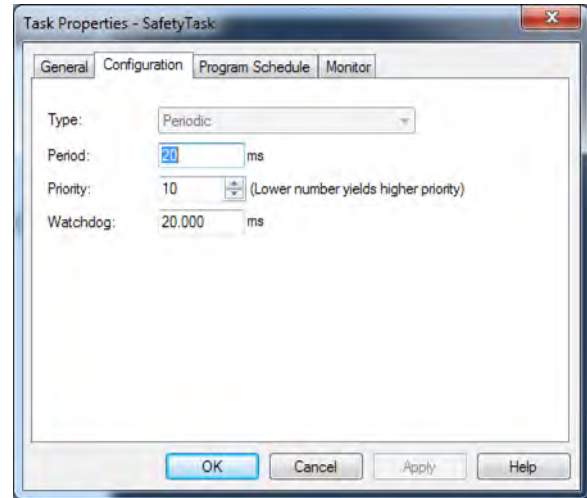
5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.

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.

Consumer's Project



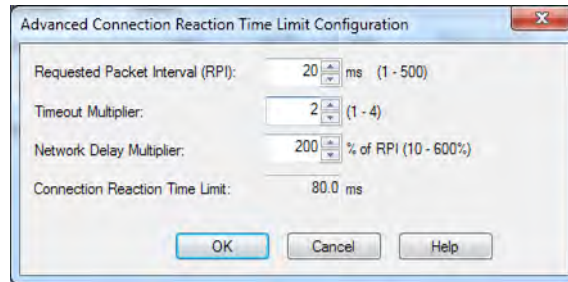
Producer's Project



- 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 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.

TIP 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. If you use wireless networks, you may need to increase the values above the default.

Table 31 - More Resources

Resource	Description
Connection Reaction Time Limit on page 140	Provides more information on setting the RPI and understanding how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time
Monitor Safety Connections on page 198	Contains information on the CONNECTION_STATUS predefined data type
Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011	Provides detailed information on using produced and consumed tags

Safety Tag Mapping

A safety routine cannot directly access standard tags. To allow standard tag data to be used within safety task routines, the GuardLogix controllers provide a safety tag mapping feature that lets standard tag values be copied into safety task memory.

Mapped tags are copied from the standard tags to their corresponding safety tags at the beginning of the safety task. This can increase the safety task scan time.

TIP Standard task routines can directly read safety tags.

Restrictions

Safety tag mapping is subject to 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 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 key switch is in RUN position.
 - A nonrecoverable safety fault exists.
 - An invalid partnership exists between the primary controller and safety partner.

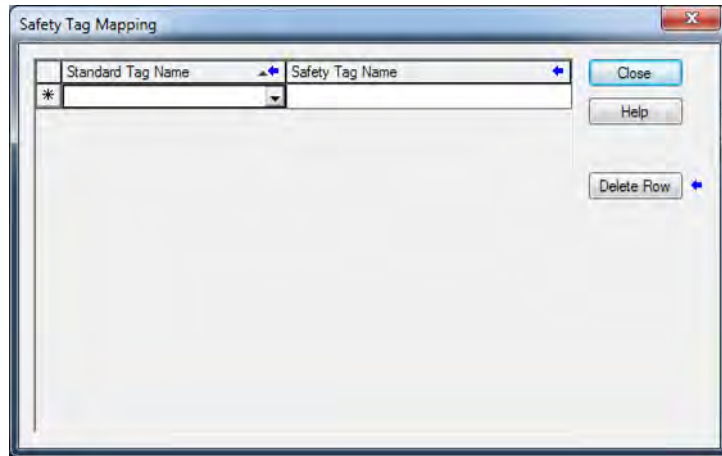


ATTENTION: When using standard data in a safety routine, you must verify that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 2/PLd or SIL 3/PLe safety output with standard tag data.

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

Create Tag Mapping Pairs

1. Choose Map Safety Tags from the Logic menu to open the Safety Tag Mapping dialog box.



2. Add an existing tag to the Standard Tag Name or Safety Tag Name column by typing the tag name into the cell or choosing a tag from the pull-down menu.

Click the arrow to display a filtered tag browser dialog box. If you are in the Standard Tag Name column, the browser shows only controller-scoped standard tags. If you are in the Safety Tag Name column, the browser shows controller-scoped safety tags.







3. Add a new tag to the Standard Tag Name or Safety Tag Name column by right-clicking in the empty cell and selecting New Tag and typing the tag name into the cell.
4. Right-click in the cell and choose New tagname, where tagname is the text you entered in the cell.

Monitor Tag Mapping Status

The leftmost column of the Safety Tag Mapping dialog box indicates the status of the mapped pair.

Table 32 - Tag Mapping Status Icons

Cell Contents	Description
Empty	Tag mapping is valid.
	When offline, the X icon indicates that tag mapping is invalid. You can move to another row or close the Safety Tag Mapping dialog box. ⁽¹⁾ When online, an invalid tag map results in an error message explaining why the mapping is invalid. You cannot move to another row or close the Safety Tag Mapping dialog box if a tag mapping error exists.
	Indicates the row that currently has the focus.
	Represents the Create New Mapped Tag row.
	Represents a pending edit.

(1) Tag mapping is also checked during project verification. Invalid tag mapping results in a project verification error.

For more information, see the tag mapping restrictions on page [186](#).

Safety Application Protection

You can protect your application program from unauthorized changes by generating a safety signature, setting passwords, and safety-locking the controller.

Safety-lock the Controller



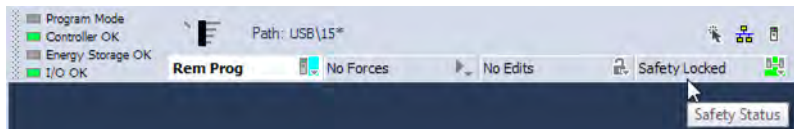
ATTENTION: Safety-locking alone does not satisfy SIL 2/PLd or SIL 3/PLe requirements.

You can safety-lock the GuardLogix 5580 controller to protect safety-related control components from modification, and prevent the safety signature from being deleted accidentally.

The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety Add-On Instructions, safety tags, safety I/O, and the safety signature.

TIP There are multiple ways to view the safety lock status of the controller:

- The 4-character display on the controller indicates lock status.
- In the Logix Designer application, the text of the online bar's safety status button indicates the safety-lock status.



- The Logix Designer application tray also displays the following icons to indicate the safety controller's safety-lock status.



= controller safety-locked



= controller safety-unlocked

You can safety-lock the controller project regardless of whether you are online or offline and regardless of whether you have the original source of the program. However, no safety forces or pending online safety edits can be present.

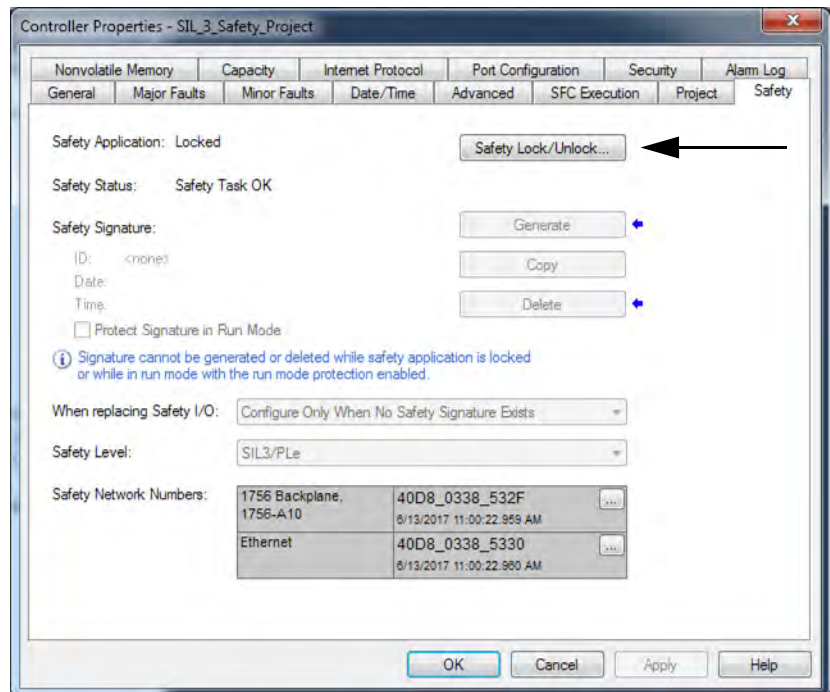
You cannot change the Safety-locked or -unlocked status when the controller keyswitch is in the RUN position.

TIP Safety-lock or -unlock actions are logged in the controller log.

For more information on accessing the controller log, refer to Logix 5000 Controllers Controller Information and Status Programming Manual, publication [1756-PM015](#).

You can safety-lock and -unlock the controller from the Safety tab of the Controller Properties dialog box.

Figure 42 - Safety-lock the Controller



TIP In the Logix Designer application, you can also choose Tools > Safety > Safety Lock/Unlock.

If you set a password for the safety-lock feature, you must type it in the Enter Password field. Otherwise, click Lock.

Figure 43 - Safety-locking the Controller



You can also set or change the password from the Safety Lock dialog box. See [Set Passwords for Safety-locking and Unlocking on page 191](#).

The safety-lock feature, described in this section, and standard security measures in the Logix Designer application are applicable to GuardLogix controller projects.

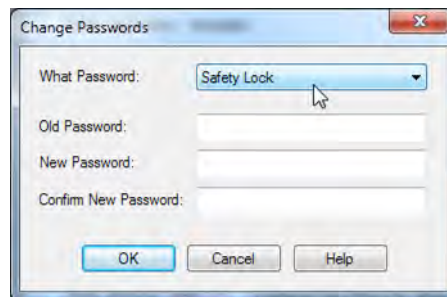
Refer to the Logix 5000 Controllers Security Programming Manual, publication [1756-PM016](#), for information on Logix Designer security features.

Set Passwords for Safety-locking and Unlocking

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

Follow these steps to set passwords.

1. On the Logix Designer menu bar, click Tools > Safety > Change Passwords.
2. From the What Password pull-down menu, choose either Safety Lock or Safety Unlock.



3. Type the old password, if one exists.
4. Type and confirm the new password.
5. Click OK.

TIP 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.

Generate a Safety Signature

IMPORTANT To generate a signature, the controller must be in Program mode.

Before verification testing, you must generate the safety signature. You can generate the safety signature only when these conditions exist:

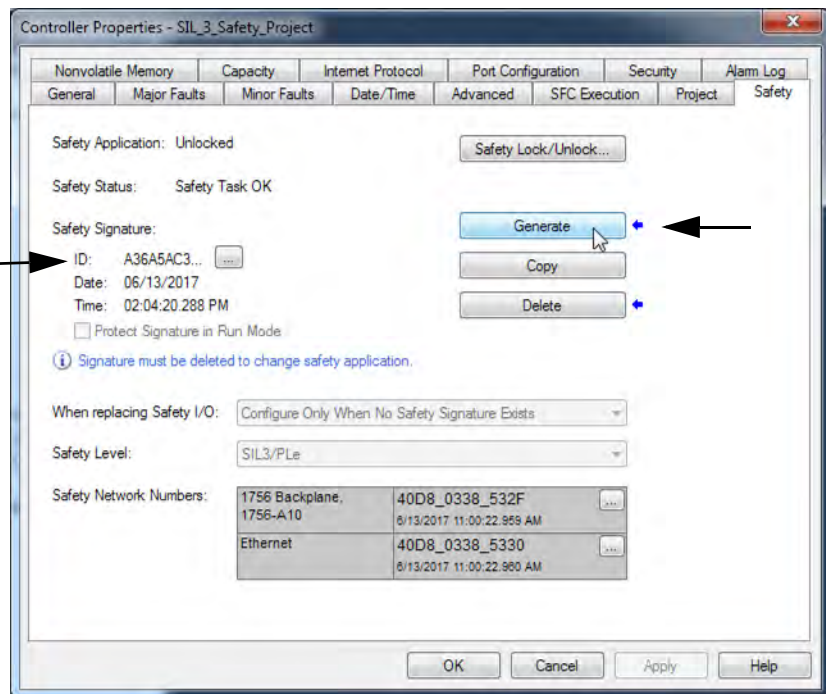
- The safety-unlocked GuardLogix 5580 controller project is online.
- There are no safety forces, pending online safety edits, or safety faults.
- The safety status must be Safety Task OK.

TIP You can view the safety status via the safety status button on the online bar, or on the Safety tab of the Controller Properties dialog box.

To generate the safety signature from the Safety tab of the Controller Properties dialog box, click Generate.

Figure 44 - Generate Safety Signature

For the safety signature, GuardLogix 5580 controllers have a 32 byte ID. Only the first 4 bytes of the ID display on the tab. To view and copy the entire 32 byte ID, click [...] to open the Safety Signature ID dialog box.



TIP In the Logix Designer application, you can also choose Tools > Safety > Generate Signature.

If a previous signature exists, you are prompted to overwrite it.

TIP Safety signature creation and deletion is logged in the controller log. For more information on accessing the controller log, refer to Logix 5000 Controllers Controller 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
- Safety data manipulation (except by safety routine logic)
- Download a new safety application

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.

Click Copy to copy the ID, Date, and Time components to the Windows clipboard.

Delete the Safety Signature

Click Delete to delete the safety signature. The safety signature cannot be deleted when the following is true:

- The controller is safety-locked.
- The controller is in Run mode with the keyswitch in RUN.
- The controller is in Run or Remote Run mode with Protect Signature in Run Mode enabled.



ATTENTION: If you delete the safety signature, you must retest and re-validate your system to meet SIL2/PLd or SIL 3/PLe.

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

Programming Restrictions

Restrictions limiting the availability of some menu items and features (that is, cut, paste, delete, and replace) are imposed by the Logix Designer application 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 apply, 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 new 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.

Monitor Safety Status

You can use the following to monitor the controller status:

- The Online bar in the Logix Designer application.
- The Safety tab in the Controller Properties dialog box.


View Status via the Online Bar

The online bar displays project and controller information, including the controller status, force status, online edit status, and safety status.

Figure 45 - Status Buttons

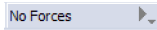


Controller Status


When the Controller Status button  is selected as shown above, the online bar shows the controller's mode (Remote Program) and status (OK). The Energy Storage OK indicator combines the status of the primary controller and the safety partner.

If either or both have an energy storage fault, the status indicator illuminates. The I/O indicator combines the status of standard and safety I/O. The I/O with the most significant error status is displayed next to the status indicator.

Forces status

The Forces Status button  indicates Forces or No Forces. When the button is selected, the online bar shows whether I/O or SFC forces is enabled or disabled and installed or not installed. The ForcesStatus menu contains commands to remove, enable, or disable all forces.

Online Edit status

The Online Edit Status button  indicates whether edits or no edits exist in the online ladder routine or function block diagram. When the button is selected, the online bar shows the edit state of the controller. If edits are made by another user, this area will also shows a textual description of the edits.

Safety Status


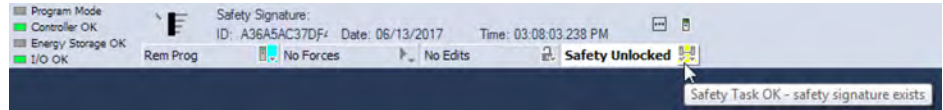
When you click the Safety Status button , the online bar displays the safety signature.

Figure 46 - Safety Signature Online Display



The Safety Status button itself indicates whether the controller is safety-locked or -unlocked, or faulted. It also displays an icon that shows the safety status.













When a safety signature exists, the icons include a small check mark. 

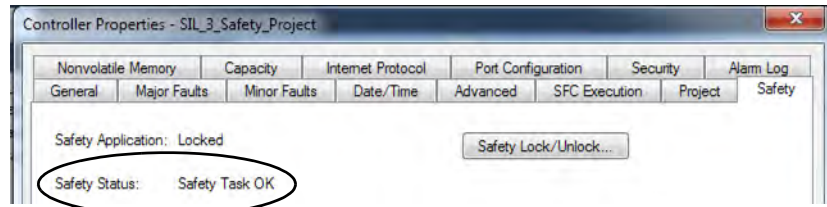
Table 33 - Safety Status Icon

If the safety status is	This icon appears	
	SIL 2/PLd Application, both online and offline	SIL 3/PLe Application
Safety Unlocked		 The controller is not safety locked and online.  The controller is not safety locked and offline.
Safety Locked		 The controller is safety locked and online.  The controller is safety locked and offline.
Safety Faulted		
Safety Task Inoperable	 The controller is not safety locked and the safety task is inoperable  The controller is safety locked and the safety task is inoperable.  There is a safety fault and the safety task is inoperable.	

View Status via the Safety Tab

View controller safety status information on the safety status button on the online bar and on the Safety tab of the Controller Properties dialog box.

Figure 47 - Safety Task Status



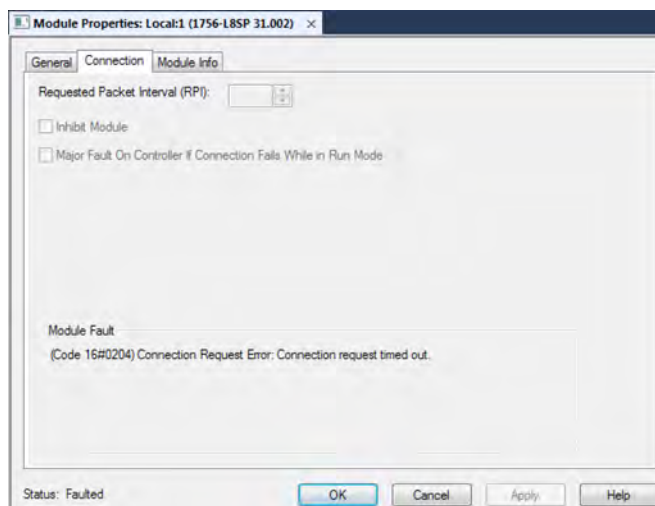
- Safety partner is missing or unavailable (SIL 3).
- Safety partner hardware is incompatible with primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety task OK.

With the exception of safety task OK, the descriptions indicate that nonrecoverable safety faults exist.

See [Major Safety Faults \(Type 14\) on page 203](#) for fault codes and corrective actions.

The status of the safety partner can be viewed on the Connections tab of its Module Properties dialog box.

Figure 48 - Safety Partner Status



Monitor Safety Connections

For tags associated with consumed safety data, you can monitor the status of safety connections by using the CONNECTION_STATUS member. For monitoring input and output connections, safety I/O tags have a connection status member called SafetyStatus. Both data types contain two bits: ConnectionFaulted and RunMode.

The ConnectionFaulted value indicates whether the safety connection between the safety producer and the safety consumer is Valid (0) or Faulted (1). If ConnectionFaulted is set to Faulted (1) for any reason, the safety data is reset to zero and the RunMode value is set to Idle State (0).

The RunMode value indicates if consumed data is actively being updated by a device that is in the Run Mode (1) or Idle State (0). Idle state is indicated if the connection is closed, the safety task is faulted, or the remote controller or device is in Program mode or Test mode. For safety I/O connections, the RunMode is always inverse the ConnectionFaulted status. It does not provide unique data.

The following table describes the combinations of the ConnectionFaulted and RunMode states.

Table 34 - Safety Connection Status

ConnectionFaulted Status	RunMode Status	Safety Connection Operation
0 = Valid	1 = Run	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Valid	0 = Idle	The connection is active and the producing device is in the Idle state. The safety data is reset to zero. This applies to consumed connections only.
1 = Faulted	0 = Idle	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero and the RunMode value is set to Idle State (0).
1 = Faulted	1 = Run	Invalid state.

If a device is inhibited, the ConnectionFaulted bit is set to Faulted (1) and the RunMode bit is set to Idle (0) for each connection associated with the device. As a result, safety consumed data is reset to zero.

Utilizing Status

Connection Status(.ConnectionFaulted) is the status of the safety connection between the safety controller and safety I/O module. When the connection is operating properly, this bit will be LO (0). When the connection is NOT operating properly, this bit will be HI (1). When the connection status is HI (connection not operating properly), all of the other module defined tags are LO, and should be considered 'invalid' data.

Point Status is available for both safety inputs (.PtxxInputStatus) and safety outputs (.PtxxOutputStatus). When a point status tag is HI (1), it indicates that individual channel is functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which this channel resides is operating properly.

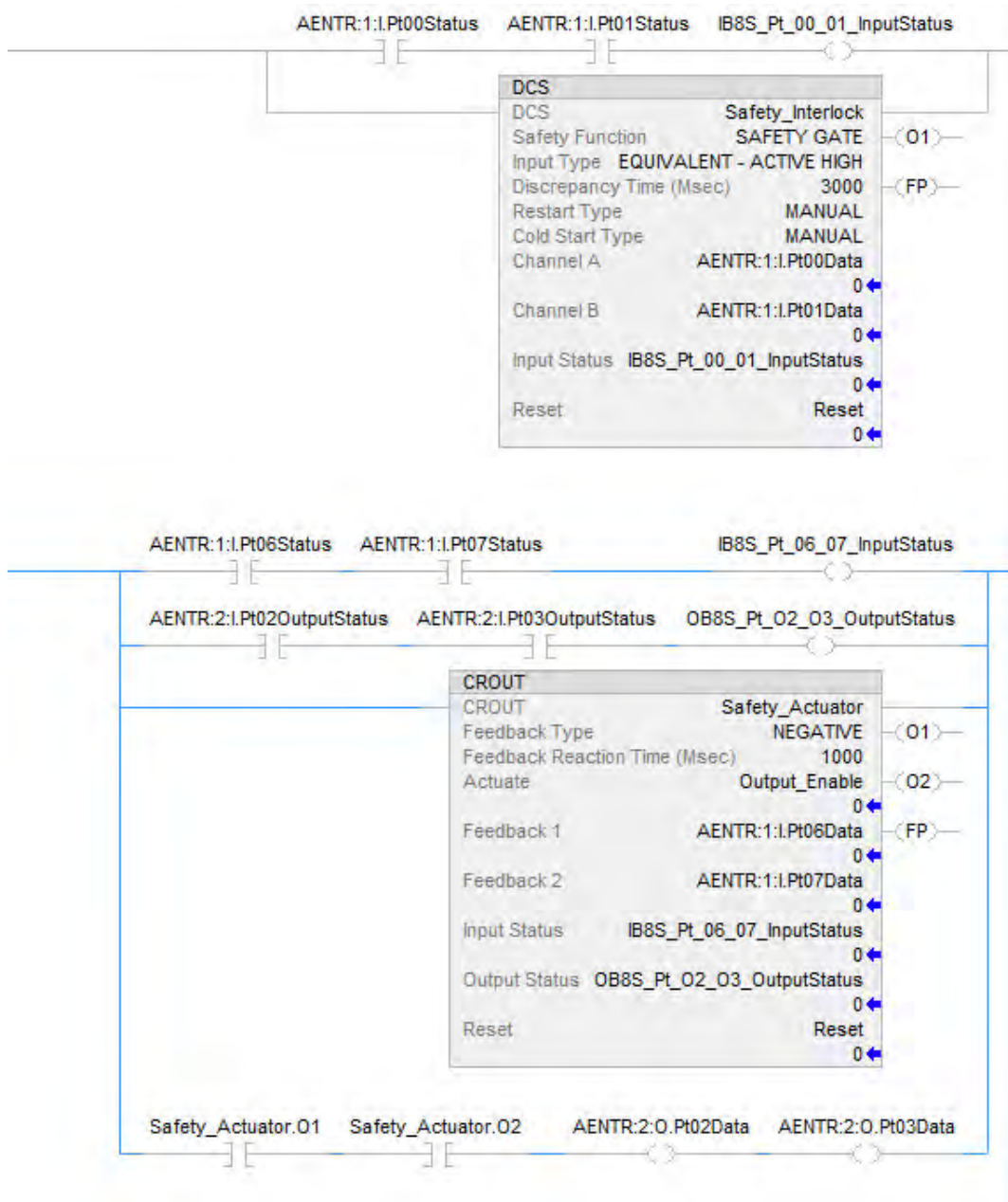
Combined Status is also available for both safety inputs (.CombinedInputStatus) and safety outputs (.CombinedOutputStatus). When the combined status tag is HI (1), it indicates that all input or output channels on the module are functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which these channels reside is operating properly.

Whether combined status or point status is used is application dependent. Point status simply provides more granular status.

The dual-channel 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) has input status for input channels A and B. The CROUT instruction has input status for Feedbacks 1 and 2, and has output status for the output channels driven by the CROUT outputs O1 and O2. The status tags used in these instructions must be HI (1) for the safety instruction output tag(s) (O1 for input instructions and O1/O2 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 [Figure 49](#).

Figure 49 - Instruction Examples



Safety I/O status should be interrogated when using instructions such as XIC and OTE. The responsibility for this falls to the user. The user should verify safety input channel status is HI (1) before using a safety input channel as an interlock. The user should verify safety output channel status is HI (1) before energizing a safety output channel.

Safety Faults

Major Faults in the GuardLogix system can be:

- Recoverable controller faults
- Nonrecoverable controller faults
- Nonrecoverable safety faults in the safety application
- Recoverable safety faults in the safety application

Nonrecoverable Controller Faults

These occur when the controller's internal diagnostics fail. 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.

If a fault occurs, diagnostic data is automatically written to the SD card. Rockwell Automation can then use the data to help investigate the cause of the fault. Contact Technical Support.

Nonrecoverable Safety Faults in the Safety Application

If a nonrecoverable safety fault occurs in the safety application, safety logic and the safety protocol are terminated. 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.

If a safety signature exists, you can clear the fault to enable the safety task to run. If no safety signature exists, the safety task cannot run again until the entire application is downloaded again.

- If you use the Clear Majors button or Clear Faults menu item in Logix Designer to clear the fault, the standard application should continue to run while the safety application is recovered from the snapshot.
- If you use the keyswitch method (turn the keyswitch to Program, then back to Run), the safety application is recovered from the snapshot, but the standard application briefly transitions out of Run mode.

Recoverable Faults in the Safety Application

If a recoverable fault occurs in the safety application, the system can halt the execution of the safety task, depending upon whether or not the fault is handled by Program Fault Routines in the safety application.

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 program execution is stopped, and safety protocol connections are closed and reopened to re-initialize 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 eliminate these faults, rather than handling them at run-time.



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.

View Faults

The Recent Faults dialog box on the Major Faults tab of the Controller Properties dialog box contains two sub-tabs, one for standard faults and one for safety faults.

The status display on the controller also shows fault codes with a brief status message, as described beginning on page [205](#).

Fault Codes

[Table 35](#) shows the fault codes specific to GuardLogix controllers. The type and code correspond to the type and code displayed on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

Table 35 - Major Safety Faults (Type 14)

Code	Cause	Status	Corrective Action
01	Task watchdog expired. User task has not completed in a specified period of time. A program error caused an infinite loop, the program is too complex to execute as quickly as specified, a higher priority task is keeping this task from finishing, or the safety partner has been removed.	Nonrecoverable	Clear the fault. If a safety signature exists, safety memory is re-initialized and the safety task begins executing. If a safety signature does not exist, you must re-download the program so the safety task can run. Reinsert the safety partner, if it was removed.
02	An error exists in a routine of the safety task.	Recoverable	Correct the error in the user-program logic.
03	Safety partner is missing.	Nonrecoverable	Install a compatible safety partner.
04	Safety partner is unavailable.	Nonrecoverable	Install a compatible safety partner.
05	Safety partner hardware is incompatible.	Nonrecoverable	Install a compatible safety partner.
06	Safety partner firmware is incompatible.	Nonrecoverable	Update the safety partner so that the firmware major and minor revision matches the primary controller.
07	Safety task is inoperable. This fault occurs when the safety logic is invalid, for example a mismatch in logic exists between the primary controller and safety partner, a watchdog timeout occurred, or memory is corrupt.	Nonrecoverable	Clear the fault. If a safety signature exists, safety memory is re-initialized via the safety signature and the safety task begins executing. If a safety signature does not exist, you must download the program again so the safety task can run.
09	Safety partner nonrecoverable controller fault.	Nonrecoverable	Clear the fault and download the program. If the problem persists, replace the safety partner.

The Logix 5000 Controllers Major and Minor Faults Programming Manual, publication [1756-PM014](#), contains descriptions of the fault codes common to Logix controllers.

Develop a 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 run-time.

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 as described on page [205](#).

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 and Minor Faults Programming Manual, publication [1756-PM014](#), provides details on creating and testing a fault routine.

Use 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. Note that 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.

Access FaultRecord Attributes

Create a user-defined structure to simplify access to the MajorFaultRecord and SafetyTaskFaultRecord attributes.

Table 36 - Parameters for Accessing FaultRecord Attributes

Name	Data Type	Style	Description
TimeLow	DINT	Decimal	Lower 32 bits of the fault timestamp value
TimeHigh	DINT	Decimal	Upper 32 bits of the fault timestamp 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)

Capture Fault Information

The SafetyStatus and SafetyTaskFaultRecord attributes can capture information about non-recoverable 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 in conjunction 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](#).

Notes:

Develop Secure Applications

Topic	Page
Controller Security Features	208
Configure Trusted Slot	213
Configure User-definable Major Faults	214
License-based Source and Execution Protection	216
Configure Change Detection	219
Controller Audit Log	220
Disable the Ethernet Port	221
Disable the CIP Security Ports	225
Disable the USB Port	228
Disable the SD Card	230
Disable the 4-character Status Display	232
Disable the Controller Web Pages	236

Applies to these controllers:

ControlLogix 5580

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

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

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

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

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

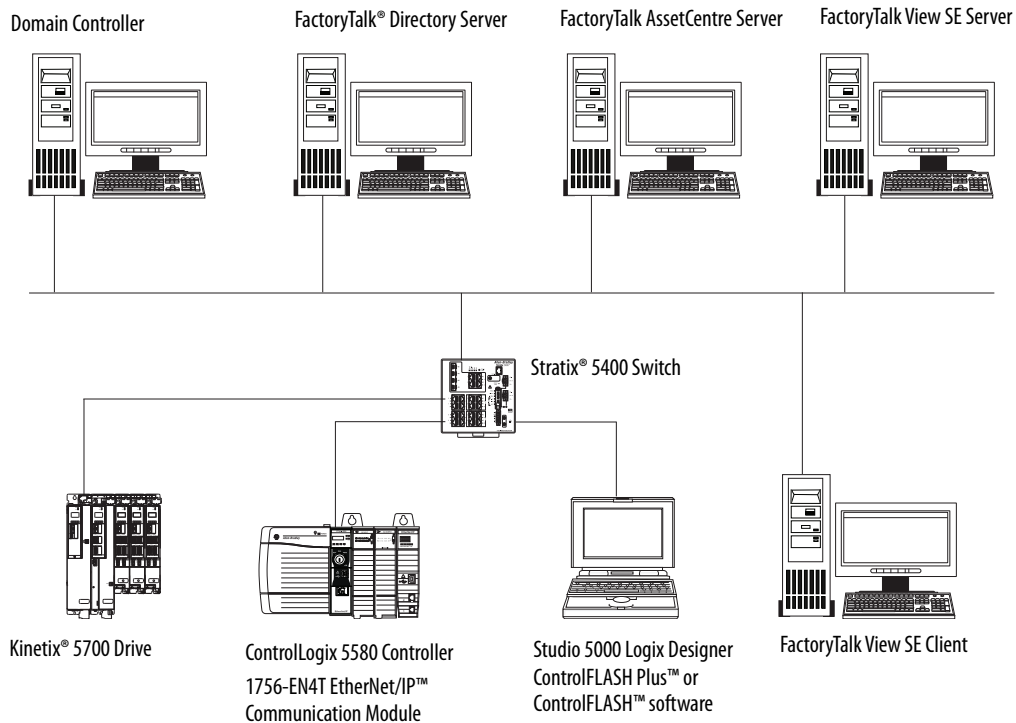
The controller accepts all values appropriate for a tag data type, and it is the responsibility of the user program to specify valid ranges and perform validity checking for those ranges. The controller verifies incoming messages for syntax, length, and format.

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

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

Controller Security Features

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



System-level Security Features

Rockwell Automation offers several products that have features that increase security at the system level. Use the following checklist to secure your controller system.

To harden the control system:

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	ControlFLASH Plus™ or ControlFLASH™ software	Yes	Use ControlFLASH Plus or ControlFLASH software to update controller firmware. Digitally signed firmware files have a .DMK (Device Management Kit) extension. ControlFLASH software authenticates the origin of a DMK file and validates the file before download in the device.
	Studio 5000 Logix Designer application	Yes	You can generate a signature on an Add-On Instruction. This signature seals (encrypts) the Add-On Instruction to help prevent modification.
	FactoryTalk AssetCentre software	Yes	The FactoryTalk AssetCentre server assists with backup and recovery. Backups do not interfere with controller operation. Configure the appropriate backup operation based on your system design, threat model, and risk assessment. For more information, see Configure System Security Features User Manual, SECURE-UM001 .

To monitor the control system:

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	The FactoryTalk AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes. 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 .

To manage programmatic user access:

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	Studio 5000 Logix Designer application	Yes	Configure the controller project in Logix Designer to use these user access methods. <ul style="list-style-type: none"> License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. The Logix Designer application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag. For more information, see Logix 5000 Controllers Security Programming Manual, 1756-PM016

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk Security software Studio 5000 Logix Designer application	Yes	<p>Configure FactoryTalk Security to define policies, user groups, and other permission sets.</p> <ul style="list-style-type: none"> The Logix Designer application enforces the policy based on the access policies that are provided to it by FT 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. In FactoryTalk Security, define which users can change controller modes and download projects to the controller. Security authority binding restricts the controller to a specific FactoryTalk Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>
	FactoryTalk Policy Manager software	Yes	<p>Use the FactoryTalk Policy Manager software to define a secure data transport over an EtherNet/IP network to the controller.</p> <p>For more information, see Configure System Security Features User Manual, SECURE-UM001.</p>

Controller-specific Security Features

The controller supports these product-specific features that you use with the system-level features. Use the following checklist to physically secure your controller.

To harden the controller:

✓	Controller Feature	Required to Meet IEC-62443-4-2 SL 1	Details
	Firmware update	Yes	To meet IEC-62443-4-2 SL 1 security requirements, you must use the latest available revision of controller firmware. The controller is designed such that: <ul style="list-style-type: none"> You cannot update firmware when the keyswitch is in the RUN position. You cannot go online with a controller that is in a firmware update process. For more information, see page 55 .
	SD card encryption	May be required based on system design, threat model, and risk assessment.	If your system allows SD card use, the load process to the SD card encrypts and digitally signs the project by using the controller key. The SD card itself is not encrypted. When you save (load) firmware to the SD card, the process stores encrypted firmware and certificates on the SD 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 SD Card. This can help prevent against potential loss of controller logs before FactoryTalk AssetCentre can read them. For more information, see page 91 .
	Trusted slot	To maintain network segmentation, configure Trusted slot.	The trusted slot feature restricts communication paths through which certain operations are performed on Logix 5000™ controllers. A trusted slot is not configured by default. For more information, see page 213 .
	User-definable major faults	May be required based on system design, threat model, and risk assessment.	If your application requires a require a major fault, in addition to those already monitored by the controller, define a predetermined state with a major fault so that outputs are off. For more information, see page 221 .

To monitor the controller:

✓	Controller Feature	Required to Meet IEC-62443-4-2 SL 1	Details
	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. <ul style="list-style-type: none"> License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. The Logix Designer application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag. For more information, see page 216 . Yes
	Change detection	Yes	Enable the change detection feature to monitor program components to determine whether they change. The change detection feature is not enabled by default. For more information, see page 219 .
	Controller audit log	Yes	The controller audit log automatically stores security-related events that can be written accessed via FactoryTalk AssetCentre software. For more information, see page 220 .

To manage physical user access to the controller:

✓	Controller Feature	Required to Meet IEC-62443-4-2 SL 1	Details
	Keyswitch position	May be required based on system design, threat model, and risk assessment.	Place the keyswitch in RUN position to help prevent unauthorized remote configuration changes to the controller, and restrict some communication services. Remove the keyswitch from a running controller to help prevent modifications to the configuration or program. IMPORTANT: Do not apply a new security policy while the controller is in RUN mode. RUN mode does not help prevent updates to the security policy, and a policy change has the potential to disrupt a running control system
	Disable the Ethernet port	May be required based on system design, threat model, and risk assessment.	The Ethernet port is enabled by default. Disable the Ethernet port if required by the system design, threat model, or risk assessment. For more information, see page 221 .
	Disable Simple Network Management Protocol (SNMP)	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 page 108 .
	Disable the CIP Security ports	May be required based on system design, threat model, and risk assessment.	CIP Security ports on the controller are enabled by default. Disable the CIP Security ports if required by the system design, threat model, or risk assessment. For more information, see page 225 .
	Disable the USB ports	May be required based on system design, threat model, and risk assessment.	The USB port on the controller is enabled by default. Disable the USB port if required by the system design, threat model, or risk assessment. For more information, see page 228 .
	Disable the SD card	May be required based on system design, threat model, and risk assessment.	The SD card is enabled by default. Disable the SD card if required by the system design, threat model, or risk assessment. For more information, see page 230 .
	Disable Controller web pages	May be required based on system design, threat model, and risk assessment.	Controller web pages for diagnostics are read-only. With Studio 5000 Logix Designer application version 33.00.00 and later, controller web pages are disabled by default. If the controller web pages are currently enabled, then disable the controller web pages if required by the system design, threat model, or risk assessment. For more information, see page 236 .

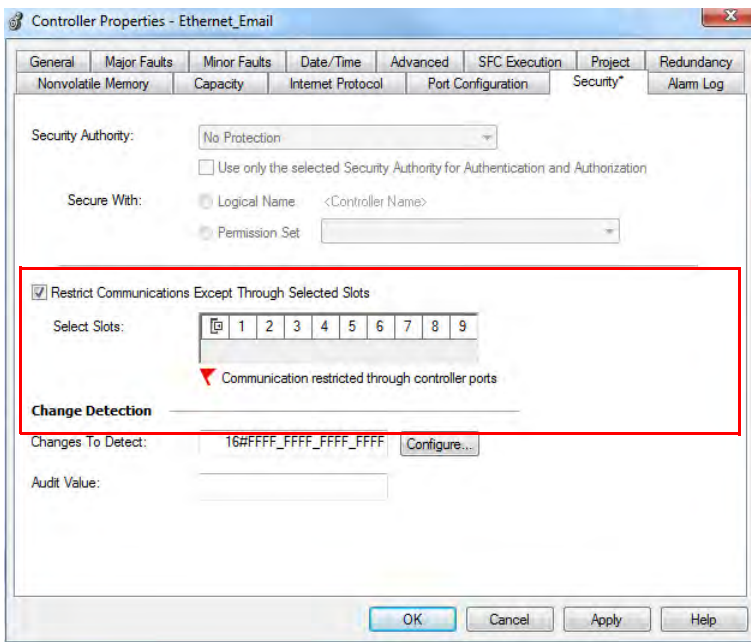
Verification of Security Implementation

Follow the above checklists to secure the system and controller. It is your responsibility to periodically monitor the system to ensure the security settings function as you configured them. For example:

- Attempt to log in with an invalid user name or password.
- Attempt to access a disabled USB port.

Configure Trusted Slot

To maintain network segmentation, configure Trusted slot. On the Controller Properties Security tab, the trusted slot feature restricts the communication paths through which certain operations are performed on Logix controllers.



Restrict Communication except through Selected Slots

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

IMPORTANT When this checkbox is selected, communication is restricted through USB or serial ports and firmware updates are restricted to trusted slots when using AutoFlash, or ControlFLASH Plus and ControlFLASH software. Support is restricted for tools that require access to restricted data through class 3 connections.

Select Slots

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

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

Configure User-definable Major Faults

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

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

To create a user-defined major fault, do the following:

1. Create a fault routine for the program.
2. Configure the program to use the fault routine.
3. Jump to the fault routine.

Create a Fault Routine

To create a fault routine, do the following:

1. In the Controller Organizer, right-click the program and click Add > New Routine.
2. On the New Routine dialog box, in the Name field, type a name for the fault routine.
3. In the Type field, use the default setting, Ladder Diagram.
4. In the In Program or Phase field, select the program or phase where the routine will reside.
5. In the Assignment field, select Fault.
6. (optional) Select the Open Routine checkbox, to open the ladder logic program immediately.
7. Click OK.

Configure the Program to Use the Fault Routine

To configure the program to use the fault routine, do the following:

1. In the Controller Organizer, right-click the program and click Properties.
2. On the Properties dialog box, click the Configuration tab.
3. In the Fault field, select the fault routine.
4. Click OK.

Jump to the Fault Routine

In the main routine of the program, enter the following rung, where:

- Fault_Routine_1 is the name of the fault routine for the program.
- 999 is the value for the fault code.



When $\text{Tag}_1.0 = 1$, execution jumps to `name_of_fault_routine`, a major fault occurs and the controller enters the faulted mode. Outputs go to the faulted state. The Controller Properties dialog box, Major Faults tab, displays the code 999.

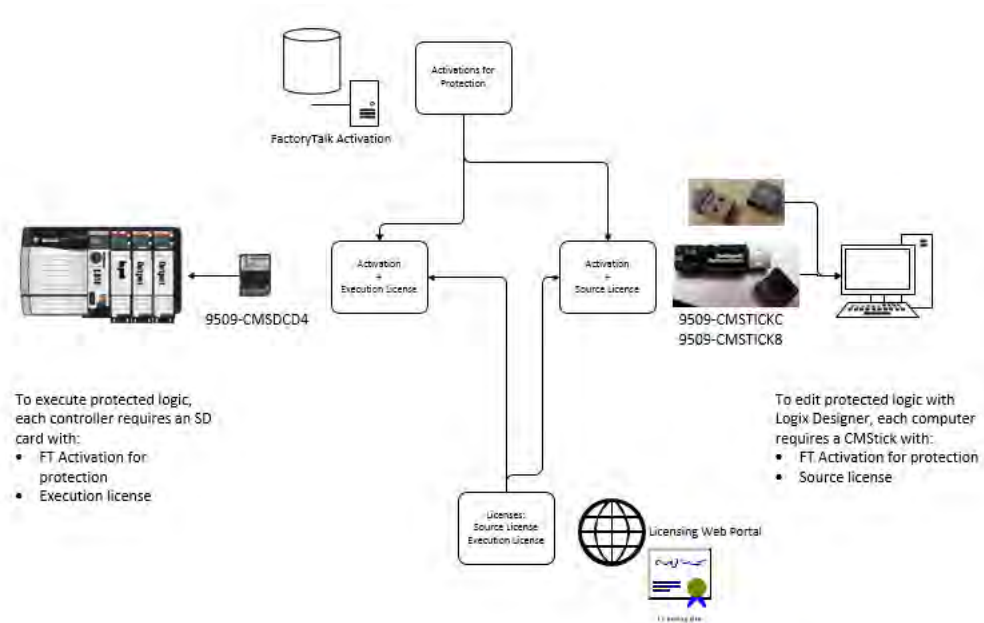


License-based Source and Execution Protection

Source protection helps prevent logic components from being modified based on a license.

Execution protection adds additional protection to controller logic. Execution protection makes sure that the right controller has access to execute the protected program. Use this with source protection to make sure the right programmer has access to modify the logic.

Each device (controller or computer) requires an activation to access protection features. Each logic component or program requires a license to be accessed or executed.

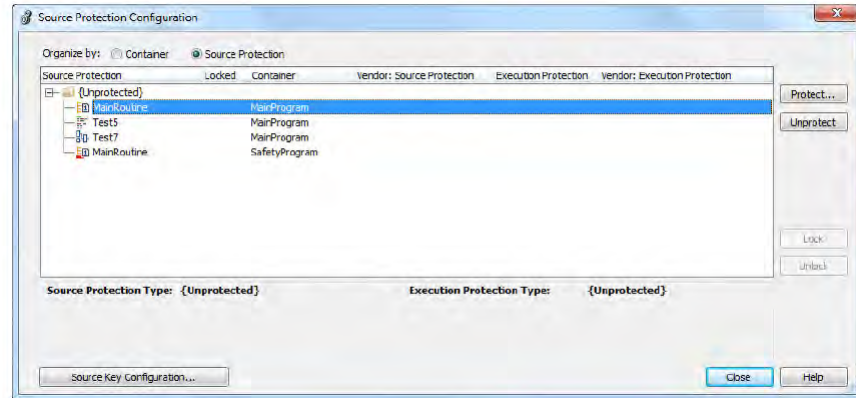


To apply license-based protection, you need the following:

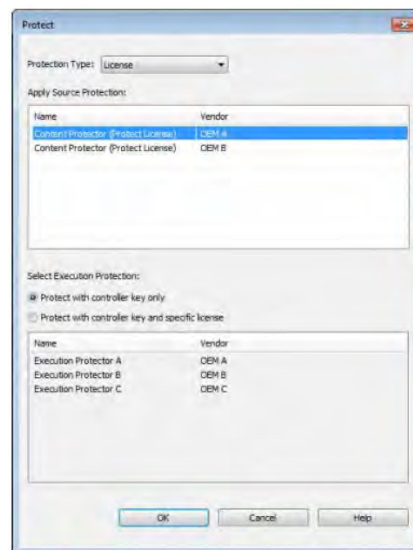
- A CmStick that contains a license with Use permission must be present locally on any USB port on the computer. Use permission cannot be obtained from a network license server. All other license privileges can be contained on the local CmStick, or provided by a license server on the network.
- A license that contains the Protect permission, either on a local CmStick or provided by a license server on the network. When components are locked, unauthorized users cannot view or edit the component, but authorized users can run the project without a CmStick.

Enable License-based Protection

1. Click 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. On ControlLogix 5580 and GuardLogix 5580 controllers, select the Execution Protection type:
 - Protect with controller key only. This option is selected by default. With this option selected, the component, when locked, runs only on a controller in the same family as the one specified for the project. For example, if you lock a License-based Protected component for a project on a ControlLogix 5580 controller, the component can only be executed on another ControlLogix 5580 controller.

- Protect with controller key and specific license. When you select this option, the component runs only on a controller in the same family as the one specified for the project and that contains a CmCard with the execution license that you select. If you select Protect with controller key and specific license, select the execution license from the list of available licenses.

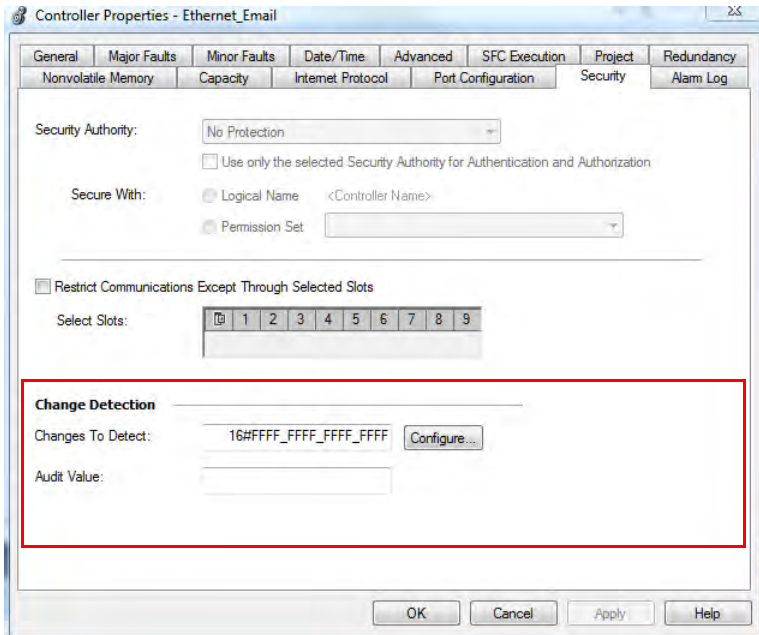
On ControlLogix 5580 and GuardLogix 5580 controllers, after components are protected, they can also be locked. When you lock a component, it prevents users from viewing or editing the component, but allows authorized users to run it.

6. To return to the Source Protection Configuration dialog box, click OK.

TIP To save changes to a component that is protected with License-Based Source Protection, a CmStick that contains the required license must be plugged into the computer that runs the Logix Designer application. Make sure that you save your edits to the project or lock the protected components before removing the CmStick that contains the required license. If the license is not present, you could lose your edits to the project.

Configure Change Detection

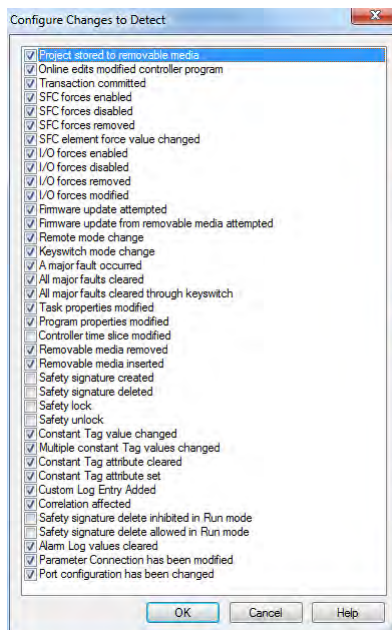
On the Controller Properties Security tab, the Change Detection Feature tracks a set of program components and audits whether these components have changed.



Changes to Detect

Identifies the types of events that can cause the Audit Value box to change. By default, all event types can cause the Audit Value to change, results in a default value of: 0xFFFFFFFFFFFFFFFF.

Click Configure to open the Configure Changes to Detect dialog box. We recommend tracking these changes for a standard ControlLogix 5580 controller:



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 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.

Controller Audit Log

The controller audit log stores various security-related events that can be written to an SD card or accessed via FactoryTalk Asset Center. Some of these events are Logix Designer application request errors, control system events, backup/restore events, and configuration changes.

- With Studio 5000 Logix Designer application version 32 or earlier, the log holds 100 events, and then rolls over and overwrites the data that is there.
- With Studio 5000 Logix Designer application version 33 or later, the log holds 500 events, and then rolls over and overwrites the data that is there.

For a more robust logging and to help prevent rollover, use FactoryTalk AssetCentre.

Disable the Ethernet Port

You can disable the controller Ethernet port with the Studio 5000 Logix Designer application, version 28.00.00 or later.

IMPORTANT Remember the following:

- Once a port is disabled, you lose any connection that is established through the controller Ethernet port.
 - You cannot disable Ethernet ports if the controller keyswitch is in Run mode or if the FactoryTalk Security settings deny this editing option.
-

Ethernet ports return to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset
- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - These examples clear the program from a controller:
 - Major non-recoverable fault occurs.
 - Firmware update occurs.

You must reconfigure the settings to disable an Ethernet port after the port returns to its default settings.

There are two ways to disable the Ethernet port:

- [Disable the Ethernet Port on the Port Configuration Tab on page 222](#)
- [Disable the Ethernet Port with a MSG Instruction on page 223](#)

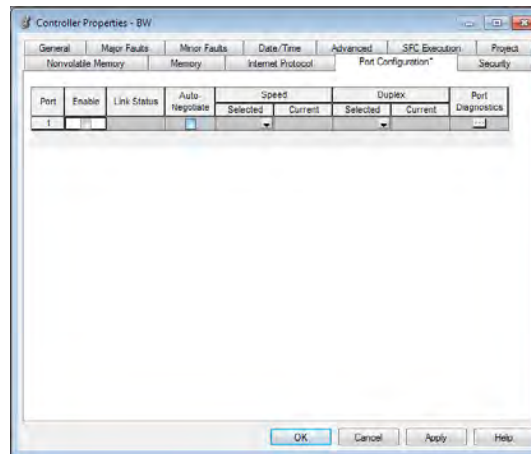
Disable the Ethernet Port on the Port Configuration Tab

You can disable the embedded Ethernet port on the controller. This method retains the setting in the project, so every time you download the project to the controller, the Ethernet port is disabled.

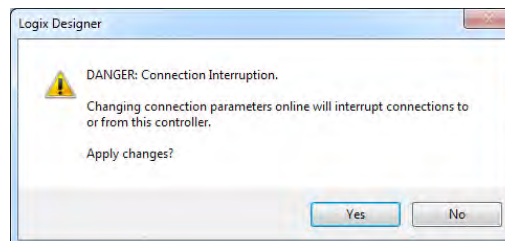
1. On the Online toolbar, click the Controller Properties button.



2. On the Controller Properties dialog box, click the Port Configuration tab.
3. On the Port Configuration tab, clear the Enable checkbox.



4. On the Port Configuration tab, click Apply.
 - If you are online when you make this change, then an Alert dialog box appears. On the dialog box, click Yes. The change takes effect immediately.



- If you are offline, then the change takes effect when you download the program to the controller.
5. On the Port Configuration tab, click OK.

Disable the Ethernet Port with a MSG Instruction

You use a CIP Generic MSG with a Path of THIS to execute this option. You cannot use this MSG instruction to disable the Ethernet port on a different controller.

1. Add a 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 a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

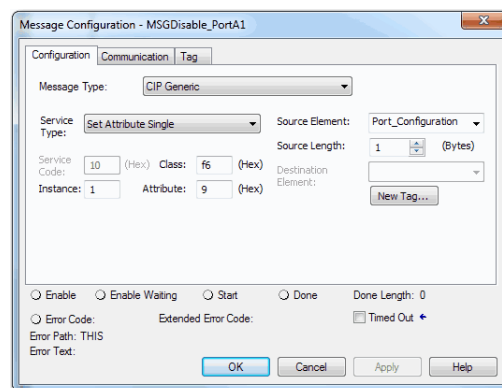
2. Configure the Configuration tab on the Message Configuration dialog box as follows:

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

- Message Type - CIP Generic
- Service Type - Set Attribute Single
- Instance - 1
- Class - f6
- Attribute - 9
- Source Element - Controller tag of SINT data type

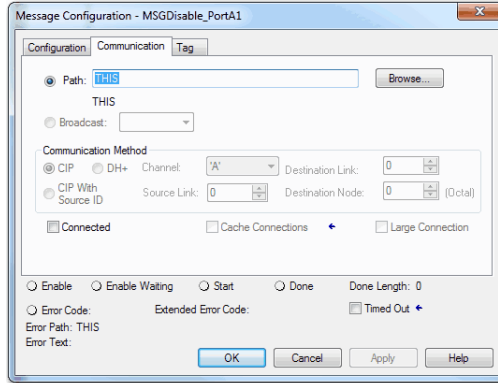
In this example, the controller tag is named Port_Configuration.

- Source Length - 1



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

IMPORTANT Messages to THIS must be unconnected messages.



4. Before you enable the MSG instruction, make sure that the Source Element tag value is 2.

IMPORTANT You can re-enable an Ethernet port after it is disabled.

To re-enable the port, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 1.

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

IMPORTANT This procedure disables the CIP Security ports. To re-enable the ports, you must use the controller reset button to perform a Stage 2 reset (return the controller to a factory default state). See [Stage 2 Reset on page 88](#).

You cannot use this MSG instruction to disable the CIP security ports on a different controller.

The message only has to execute once, it does not need to execute with every program scan.

1. Create a controller tag of SINT[9] data type.

In this example, the controller tag is named CIPSEC_DISABLE and must match the following graphic.

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

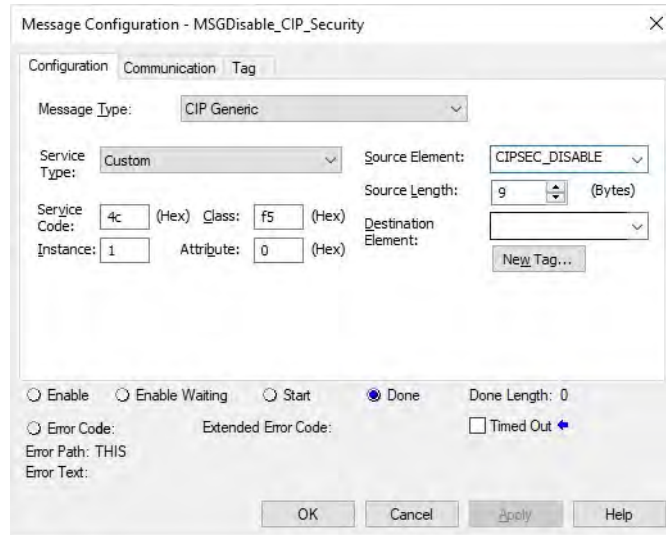
Before you enable the MSG instruction, consider the following:

- 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 a MSG instruction to your program.

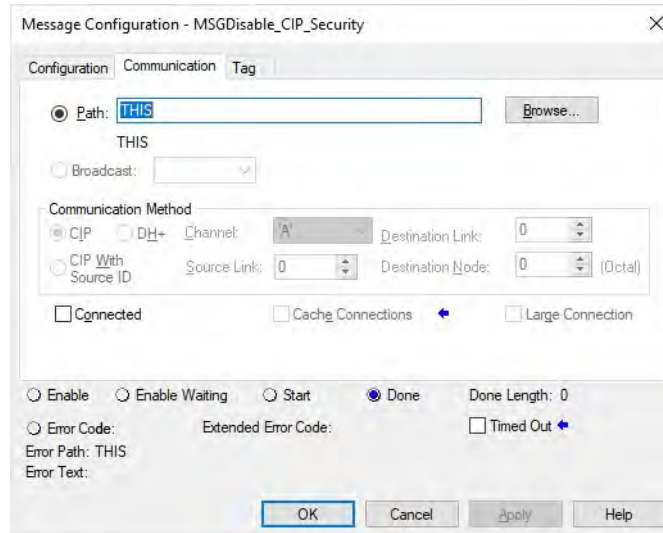
IMPORTANT You cannot add a MSG instruction to your program if the controller keyswitch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

3. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Custom
 - Service Code - 4c
 - Instance - 1
 - Class - f5
 - Attribute - 0
 - Source Element - Controller tag of SINT[9] data type. This is the controller tag that you created in step 1.
 - Source Length - 9



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

IMPORTANT Messages to THIS must be unconnected messages.



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

Disable the USB Port

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

1. Add a 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 a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

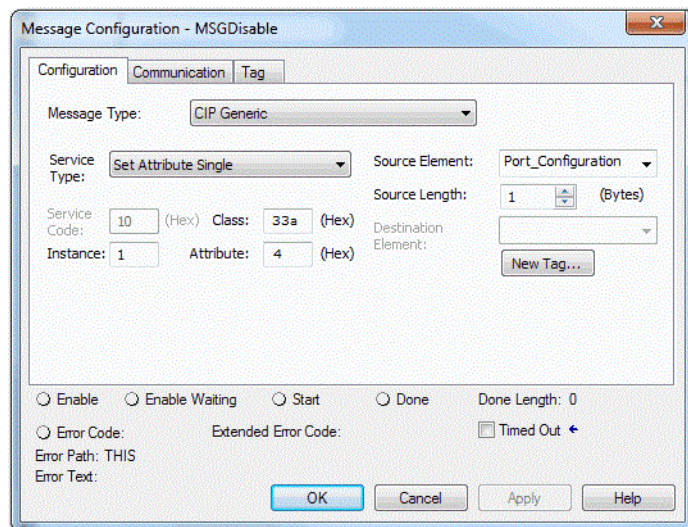
2. Configure the Configuration tab on the Message Configuration dialog box as follows:

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

- Message Type - CIP Generic
- Service Type - Set Attribute Single
- Instance - 1
- Class - 33a
- Attribute - 4
- Source Element - Controller tag of SINT data type.

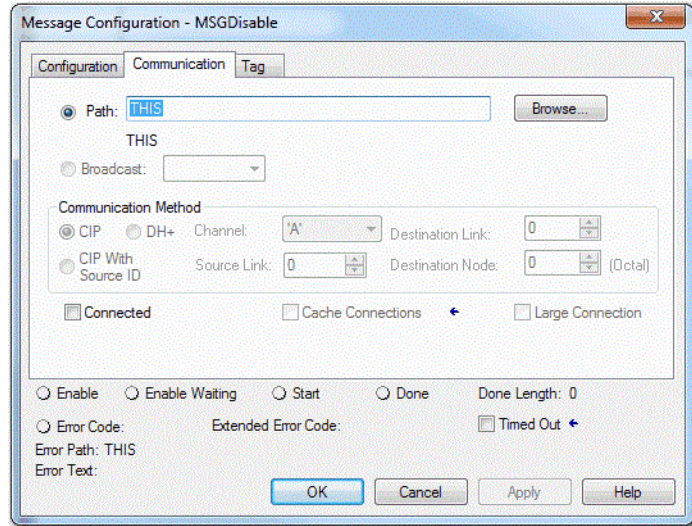
In this example, the Source Element is named Port_Configuration.

- Source Length - 1



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

IMPORTANT Messages to THIS must be unconnected messages.



Disable the SD Card

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

IMPORTANT Remember the following:

- An SD card can only be disabled with a message to self.
 - Once an SD Slot is disabled, you lose all and any ability to communicate to an SD Card inserted into the slot. This includes any diagnostic information.
 - You can re-enable the SD card again:
 - with a stage 2 reset
 - and with V33 firmware or later, a message to self
-

1. Add a MSG instruction to your program.

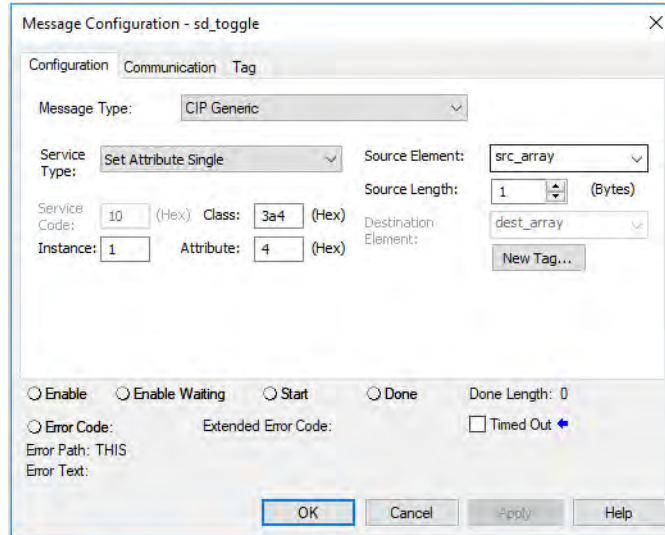
This message only has to execute once, it does not need to execute with every program scan.

IMPORTANT You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:

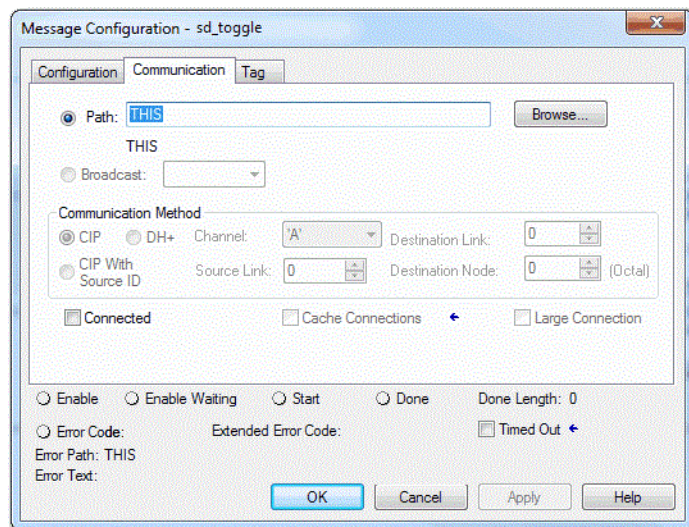
IMPORTANT These values are stored to NVS memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

- Message Type - CIP Generic
- Service Type - Set Attribute Single
- Instance - 1
- Class - 3a4
- Attribute - 4
- Source Element - Controller tag of SINT Array.
In this example, the Source Element is named src_array.
- Source Length - 1



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

IMPORTANT Messages to THIS must be unconnected messages.



Disable the 4-character Status Display

With the Studio 5000 Logix Designer application, version 29.00.00 or later, you can disable certain categories of messages on the 4-character status display:

- [Disable All Categories of Messages on page 232](#)
- [Disable Individual Categories of Messages on page 234](#)

You use a CIP Generic MSG to execute each option.

IMPORTANT You cannot disable these system messages, and they will always display:

- Powerup 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 non-recoverable fault occurs.
 - Firmware update occurs.

You must reconfigure the settings to disable the 4-character status display after it returns to its default settings.

Disable All Categories of Messages

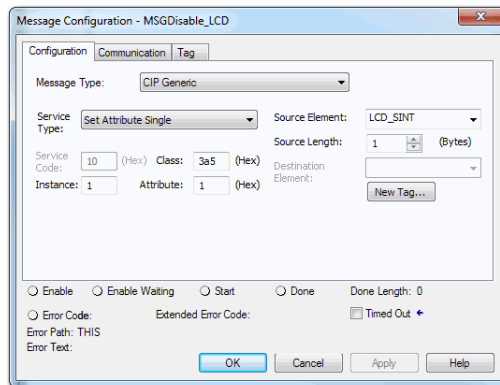
When you disable all categories of messages, this information no longer shows:

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

Complete these steps.

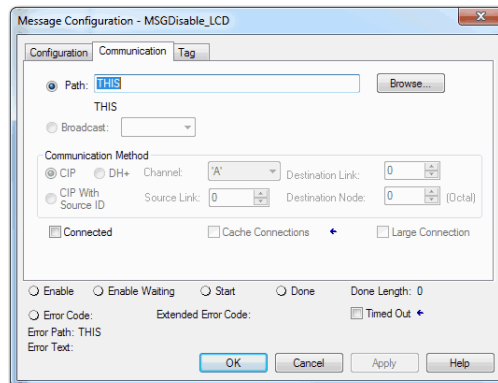
1. Add a MSG instruction to your program.
2. Configure the Configuration tab on the Message Configuration dialog box:
 - Message Type - CIP Generic
 - Service Type - Set Attribute Single
 - Instance - 1
 - Class - 3a5
 - Attribute - 1

- Source Element - Controller tag of SINT data type
In this example, the controller tag is named LCD_SINT.
- Source Length - 1



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 4-character display after it is disabled.

To re-enable the 4-character display, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 0.

Disable Individual Categories of Messages

You can disable a subset of the information that scrolls across the controller 4-character display. You can disable these subsets:

- Project name and link status
- Port status and IP address

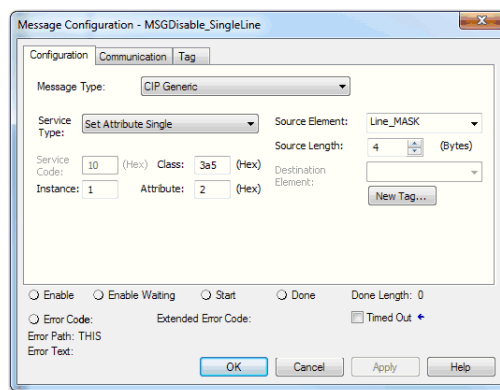
Complete these steps.

1. Add a MSG instruction to your program.

This message only has to execute once, it does not need to execute with every program scan.

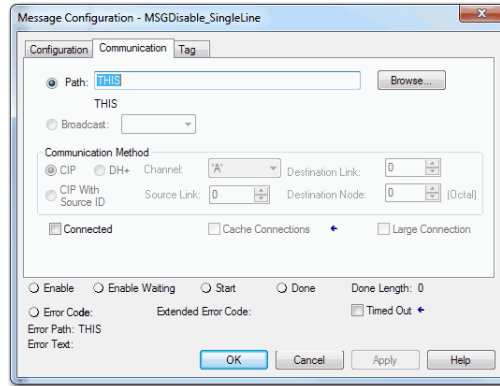
IMPORTANT You cannot add a MSG instruction to your program if the controller keyswitch is in Run mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Set Attribute Single
 - Instance - 1
 - Class - 3a5
 - Attribute - 2
 - Source Element - Controller tag of DINT data type
In this example, the controller tag is named Line_MASK.
 - Source Length - 4



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

IMPORTANT Messages to THIS must be unconnected messages.



- Before you enable the MSG instruction, make sure that the Source Element uses one of the following tag values that are based on what information that you want to disable:
 - Project name and link status - Bit 0 of the Source Element = 1
 - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT You can re-enable the subsets of information on the 4-character display after they are disabled.

To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure the appropriate bit in the Source Element tag value is 0.

Disable the Controller Web Pages

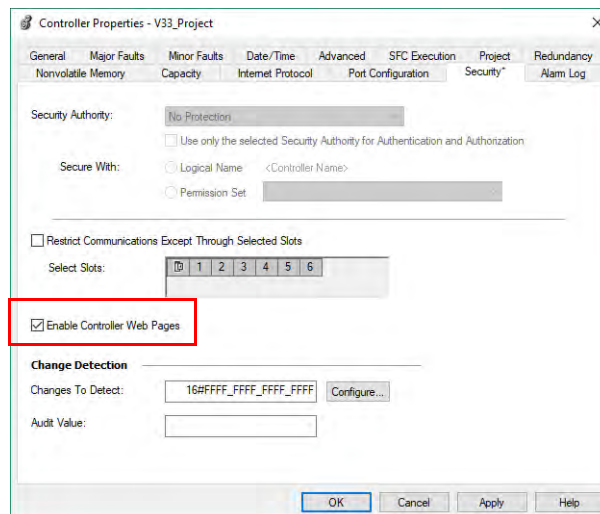
You can disable the controller web pages with the Studio 5000 Logix Designer application, version 28.00.00 or later.

Studio 5000 Logix Designer Application Version 33.00.00 and Later

With the Studio 5000 Logix Designer application version 33.00.00 and later, controller web pages are disabled by default.

While using a CIP Generic MSG to disable Controller Web pages is supported in version 33.00.00 and later, Rockwell Automation recommends these methods to disable the controller web pages:

- If the controller web pages are enabled, clear the check box on the Logix Designer Controller Properties Security tab to disable the webpages.



- For CIP Security applications, you can also use FactoryTalk Policy Manager to disable the web pages (this overrides the Controller Properties check box).

Studio 5000 Logix Designer Application Version 32.00.00 or Earlier

For Studio 5000 Logix Designer application, version 32.00.00 or earlier, you use a CIP Generic MSG to execute this option.

See:

- [Use a CIP Generic MSG to Disable the Controller Web Pages on page 238.](#)
- [Use a CIP Generic MSG to Enable the Controller Web Pages on page 240](#)

Controller Web Page Default Settings

The default settings for controller web pages are:

- Web pages enabled for controller firmware revision 32 and earlier.
- Web pages disabled for controller firmware revision 33 and later.

Controller web pages return to the default setting in these situations:

- A stage 1 reset for all versions of the Logix Designer application.
- A stage 2 reset for all versions of the Logix Designer application.

IMPORTANT When you update the controller firmware to revision 33 or later without a reset, the controller retains the previous controller web page configuration (web pages enabled) and does not automatically change to the default setting for V33 (disable the web pages).

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

The setting of the controller web pages changes after the following occurs on the controller:

- New project is downloaded - in this case, the settings in the new project take effect.
- When the controller receives a configuration message, it takes the setting from the configuration message.

Use a CIP Generic MSG to Disable the Controller Web Pages

IMPORTANT If you use FactoryTalk Policy Manager to disable the web pages in a CIP Security application, the CIP generic message-to-self overrides the FactoryTalk Policy Manager setting.

1. Add a MSG instruction to your program.

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

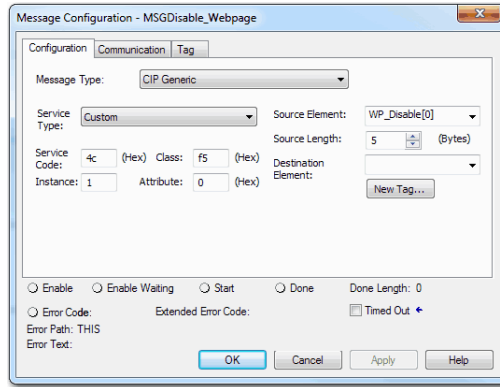
2. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Custom
 - Service Code - 4c
 - Instance - 1
 - Class - f5
 - Attribute - 0
 - Source Element - Controller tag of SINT[5] data type.

In this example, the controller tag is named WP_Disable and must match the following graphic.

IMPORTANT The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not disabled.

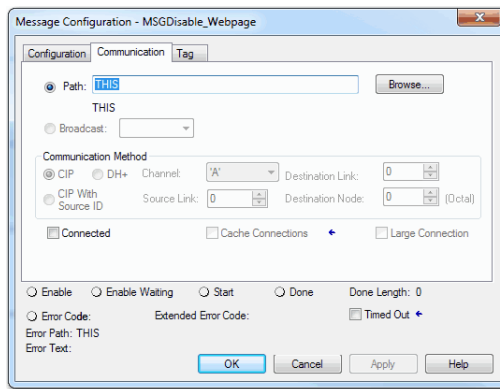
WP_Disable	{...}	Decimal	SINT[5]
WP_Disable[0]	1	Decimal	SINT
WP_Disable[1]	80	Decimal	SINT
WP_Disable[2]	0	Decimal	SINT
WP_Disable[3]	6	Decimal	SINT
WP_Disable[4]	0	Decimal	SINT

– Source Length - 5



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

IMPORTANT Messages to THIS must be unconnected messages.



Use a CIP Generic MSG to Enable the Controller Web Pages

1. Add a MSG instruction to your program.

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

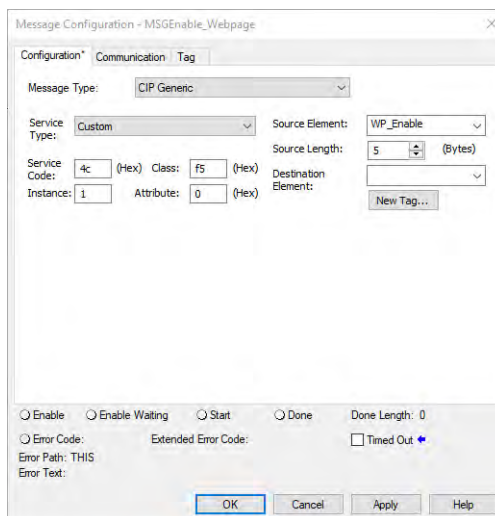
2. Configure the Configuration tab on the Message Configuration dialog box as follows:
 - Message Type - CIP Generic
 - Service Type - Custom
 - Service Code - 4c
 - Instance - 1
 - Class - f5
 - Attribute - 0
 - Source Element - Controller tag of SINT[5] data type.

In this example, the controller tag is named WP_Enable and must match the following graphic.

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.

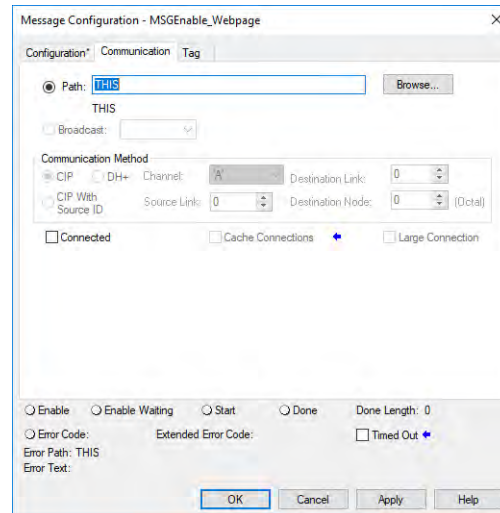
WP_Enable	{...}	Decimal	SINT[5]
WP_Enable[0]	1	Decimal	SINT
WP_Enable[1]	80	Decimal	SINT
WP_Enable[2]	0	Decimal	SINT
WP_Enable[3]	6	Decimal	SINT
WP_Enable[4]	1	Decimal	SINT

- Source Length - 5



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

IMPORTANT Messages to THIS must be unconnected messages.



Notes:

Develop Motion Applications

Topic	Page
Motion Overview	244
Obtain Axis Information	247
Program Motion Control	245

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controllers support these motion interfaces:

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

For more information, see these publications:

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

Motion Overview

The controllers support up to 256 axes of integrated motion. The 256 axes can be any combination of CIP™, Virtual, and Consumed axes. You can add all axes to one Motion Group, and you can assign any combination of axes to different axis update schedules.

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

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

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

1. Create a controller project.
2. Select the type of drive.

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

3. Create axis tags as needed.
4. Configure the drive.
5. Create axes as needed.

Program Motion Control

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

- The controller uses these instructions just like the rest of the Logix 5000™ instructions.
- Each motion instruction works on one or more axes.
- You can program by using motion control instructions in these programming languages:
 - Ladder Diagram (LD)
 - Structured Text (ST)
 - Sequential Function Chart (SFC)
- Each motion instruction needs a motion control tag. The tag uses a MOTION_INSTRUCTION data type and stores the information status of the instruction.

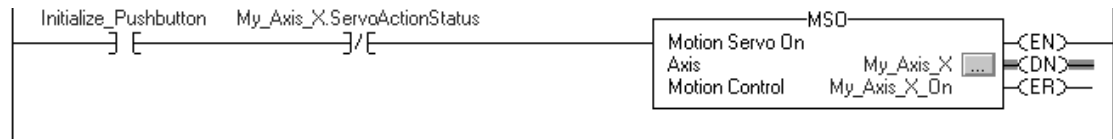
For more information, see the Logix 5000 Controller Motion Instructions Reference Manual, publication [MOTION-RM002](#).



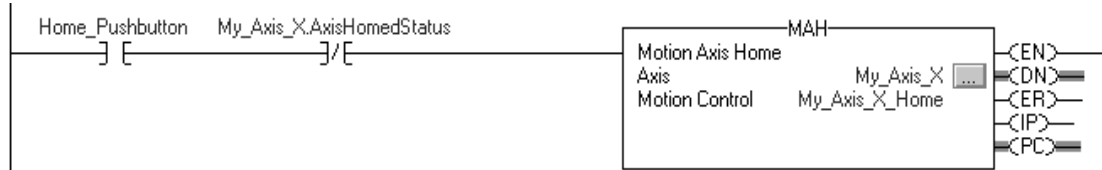
ATTENTION: Use each motion control tag in only one motion instruction. Unintended operation can result if you reuse the same motion control tag in other motion instructions, or if you write to any of the motion control tag elements.

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

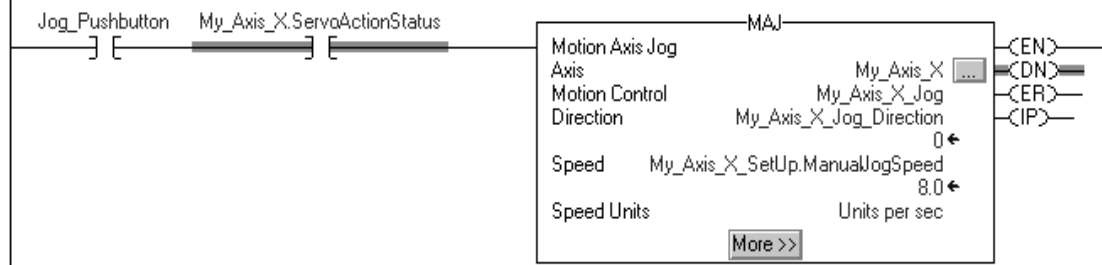
If Initialize_Pushbutton = on and the axis = off (My_Axis_X.ServoActionStatus = off) then the MSO instruction turns on the axis.



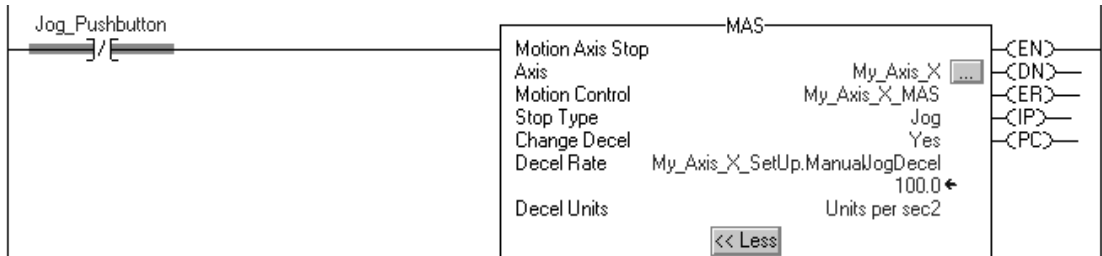
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off) then the MAH instruction homes the axis.



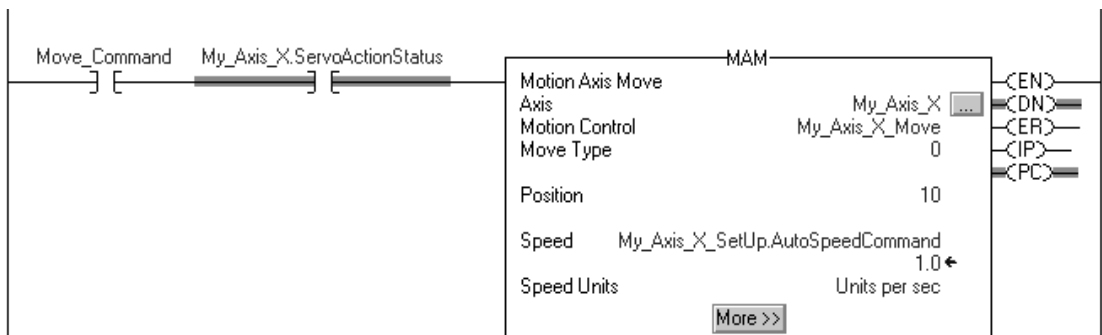
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAJ instruction jogs the axis forward at 8 units/second.



If Jog_Pushbutton = off then the MAS instruction stops the axis at 100 units/second². Make sure that Change Decel is Yes. Otherwise, the axis decelerates at its maximum speed.



If Move_Command = on and the axis = on (My_Axis_X.ServoActionStatus = on) then the MAM instruction moves the axis. The axis moves to the position of 10 units at 1 unit/second.

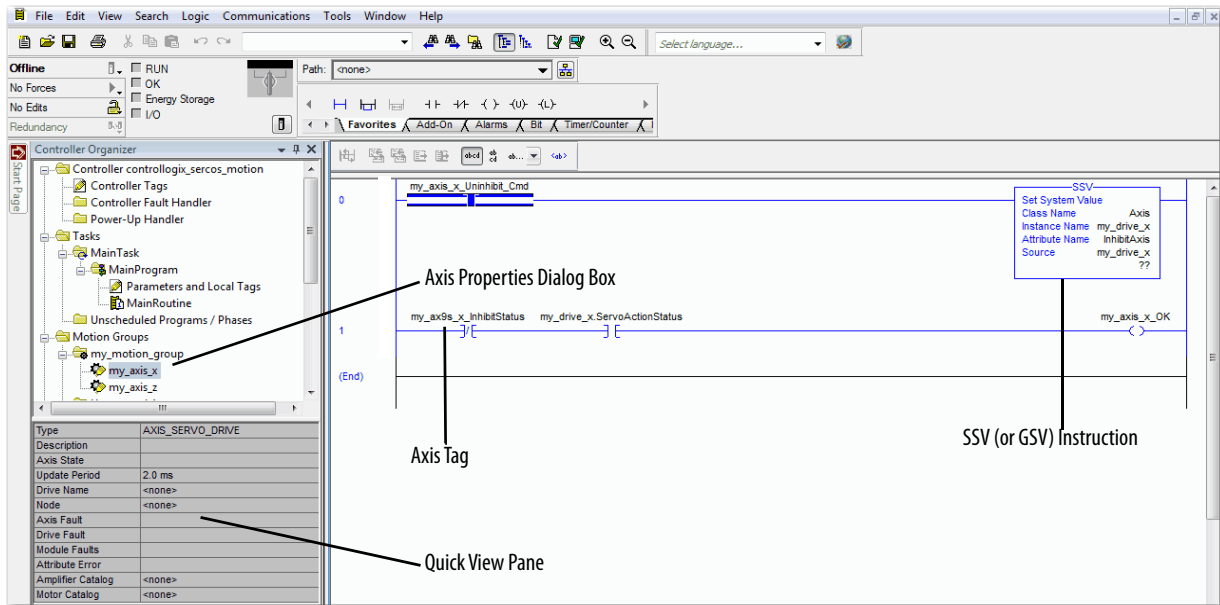


Obtain Axis Information

You can obtain axis information by using these methods:

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

Figure 50 - Obtain Axis Information



Notes:

Troubleshoot the Controller

Topic	Page
Automatic Diagnostics	249
Considerations for Communication Loss Diagnostics	250
Controller Diagnostics with Logix Designer	251
Controller Diagnostics with Linx-based Software	260
Controller Web Pages	261

This chapter describes how to troubleshoot the controller if issues occur during normal operation. In addition to the ways described in this chapter, you can use messages on the 4-character display to troubleshoot the controller. For more information, see [Status Indicators on page 267](#).

Automatic Diagnostics

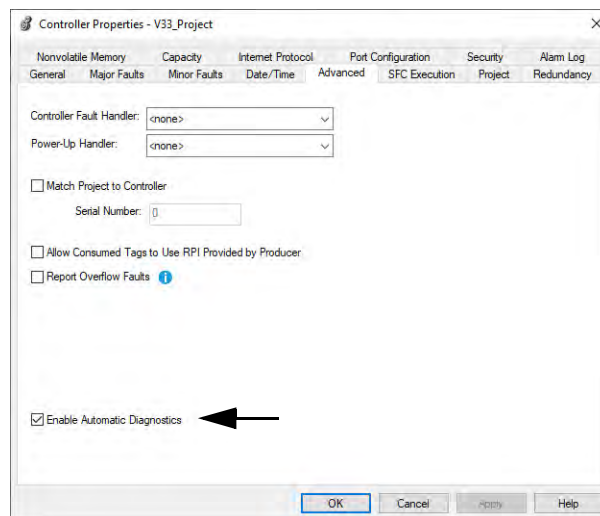
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

Automatic Diagnostics is enabled by default in Logix 5000 controllers with firmware revision 33 or later. You can disable and enable the whole feature while online or offline from the Advanced tab on the Controller Properties dialog. You can also disable Automatic Diagnostics for a specific device in the device's configuration.



Considerations for Communication Loss Diagnostics

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

Type of Connection	Device Behavior
Direct connection to a Logix 5000 controller	Device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter
No connection to a Logix 5000 controller	Communication adapters that do not have a connection to the controller do not report a communication loss diagnostics. It is recommended that you configure your communications adapters for a status connection to ensure they report any communication loss diagnostic in a timely manner.
Data connection	Device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter
Rack-optimized connection	Device does not report communication loss diagnostics. The communication adapter reports communication loss diagnostics. A device with a rack optimized connection has a reduced set of diagnostics as compared to a direct connection.

When enabled, the Automatic Diagnostics feature enables:

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

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

I/O Module Properties Tab

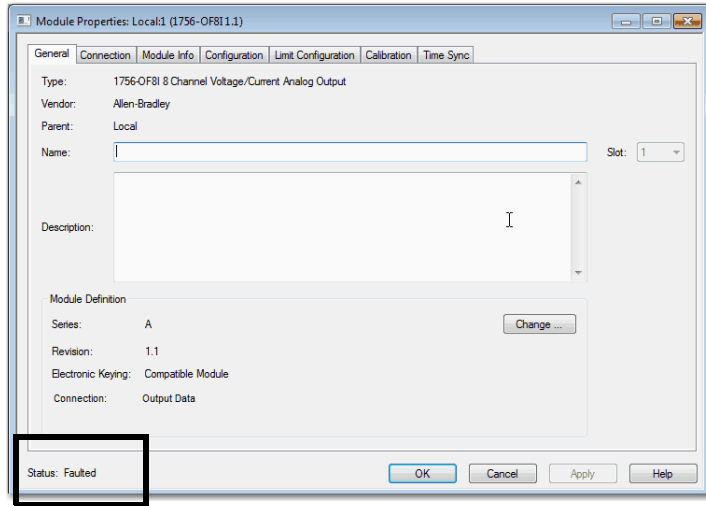
Applies to these controllers:

ControlLogix 5580

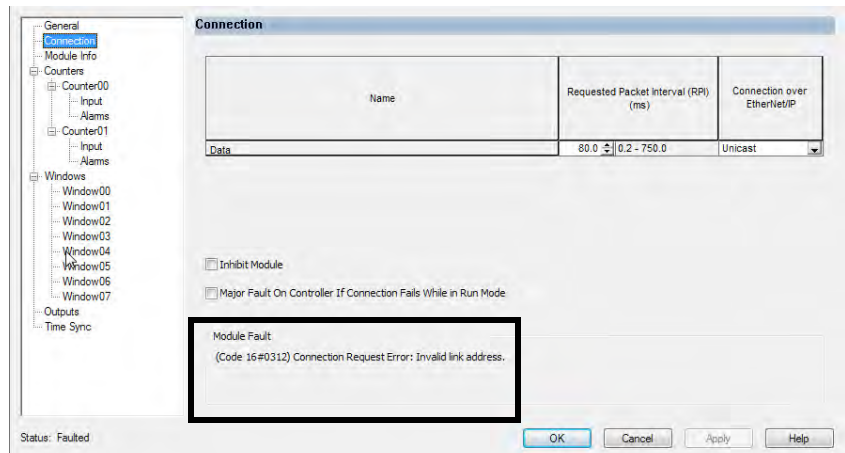
GuardLogix 5580

The General, Connection, and Module Info tabs show fault information.

- Message in the status line on the General Tab of an I/O module Properties.



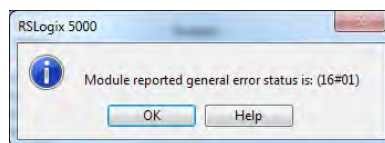
- The Connection tab shows the module fault. This example shows a communications fault.



- On the Module Info tab, the Status section lists the Major and Minor Faults along with the Internal State of the module.

The Module Info tab requires successful communications. If communication to the I/O module is OK, but the module itself is faulted, then the Module Info tab helps in troubleshooting the fault. If there is a communication fault, then the Connection Tab would be of more use.

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



Notification in the Tag Monitor

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

General module faults are also reported in the Tag Monitor. Diagnostic faults are reported only in the Tag Monitor. When the Value field is set to 1, a fault is present.

Figure 51 - I/O Module Fault

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

Figure 52 - Safety I/O Connection Fault

Name	Value	Force Mas	Style	Data Type
Remote_Safety_Input_2:I	{...}	{...}		AB:1732ES_IB12XOB4_Safe
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

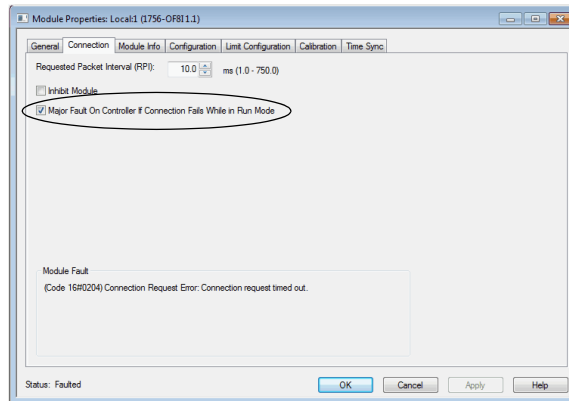
Applies to these controllers:

ControlLogix 5580

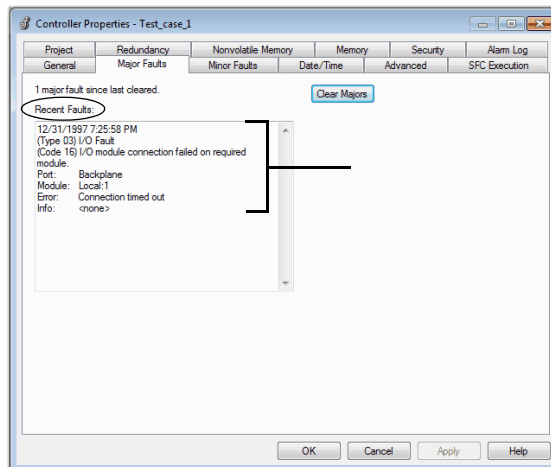
To display recent I/O fault information in the Major Faults tab of the Controller Properties screen, you must first check the Major Fault on Controller option on the I/O Properties Connection tab.



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.



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 indicates the type of fault under Recent Faults.



Port Diagnostics

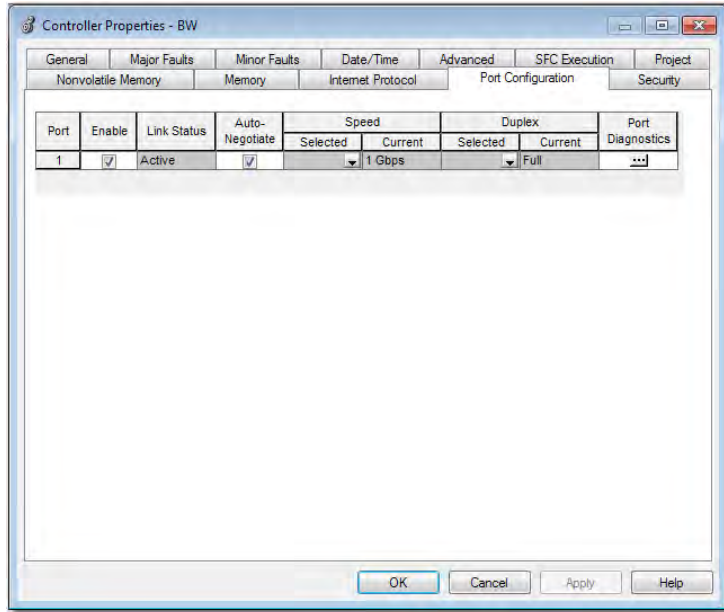
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

1. In the I/O Configuration, double-click on the controller to display the Controller Properties.
2. Click the Port Configuration tab.
3. On the Port Configuration tab, click the Port Diagnostics button.



The Port Diagnostics page, displays information for the port. See [Table 37 on page 256](#) for parameter descriptions.

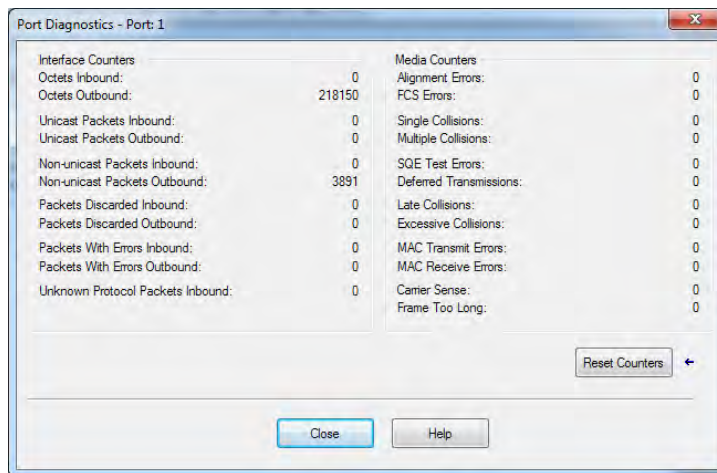


Table 37 - Port Diagnostics Parameters - Logix Designer Application

Parameter	Description
Interface Counters	The Interface Counters values have no value when you are offline or online and there is a communication error.
Octets Inbound	Displays the number of octets that are received on the interface.
Octets Outbound	Displays the number of octets that are transmitted to the interface.
Unicast Packets Inbound	Displays the number of unicast packets that are received on the interface.
Unicast Packets Outbound	Displays the number of unicast packets that are transmitted on the interface.
Non-unicast Packets Inbound	Displays the number of non-unicast packets that are received on the interface.
Non-unicast Packets Outbound	Displays the number of non-unicast packets that are transmitted on the interface.
Packets Discarded Inbound	Displays the number of inbound packets that are received on the interface but discarded.
Packets Discarded Outbound	Displays the number of outbound packets that are transmitted on the interface but discarded.
Packets With Errors Inbound	Displays the number of inbound packets that contain errors (excludes discarded inbound packets).
Packets With Errors Outbound	Displays the number of outbound packets that contain errors (excludes discarded outbound packets).
Unknown Protocol Packets Inbound	Displays the number of inbound packets with unknown protocol.
Media Counters	The Media Counters values have no value when you are offline or online and there is a communication error.
Alignment Errors	Displays the number of frames received that are not an integral number of octets in length.
FCS Errors	Displays the number of frames received that do not pass the FCS check.
Single Collisions	Displays the number of successfully transmitted frames that experienced exactly one collision.
Multiple Collisions	Displays the number of successfully transmitted frames that experienced multiple collisions.
SQE Test Errors	Displays the number of times an SQE test error message was generated.
Deferred Transmissions	Displays the number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Displays the number of times a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	Displays the number of frames for which transmission fails due to excessive collisions.
MAC Transmit Errors	Displays the number of frames for which transmission fails due to an internal MAC sub layer transmit error.
MAC Receive Errors	Displays the number of frames for which reception on an interface fails due to an internal MAC sub layer receive error.
Carrier Sense	Displays the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frame Too Long	Displays the number of frames received that exceed the maximum permitted frame size.
Reset Counters	Click Reset Counter to cause the interface and media counter values on the module to set to zero, and the values in the dialog to update to the current counter values. Reset Counter appears dimmed when: <ul style="list-style-type: none"> • offline • online and a communication error has occurred

Advanced Time Sync

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The Advanced Time Sync dialog displays information that is related to CIP Sync™ time synchronization. The information appears only if the project is online, and Time Synchronization is enabled on the Date/Time tab.

IMPORTANT Precision Time Protocol (PTP) Software

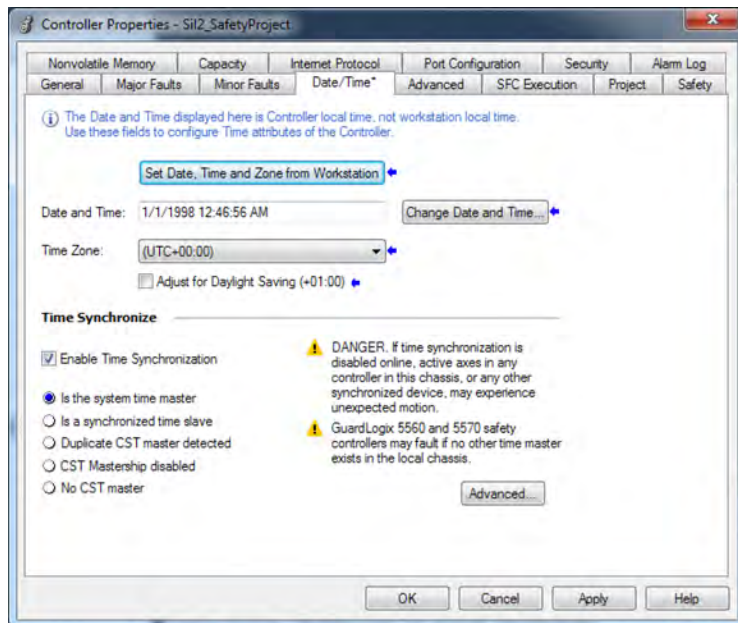
- Access to software that manages/updates the Precision Time Protocol on a control system network should be limited to users who are trained on the administration of industrial control system time including PTP.

This includes the PTP update tool 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 off line).

- When disabling PTP on a controller, to give the controller time to process the disable, use a two-second delay before setting the WallClockTime (WCT) in the controller. Otherwise, there is a risk of the grandmaster clock overwriting the WCT.

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



The Advanced Time Sync dialog box opens. See [Table 38 on page 258](#) for parameter descriptions.

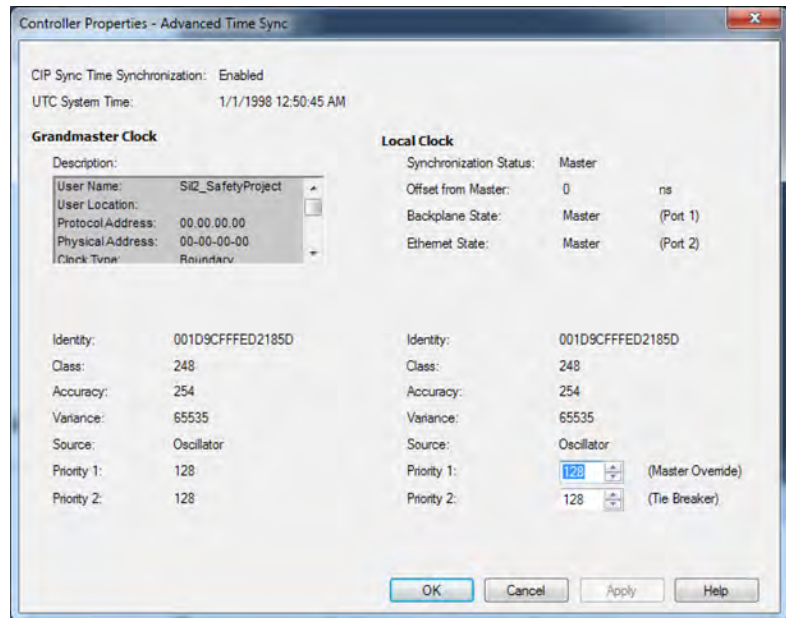


Table 38 - Time Sync Parameters

Grandmaster Clock	
Description	<p>Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified:</p> <ul style="list-style-type: none"> • User Name • User Location • Protocol Address • Physical Address • Clock Type • Manufacturer Name • Model • Serial Number • Hardware Revision • Firmware Revision • Software Revision • Profile Identity • Physical Protocol • Network Protocol • Port Number <p>Use the vertical scroll bar to view the data.</p>
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0...255 with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.

Table 38 - Time Sync Parameters (continued)

Source	Displays the time source of the Grandmaster clock. The available values are: <ul style="list-style-type: none"> • Atomic Clock • GPS • Radio • PTP • NTP • HAND set • Other • Oscillator
Priority 1 / Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The priority values range from 0 . . . 255. The highest priority is zero. The default value for both settings is 128.
Local Clock	
Synchronization Status	Displays whether the local clock is synchronized or not synchronized with the Grandmaster reference clock. A clock is synchronized if it has one port in the slave state and is receiving updates from the time master.
Offset to Master	Displays the amount of deviation between the local clock and the Grandmaster clock in nanoseconds.
Backplane State	Displays the current state of the backplane. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Ethernet State	Displays the state of the Ethernet port. The available values are: Initializing, Faulty, Disabled, Listening, PreMaster, Master, Passive, Uncalibration, Slave, or None.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of quality of the local clock. Values are defined from 0 . . . 255, with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the local clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the local clock. The available values are: <ul style="list-style-type: none"> • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP • HAND set • Other • Oscillator

Controller Diagnostics with Linx-based Software

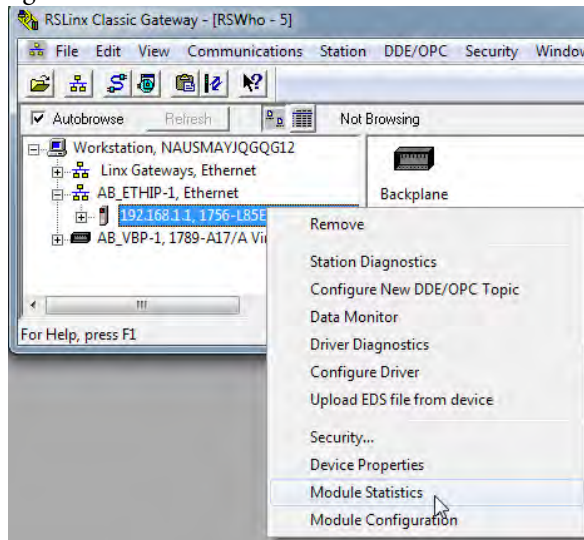
Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

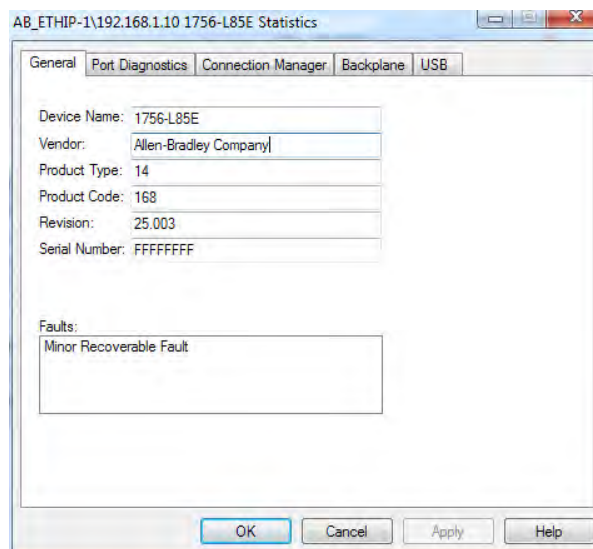
You can also view diagnostic information in Linx-based software.

1. From the Communications menu, choose RSWho.
- The RSWho dialog box appears.
2. Navigate to the Ethernet network.
 3. Right-click the controller and choose Module Statistics.



The Module Statistics dialog provides this information:

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



Controller Web Pages

Applies to these controllers:

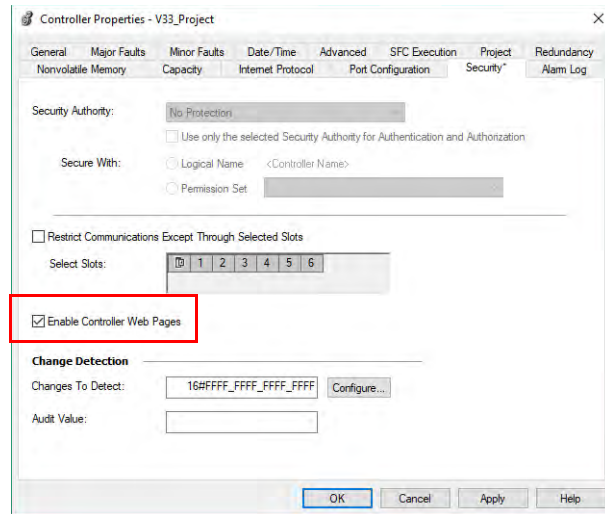
ControlLogix 5580

GuardLogix 5580

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

IMPORTANT With the Studio 5000 Logix Designer application version 33.00.00 and later, controller web pages are disabled by default.

- To enable the controller web pages, select the checkbox on the Logix Designer Controller Properties Security tab.



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

To access the diagnostic web pages, follow these steps.

1. Open your web browser.
2. In the Address field, type the IP address of the controller and press Enter.

To access the diagnostic web pages, open the Diagnostics folder in the left-most navigation bar, and click the link for each diagnostic web page you need to monitor.

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

Also see:

- [Home Web Page on page 262](#)
- [Faults Web Page on page 263](#)
- [Tasks Webpage on page 264](#)
- [Browse Chassis Webpage on page 265](#)

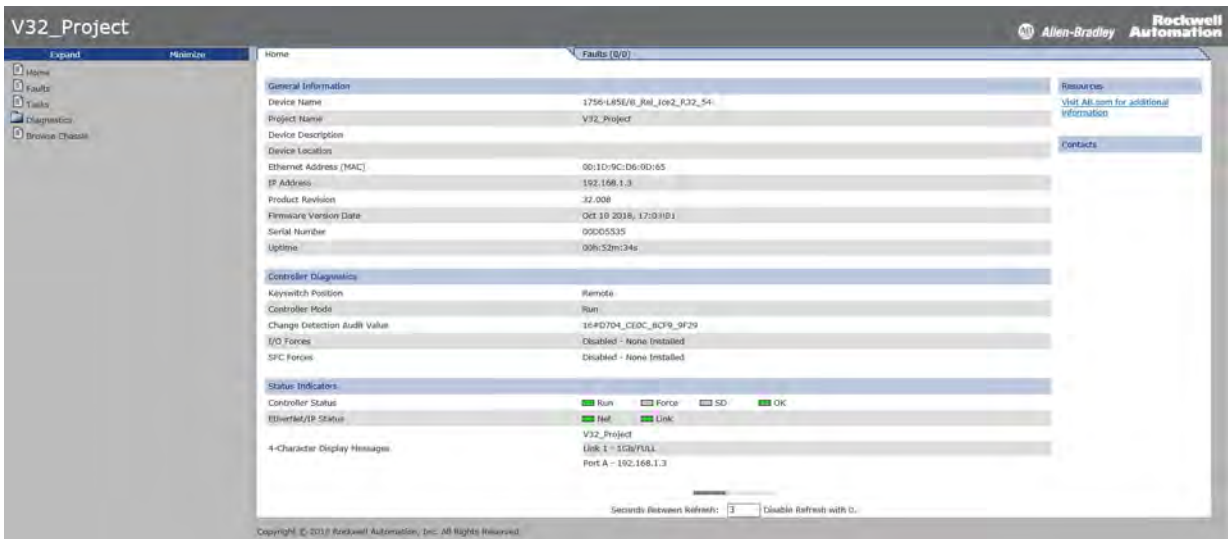
Home Web Page

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

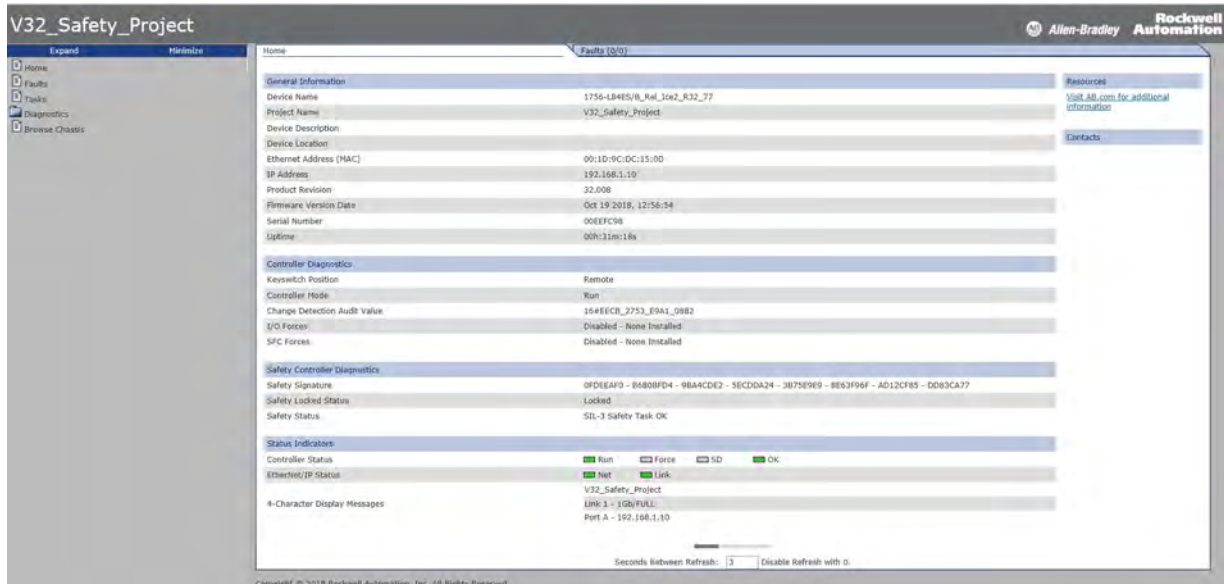
- Current 4-character display messages
- Controller status indicators state
- EtherNet/IP status indicators state
- Safety Signature, Safety Locked Status, Safety Status (for GuardLogix® 5580 and Compact GuardLogix 5380 controllers)

To set the refresh rate of the web pages, input the number of seconds into the Refresh field at the bottom of the web page.

ControlLogix 5580 Home Web Page



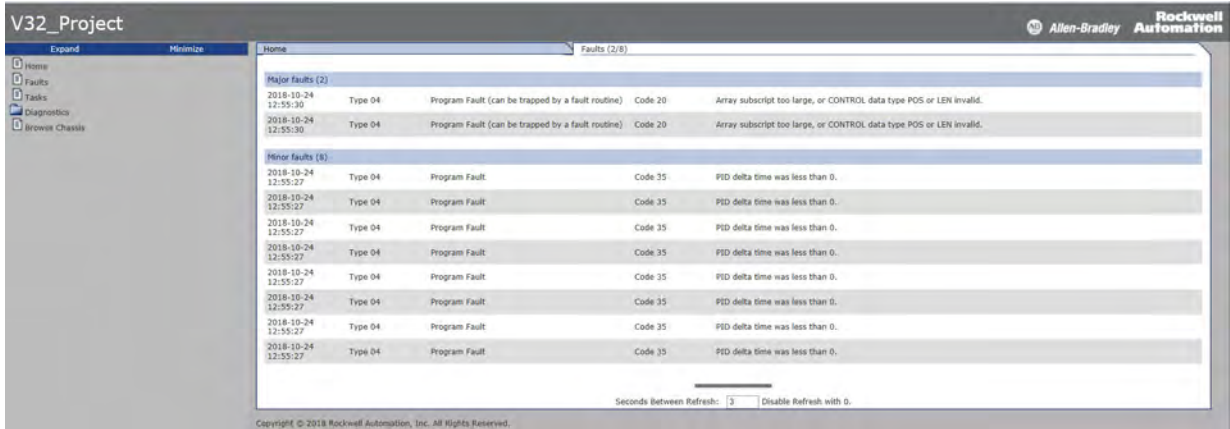
GuardLogix 5580 Home Web Page



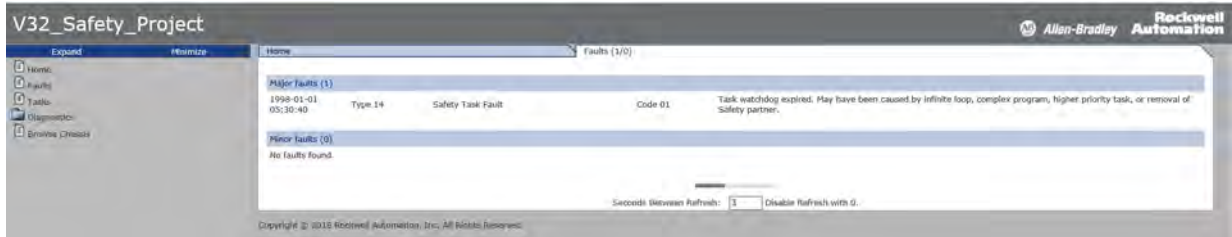
Faults Web Page

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

ControlLogix 5580 Faults Web Page



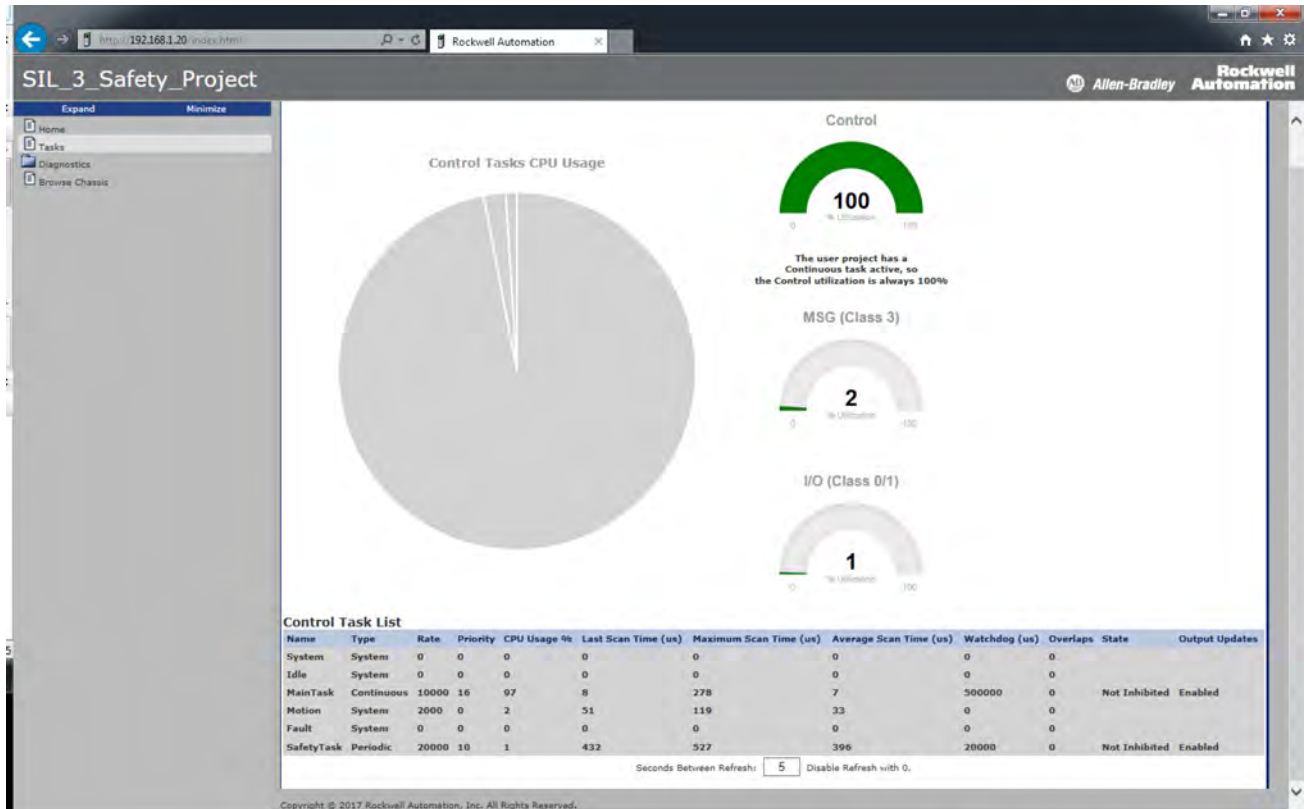
GuardLogix 5580 Faults Web Page



Tasks Webpage

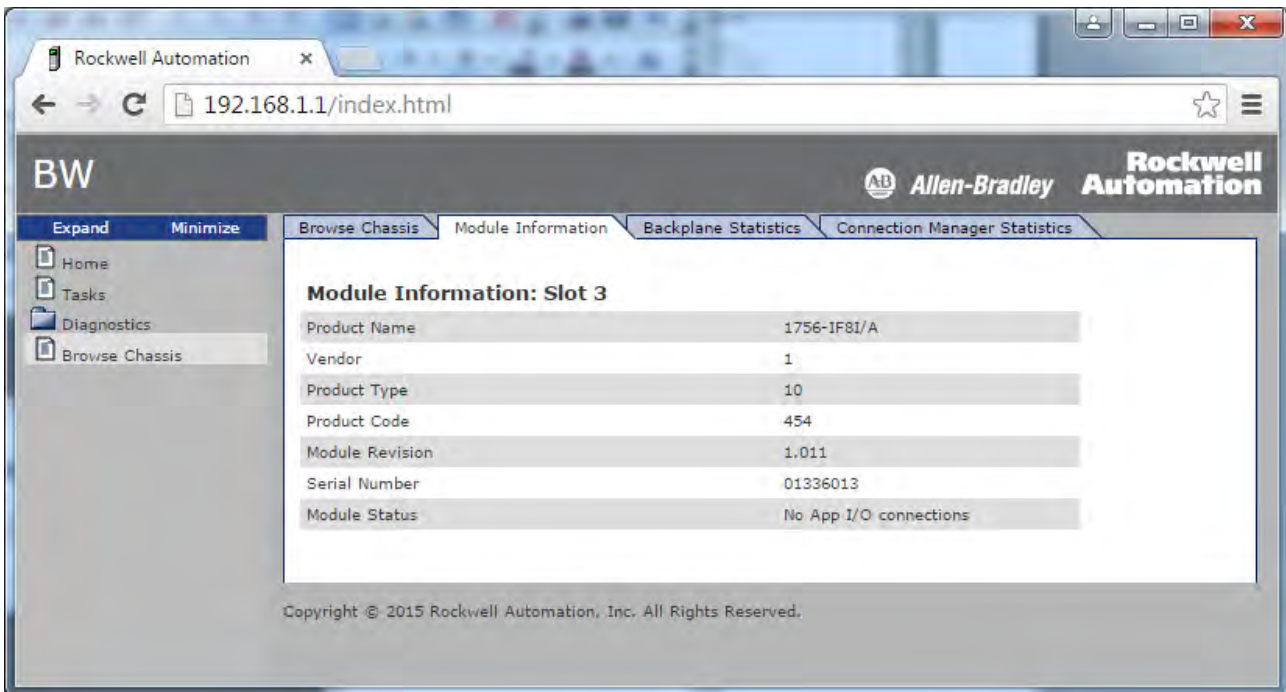
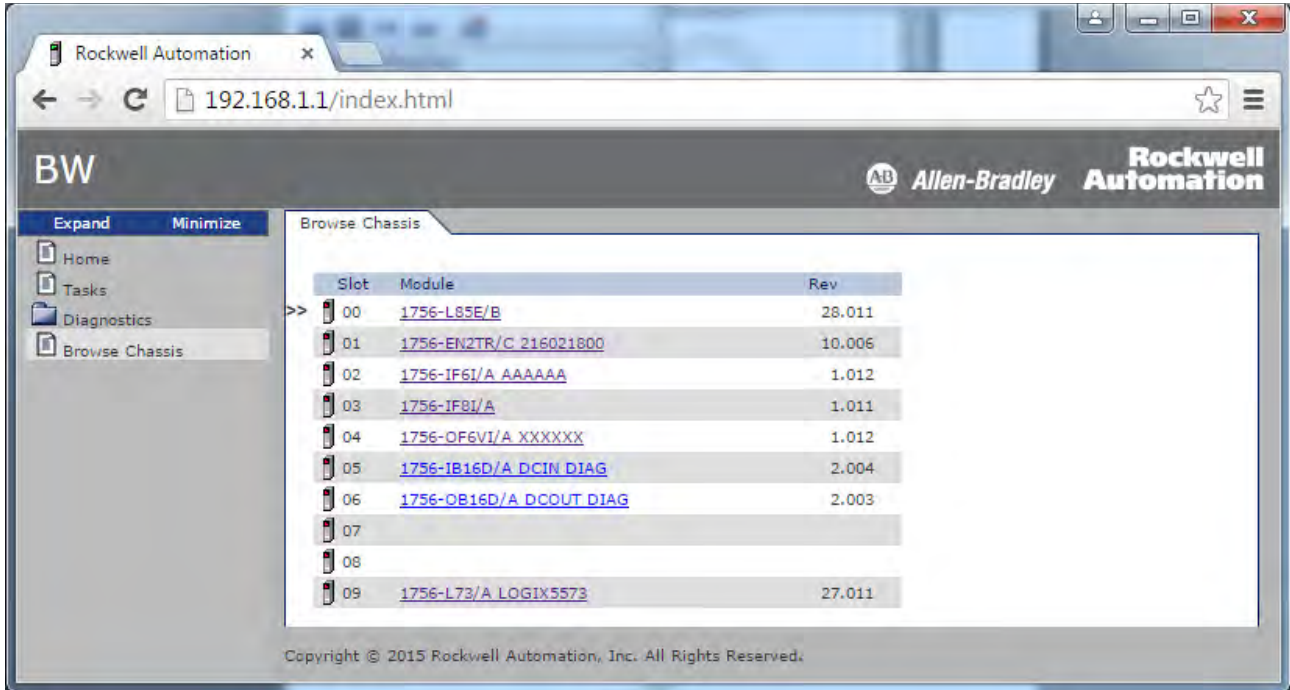
On the Tasks webpage, the pie chart shows the percentage of the control core's CPU consumed by the tasks that are on that core. The gauges show the CPU utilization of the control and communications cores. The table shows the tasks that are running on the control core (all system tasks are summarized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

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



Browse Chassis Webpage

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



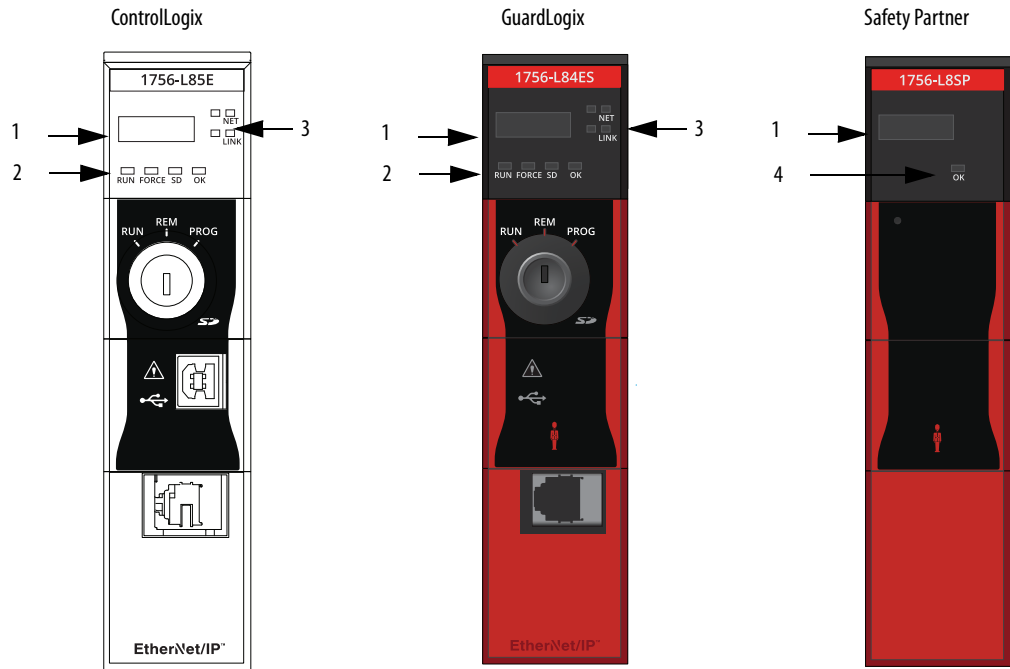
Notes:

Status Indicators

The controller has six status indicators and one four-character scrolling status display. The 1756-L8SP safety partner has the four-character scrolling status display and the OK status indicator.

Topic	Page
Status Display and Indicators	268
General Status Messages	269
GuardLogix Status Messages	271
Safety Partner Status Messages	271
Fault Messages	271
Major Fault Messages	272
I/O Fault Codes	273
Controller Status Indicators	274
Safety Partner OK Indicator	276
EtherNet/IP Indicators	276
Thermal Monitoring and Thermal Fault Behavior	277

Status Display and Indicators



Item	Description
1	4-Character Scrolling Status Display You can disable some of these messages, see Security Options on page 255 .
2	Controller Status Indicators, see page 274 .
3	EtherNet/IP™ Status Indicators, see page 276 .
4	Safety Partner OK Status Indicator, see page 276 .

General Status Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The scrolling messages that are described in [Table 39](#) are typically indicated upon powerup, powerdown, and while the controller is running to show the status of the controller.

Table 39 - Controller General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Check the OK indicator to determine if the controller is powered and determine the state of the controller.
Identity Mismatch - Contact Tech Support	This product's identity has been modified from its original production state and the integrity of the product has been compromised. This could be the result of unauthorized modifications made to the product or the product may not be a genuine Rockwell Automation product. This product should not be placed into service.
TEST	The controller is conducting power-up tests.
CHRG	The embedded energy storage circuit is charging.
PASS	Power-up tests have been successfully completed.
Saving... Do Not Remove SD Card	The controller is about to save an image to the SD card.
SAVE	A project is being saved to the SD card. You can also view the SD Indicator (see page 275) for more status information. Allow the save to complete before: <ul style="list-style-type: none"> • Removing the SD card. • Disconnecting the power. <p>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.</p>
LOAD	A project is being loaded from the SD card. You can also view the SD Indicator (see page 275) for more status information. Allow the load to complete before doing the following: <ul style="list-style-type: none"> • Removing the SD card • Disconnecting the power <p>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.</p>
UPDT	A firmware update is being conducted from the SD card upon powerup. You can also view the SD Indicator (see page 275) for more status information. If you do not want the firmware to update upon powerup, change the Load Image property of the controller.
Rev XX.xxx	The major and minor revision of the firmware of the controller.
1756-L8XX	The controller catalog number and series.
Link Down	Message appears when the EtherNet/IP port does not have a connection. Message scrolls continuously during operation.
Link Disabled	Message appears when you have disabled the EtherNet/IP port. Message scrolls continuously during operation.
DHCP- 00:00:XX:XX:XX:XX	Message appears when the controller is set for DHCP, but not configured on a network. The message shows the MAC address of the controller. Message scrolls continuously during operation if no IP address is set.
Ethernet Port Rate/Duplex State	The current port rate and duplex state when the EtherNet/IP port has a connection. Message scrolls continuously during operation.
IP Address	The IP address of the controller. Appears on powerup, then scrolls continuously during operation. If the IP address is not yet set, then the MAC address appears.
Duplicate IP - 00:00:XX:XX:XX:XX	Message appears when the controller detects a device on the network that has the same IP Address as the controller Ethernet port. The message shows the MAC address of the device with the duplicate IP Address. Message scrolls continuously during operation.

Table 39 - Controller General Status Messages (continued)

Message	Interpretation
No Project	No project is loaded on the controller. To load a project, do one of the following: <ul style="list-style-type: none"> • Use the Studio 5000 Logix Designer® application to download a project to the controller • Use an SD card to load a project to the controller
Project Name	The name of the project that is loaded on the controller.
BUSY	The I/O modules that are associated with the controller are not yet fully powered. Allow time for powerup and I/O module self-testing.
Corrupt Certificate Received	The security certificate that is associated with the firmware is corrupted. Go to http://www.rockwellautomation.com/support/ and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Corrupt Image Received	The firmware file is corrupted. Go to http://www.rockwellautomation.com/support/ and download the firmware revision you are trying to update to. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
Backup Energy HW Failure - Save Project	A failure with the embedded storage circuit has occurred, and the controller is incapable of saving the program in the event of a powerdown. If you see this message, then save your program to the SD card before you remove power, and then replace the controller.
Backup Energy Low - Save Project	The embedded storage circuit does not have sufficient energy to enable the controller to save the program in the event of a powerdown. If you see this message, then save your program to the SD card before you remove power, and then replace the controller.
Flash in Progress	A firmware update that is initiated via ControlFLASH Plus™, ControlFLASH™ or AutoFlash software is in progress. Allow the firmware update to complete without interruption.
Firmware Installation Required	The controller is using boot firmware (revision 1.xxx) and requires a firmware update.
SD Card Locked	An SD card that is locked is installed.
Download in Progress	An active download is occurring
Aborting Download	An active download is being canceled. This may be due to a user initiated cancel, a download failure, or connection loss. After completion, the No Project status message displays.

GuardLogix Status Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

In addition to the general status messages in [Table 39](#), a GuardLogix® 5580 controller display can show these scrolling messages.

Table 40 - Safety Controller Status Messages

Message	Interpretation
No Safety Signature	Safety Task is in Run mode without a safety signature. Generate a safety signature.
Safety Unlocked	The controller is in Run mode with a safety signature, but is not safety-locked. Safety lock the controller.
Safety Partner Missing	The safety partner is missing or unavailable. Make sure the safety partner is seated properly in the slot that is immediately to the right of the safety controller. The controller displays this message only in a SIL 3/PLe configuration.
Hardware Incompatible	The safety partner and primary controller hardware is incompatible. You must use the 1756-L8SP safety partner with GuardLogix 5580 Controllers. The controller displays this message only in a SIL 3/PLe configuration.
Firmware Incompatible	The safety partner and primary controller firmware revision levels are incompatible. Update the modules to the correct firmware revision. The controller displays this message only in a SIL 3/PLe configuration.
Safety Task Inoperable	The safety logic is invalid. For example, a mismatch occurred between the primary controller and the safety partner, a watchdog timeout occurred, or memory is corrupt.

Safety Partner Status Messages

Applies to these controllers:

GuardLogix 5580

The safety partner display can show these scrolling messages.

Table 41 - Safety Partner Status Messages

Message	Interpretation
L8SP	Standard display text. If there is a major non-recoverable fault, then the fault code scrolls across the display.
Flash in Progress	A firmware update that is initiated via ControlFLASH Plus, ControlFLASH or AutoFlash software is in progress. Allow the firmware update to complete without interruption.

Fault Messages

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

Table 42 - Fault Messages

Message	Interpretation
Major Fault TXX:CXX message	A major fault of Type XX and Code XX has been detected. For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, a JMP instruction is programmed to jump to an invalid LBL instruction. For details about major recoverable faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
I/O Fault Local:X #XXXX message	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .

Table 42 - Fault Messages (continued)

Message	Interpretation
I/O Fault <i>ModuleName</i> #XXXX message	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module is indicated with the fault code and brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named My_Module is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
I/O Fault <i>ModuleParent:X</i> #XXXX message	An I/O fault has occurred on a module in a remote chassis. The parent name of the module is indicated because no module name is configured in the I/O Configuration tree of Logix Designer application. In addition, the fault code is indicated with a brief description of the fault. For example, I/O Fault My_CNet:3 #0107 Connection Not Found indicates that a connection to a module in slot 3 of the chassis with the communication module named My_CNet is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .
X I/O Faults	I/O faults are present and X = the number of I/O faults present. If there are multiple I/O faults, the controller indicates the first fault reported. As each I/O fault is resolved, the number of indicated faults decreases and the I/O Fault message indicates the next reported fault. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014 .

Major Fault Messages

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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



This manual links to Knowledgebase Article [Logix 5000 Controller Fault Codes](#) for fault codes. Download the spreadsheet from this public article.

You might be asked to login to your Rockwell Automation web account, or create an account if you do not have one. You do not need a support contract to access the article.

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

I/O Fault Codes

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

The controller indicates I/O faults on the status display in one of these formats:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent:X #XXXX message*

The first part of the format is used to indicate the location of the module with a fault. How the location is indicated depends on your I/O configuration and the properties of the module that are specified in Logix Designer application.

The latter part of the format, *#XXXX message*, can be used to diagnose the type of I/O fault and potential corrective actions.



This manual links to Knowledgebase Article [Logix 5000 Controller Fault Codes](#) for fault codes. Download the spreadsheet from this public article.

You might be asked to login to your Rockwell Automation web account, or create an account if you do not have one. You do not need a support contract to access the article.

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

Controller Status Indicators

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

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

IMPORTANT Safety Consideration

Status indicators are not reliable indicators for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

RUN Indicator

The RUN indicator shows the current mode of the controller.

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

Table 43 - RUN Indicator

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

FORCE Indicator

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

Table 44 - FORCE Indicator

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

SD Indicator

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

Table 45 - SD Indicator

State	Description
Off	No activity is occurring with the SD card.
Flashing green	The controller is reading from or writing to the SD card.
Solid green	IMPORTANT: Do not remove the SD card while the controller is reading or writing. Allow the read/write to complete without interruption. If you interrupt the read/write, data corruption or loss can occur.
Flashing red	The SD card does not have a valid file system.
Solid red	The controller does not recognize the SD card.

OK Indicator

The OK indicator shows the state of the controller.

Table 46 - ControlLogix® and GuardLogix Controllers OK Indicator

State	Description
Off	No power is applied to the controller.
Flashing red	One of the following is true: <ul style="list-style-type: none"> It is a new controller, out of the box, and it requires a firmware update. If a firmware update is required, the status display indicates Firmware Installation Required. To update firmware, see Update Controller Firmware on page 55. It is a previously used or in-use controller and a major fault has occurred. All user tasks, standard and safety, are stopped. For details about major recoverable and nonrecoverable faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
Solid red	One of the following is true: <ul style="list-style-type: none"> The controller is completing power-up diagnostics. The charge of the capacitor in the ESM is being discharged upon powerdown. The controller is powered, but is inoperable. The controller is loading a project to nonvolatile memory. The controller is experiencing a Hardware Preservation Fault due to a high internal module temperature. In this condition, only the status indicator receives power. Once the controller cools down to an acceptable temperature, then full power is applied.
Solid green	The controller is operating normally.

Safety Partner OK Indicator

The safety partner has an OK status indicator.

Applies to these controllers:
GuardLogix 5580

Table 47 - 1756-L8SP Safety Partner OK Indicator

Sate	Description
Off	No power is applied.
Green	The safety partner is operating with no faults.
Red	One of the following is true: <ul style="list-style-type: none"> The safety partner is completing power-up diagnostics. The charge of the capacitor in the ESM is being discharged upon powerdown. The safety partner is powered, but is inoperable. The safety partner is loading a project to nonvolatile memory. The safety partner is experiencing a Hardware Preservation Fault due to a high internal module temperature. In this condition, only the status indicator receives power. Once the safety partner cools down to an acceptable temperature, then full power is applied.
Flashing Red	Controller is configured for SIL 2 operation but a safety partner is installed.

EtherNet/IP Indicators

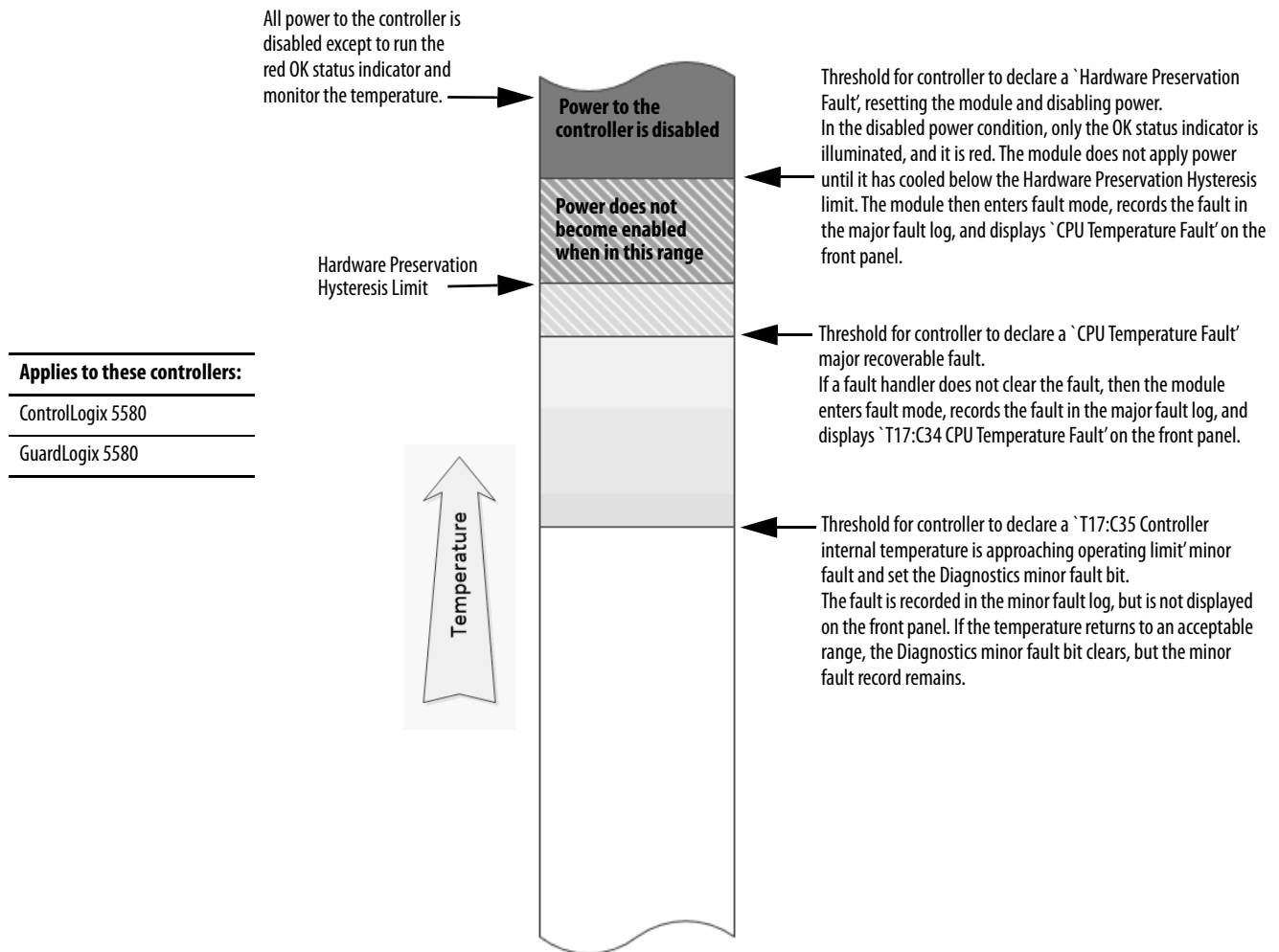
The EtherNet/IP indicators show the state of the EtherNet/IP port and communications activity.

Applies to these controllers:
ControlLogix 5580
GuardLogix 5580

Indicator	State	Description
NET	Off	<ul style="list-style-type: none"> The controller is not configured, or does not have an IP address. The port is administratively disabled.
	Flashing green	The controller has an IP address, but no active connections are established.
	Steady green	The controller has an IP address and at least one established active connection.
	Steady red	Duplicate IP Address or invalid configuration.
LINK	Off	No activity. One of these conditions exists: <ul style="list-style-type: none"> No link exists on the port. Verify that the RJ45 cables are properly seated in the adapter and connected devices. The port is administratively disabled.
	Flashing green	Activity exists on the port.

Thermal Monitoring and Thermal Fault Behavior

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



IMPORTANT If you follow the recommended limits for ambient (inlet) temperature and apply the required clearances around the chassis, the controller should not reach the initial warning (minor fault) temperature. See the 1756 ControlLogix Controllers Technical Data, publication [1756-TD001](#).

IMPORTANT The presence of any temperature warning indicates that measures need be taken to reduce the ambient temperature of the module. Instructions for using relay ladder logic to check for a minor fault can be found in the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#). A GSV instruction can be used to read the MinorFaultBits attribute of the FaultLog class name. If the Diagnostics minor fault bit (Bit 17) is set, then a temperature minor fault can be present. Check the Minor Faults tab of the Controller Properties dialog box in the Logix Designer application to see if the minor fault is a temperature warning.

Notes:

Change Controller Type

Topic	Page
Change from a Standard to a Safety Controller	279
Change from a Safety to a Standard Controller	280
Change Safety Controller Types	280

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

Changing controller type affects the following:

- Supported features
- Physical configuration of the project (safety partner and safety I/O)
- Controller properties
- Project components such as tasks, programs, routines, and tags
- Safety Add-On Instructions

Change from a Standard to a Safety Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

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

- The safety task is created only if the maximum number of downloadable tasks has not been reached. The safety task is initialized with its default values.
 - TIP** If your project already contains 32 tasks, and you request a change from a standard to a safety controller, the project does not convert and stays with the standard controller.
- Safety components are created (safety task, safety program, and so forth).
- The safety project defaults to safety level SIL 2/PLd.
- A time-based safety network number (SNN) is generated for the local chassis.
- A time-based safety network number (SNN) is also generated for the embedded EtherNet/IP™ port.
- Standard controller features that are not supported by the safety controller, such as redundancy, are removed from the Controller Properties dialog box (if they existed).

Change from a Safety to a Standard Controller

Applies to these controllers:

ControlLogix 5580

GuardLogix 5580

Upon confirmation of a change from a safety controller project to a standard controller, some components are changed and others are deleted, as described below:

- The safety partner is deleted from the I/O chassis if it existed.
- Safety I/O devices and their tags are deleted.
- The safety task, programs, and routines are changed to a standard task, programs, and routines.
- All safety tags, except safety consume tags, are changed to standard tags. Safety consume tags are deleted.
- Safety tag mappings are deleted.
- The safety network numbers (SNN) are deleted.
- Safety-lock and -unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, those new features are visible in the Controller Properties dialog box.

TIP Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

If the safety controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

Change Safety Controller Types

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

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

Numerics

10/100/1000 51

1756-CN2
uses 43

1756-CN2R
uses 43

1756-CN2RXT
uses 43

1756-CNB
uses 43

1756-CNBR
uses 43

1756-DHRIO 45
communication via 46
uses
remote I/O 47

1756-DHRIOXT
uses 45, 47

1756-DNB
uses 45

1756-EN2F
uses 40

1756-EN2T
uses 40

1756-EN2TR
uses 40

1756-EN2TRXT
uses 40

1756-EN2TSC
uses 40

1756-EN2TXT
uses 40

1756-EN3TR
uses 40

1756-ENBT
uses 40

1756-EWEB
uses 40

1756-IF8H
uses 50

1756-N2 115

1756-N2XT 115

1756-RIO
uses 47

1784-SD1
load from 98

1784-SD2
load from 98

1788-CN2DN
uses 45

1788-CN2FFR
uses 49

1788-EN2DNR
uses 45

1788-EN2FFR
uses 49

A

add
local I/O 115
remote I/O 121, 123

Add-On Instructions 27, 280
in project 163

allow communication 104

application
elements 153
networks and 35

audit value 220

AutoFlash
update 58

automatic diagnostics 249

axes
consumed 244
virtual 244

axis
obtain information 247

B

behavior
thermal fault 277

block communication 104

C

cache
message options 108
messages
about 107

changing controllers 280

chassis
ControlLogix
list 115

CIP Safety 33, 152

CIP Safety I/O
adding 131
node address 131

CIP Security ports
disable 225

clear
faults 201

communication
allow 104
block 104
Data Highway Plus 45, 46
Foundation Fieldbus 49
HART 50
network options 25, 26
path
set 71
universal remote I/O 47

configuration owner 142
resetting 143, 145

configuration signature
components 141
copy 141

- configure**
 - motion 244
 - configure always** 152
 - configure change detection** 219
 - audit value 220
 - changes to detect 219
 - configure trusted slot** 213
 - restrict communication 213
 - select slots 213
 - conformal coated controllers** 15
 - connection**
 - DeviceNet
 - network 45
 - EtherNet/IP 102
 - message, required 107
 - scheduled
 - ControlNet 106
 - status 198
 - unscheduled
 - ControlNet 106
 - connection reaction time limit** 184
 - CONNECTION_STATUS** 177, 198
 - ConnectionFaulted bit** 198
 - consume**
 - data 105
 - consume tag data** 183
 - consumed tag** 177
 - continuous task** 156
 - control data** 104
 - controler security** 208
 - ControlFLASH Plus software** 57, 74
 - ControlFLASH software** 57, 74
 - controller**
 - available modes 83
 - behavior 104
 - catalog numbers
 - conformal coated controllers 15
 - safety controllers 15
 - standard controllers 15
 - change type 279 - ??
 - communication path
 - set 71
 - ControlLogix 5580
 - communication options 25, 26
 - design system with 24
 - fault handler 204
 - firmware 55
 - obtain 57
 - go online 71
 - logging
 - safety lock, unlock 189
 - safety signature 192
 - match 73
 - monitor
 - connections 167
 - operation mode
 - change with keyswitch 84
 - change with Logix Designer 85
 - program 157
 - routine 160
 - serial number 73
 - serial number mismatch 76, 79
 - status indicators 274
 - tags 161
 - tasks 155
 - upload a project 80
 - controller audit log** 220
 - controller web pages** 261
 - disable 236
 - controller-specific security** 211
 - harden the control system 211
 - manage physical user access to the controller 212
 - monitor the control system 211
 - ControlLogix**
 - chassis
 - list 115
 - design system 24
 - I/O
 - remote 120
 - selection 113
 - remote I/O
 - local 115
 - slot filler 115
 - ControlLogix 5580 process controller** 17
 - ControlLogix No Stored Energy (NSE) Controllers** 16
 - ControlLogix Redundant Controllers** 17
 - ControlLogix system**
 - minimum requirements 15
 - ControlLogix-XT**
 - chassis
 - list 115
 - ControlLogix-XT Controllers** 16
 - ControlNet**
 - example 42
 - module 42
 - network 41
 - scheduled connection
 - scheduled connection 106
 - unscheduled connection
 - unscheduled connection 106
 - copy**
 - safety signature 193
 - create a fault routine** 214
- ## D
- Data Highway Plus** 45
 - data types**
 - CONNECTION_STATUS 177
 - data-only connection** 142
 - delete**
 - safety signature 193
 - design**
 - system 24
 - detect changes to the controller** 219

develop

- applications 153
- motion applications 243

DeviceNet

- connection use 45
- network 44

DH+ 45**diagnostic coverage** 33**diagnostics**

- with Logix Designer 251
 - port configuration category 255
 - time sync category 257
- with RSLinx software 260

disable the 4-character status display 232**disable the CIP Security ports** 225**disable the controller web pages** 236**disable the Ethernet port** 88, 221

- on port configuration tab 222
- with a MSG instruction 223

disable the SD card 230**disable the USB port** 228**DNS addressing** 53**double data rate (DDR)** 40**download**

- effect of controller match 73
- effect of firmware revision match 74
- effect of safety status 74

duplicate IP address

- detection 52
- resolution 53

E**editing** 193**electronic keying**

- about 114

elements

- control application 153

enable license-based protection 217**Ethernet** 51**Ethernet port**

- diagnostics
 - Logix Designer 255
- disable 88, 221

EtherNet/IP

- connections 102
- link speeds 37
- network 37
- nodes 102

EtherNet/IP network

- integrated motion 25, 26
- network communication rates 37
- number of nodes supported 26
- optimize network performance 37

event task 156**external access** 175**F****fault**

- clear 201
- cpu temperature 277
- hardware preservation 277
- nonrecoverable controller 201
- nonrecoverable safety 197, 201
- recoverable 202, 277
- routines 204

fault code

- use GSV to get 168

fault codes

- major safety faults 203
- status display 202

fault messages 271

- I/O 273

features 25

- controller
 - communication 25
 - programming 25

filler slot

- slot filler 115

firmware

- controller 55
- obtain 57
- required 56
- update with AutoFlash, use 58

firmware revision

- match 74
- mismatch 76, 79

firmware upgrade kit 74**FORCE indicator** 274**forcing** 193**Foundation Fieldbus** 49**G****general status messages** 269**GSV**

- fault code 168
- monitor
 - connection 167

H**handshake** 104**harden the control system** 209, 211**HART. See Highway Addressable Remote Transducer.****Highway Addressable Remote Transducer** 50**I****I/O**

- ControlLogix
 - remote 120
 - selection 113
- determine data update 129
- fault codes 273
- remote 120

I/O configuration

- add
 - local I/O 115
 - remote I/O 121, 123
 - while online 127

indicator 274

- FORCE 274
- OK 275
- SD 275

instruction

- motion 245

integrated motion

- on the EtherNet/IP network 25, 26

integrated STO mode 22, 23**IP addresses**

- duplicate address detection 52
- duplicate address resolution 53

J**jump to the fault routine** 215**K****keyswitch**

- change controller operation mode 84
- position 83

L**license-based source and execution****protection** 216

- enable license-based protection 217

link speeds

- EtherNet/IP 37

load

- from memory card 98

load a project

- on corrupt memory 95
- on power up 95
- user initiated 95

local

- I/O
 - add 115
 - remote I/O 115

lock

- See safety-lock.

Logix Designer

- change controller operation mode 85

Logix Designer application

- Add-On Instructions 163
- program 157
- routine 160
- tags 161
- tasks 155

M**major faults tab** 202, 203**major safety faults** 203**MajorFaultRecord** 205**manage physical user access to the controller** 212**manage programmatic user access** 209**match project to controller** 73**maximum observed network delay**

- reset 184

memory card 94

- load from 98
- other tasks 100

message

- about 107
- cache 108
 - determine if 108
- fault 271
- status display 269

messages

- safety status 271

minimum requirements 15**minor faults tab** 203**Monitor Safety I/O Device Status** 144**monitor the control system** 209, 211**motion**

- about 244
- application 243
- instructions 245
- program 245

MVI56-HART

- uses 50

N**network**

- application and 35
- controller options 25, 26
- ControlNet 41
- Data Highway Plus 46
- DeviceNet 44
- DH+. See Data Highway Plus.
- EtherNet/IP 37
- Foundation Fieldbus 49
- HART 50
- universal remote I/O 47

network address

- DNS addressing 53

network address translation (NAT)

- set the IP address 134

network communication rates

- on an EtherNet/IP network 37

network delay multiplier 185**network status**

- indicator 148, 150

no stored energy 16**node address** 131**nodes on an EtherNet/IP network** 102**nonrecoverable controller fault** 201**nonrecoverable safety fault** 197, 201

- re-starting the safety task 201

nonvolatile memory

- tab 92

NSE controllers 16

O

- obtain**
 - axis information 247
 - firmware 57
- OK indicator** 275
- online**
 - add
 - to I/O configuration 127
 - go 71
- online bar** 195
- optimize EtherNet/IP network performance**
 - 37
- out-of-box** 147
 - reset module 143

P

- password**
 - set 63, 191
- path**
 - set
 - communication 71
- peer safety controller**
 - location 178
 - sharing data 177
 - SNN 178
- Performance Level** 33
- periodic task** 156
- port diagnostics** 255
- primary controller**
 - description 21
- priority**
 - task 157
- probability of failure on demand (PFD)**
 - definition 33
- probability of failure per hour (PFH)**
 - definition 33
- process controllers** 17
- produce**
 - data 105
- produce a tag** 182
- produce/consume**
 - data 105
- produced tag** 177
- program**
 - in project 157
 - scheduled 159
 - unscheduled 159
- program fault routine** 204
- programming** 193
- programming languages** 162
- programming restrictions** 194

project

- Add-On Instructions 163
- elements 153
- go online 71
- program 157
- routine 160
- tags 161
- tasks 155
- upload 80
- protect signature in run mode** 64
- protecting the safety application** 189 - 193
 - safety signature 192
 - safety-lock 189
 - security 190

R

- reaction time** 173
- receive**
 - messages 107
- recoverable fault** 202
 - clear 202
- remote**
 - I/O 120
- remote I/O** 45
 - add 121, 123
 - ControlLogix
 - local 115
 - universal 47
- replace**
 - configure always enabled 152
 - configure only... enabled 147
 - Guard I/O module 146
- requested packet interval** 177
 - consumed tag 184
- required**
 - connections
 - messages 107
- reset**
 - module 143
 - ownership 143
- reset button** 86
 - safety partner reset 89
 - stage 1 reset 87
 - stage 2 reset 88
- reset module** 143, 145
- restrict communication**
 - configure trusted slot 213
- restrictions**
 - programming 194
 - safety tag mapping 186
 - software 194
 - when safety signature exists 193
- RIO. See universal remote I/O**
- routine**
 - in project 160
- RSLinx software**
 - controller diagnostics 260
- RSLogix 5000 software**
 - restrictions 194
- RSWho**
 - set

path 71
RunMode bit 198

S

safe torque-off

configurations
 integrated 22, 23

safety controller catalog numbers 15

safety network number

automatic assignment 66
 copy 69
 definition 33
 description 30, 65
 managing 65
 manual assignment 67
 paste 69
 set 136

safety partner

status 197

safety programs

safety routine

using standard data 186

safety signature

copy 193
 delete 193
 effect on download 75
 effect on upload 75
 generate 192
 restricted operations 193
 restrictions 194
 storing a project 93
 view 196

safety status

button 192, 196
 effect on download 74
 programming restrictions 194
 safety signature 192
 view 74, 195, 197

safety tab

190, 192, 197
 configuration signature 141
 generate safety signature 192
 module replacement 146
 safety-lock 190
 safety-lock controller 190
 unlock 190
 view safety status 74, 197

safety tags

controller-scoped 176
 description 175
 mapping 186 - 188

safety task

execution 174
 priority 173
 watchdog time 173

safety task period

safety-lock

189
 controller 190
 effect on download 75
 effect on upload 75
 icon 189
 password 190

SafetyTaskFaultRecord

safety-unlock

controller 190
 icon 189

scan times

reset 194

scheduled

program 159

SD card

disable 230

SD indicator

secure applications

207
 configure change detection 219
 audit value 220
 changes to detect 219
 configure trusted slot 213
 controller audit log 220
 controller security 208
 controller-specific security 211
 harden the control system 211
 manage physical user access to the controller 212
 monitor the control system 211
 disable the 4-character status display 232
 disable the CIP Security ports 225
 disable the controller web pages 236
 disable the Ethernet port 221
 on port configuration tab 222
 with a MSG instruction 223
 disable the SD card 230
 disable the USB port 228
 license-based source and execution protection 216
 enable license-based protection 217
 system-level security 209
 harden the control system 209
 manage programmatic user access 209
 monitor the control system 209
 user-definable major faults 214
 verification of security implementation 212

Secure Digital (SD) card

27, 94
 disable 230
 load from 98
 other tasks 100

selection

I/O 113

send

messages 107

serial number

simple network management protocol

snmp

software

restrictions 194

specifications

standard controller catalog numbers

standard data in a safety routine

status

fault messages 271
 indicators 274
 messages 271
 display 269
 monitor

- connections 167
- safety partner 197
- store a project** 93
- system** 25
- system-level security** 209
 - harden the control system 209
 - manage programmatic user access 209
 - monitor the control system 209

T

- tag**
 - consume 105
 - in project 161
 - produce 105
- tags**
 - controller-scoped 176
 - data type 176
 - external access 175
 - naming 144
 - produced/consumed safety data 177
 - safety I/O 177
 - scope 176
- task**
 - continuous 156
 - event 156
 - in project 155
 - periodic 156
 - priority 157
- temperature**
 - limit 277
 - warning 277
- terminology** 33
- timeout multiplier** 185

U

- universal remote I/O** 47
 - communicate via 48
- unlock controller** 190
- unscheduled**
 - program 159
- update**
 - determine frequency 129
- update firmware**
 - AutoFlash, use 58
- upload**
 - effect of controller match 73
 - effect of safety signature 75
 - effect of safety-lock 75
 - project 80
- USB port**
 - disable 228
- use a fault routine** 214
- user-definable major faults** 214
 - create a fault routine 214
 - jump to the fault routine 215
 - use a fault routine 214

V

- verification of security implementation** 212
- view**
 - safety status 74

W

- watchdog time** 173
- web pages** 261
- webpages**
 - disable 236

Notes:

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
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)



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





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

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

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

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

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

Connect with us.    

rockwellautomation.com ————— expanding **human possibility**[™]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

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

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846