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

CompactLogix 5380 and Compact GuardLogix 5380 Controllers

Bulletin 5069

Allen-Bradley
by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Preface

Chapter 1

CompactLogix 5380 and Compact GuardLogix 5380 Systems and Controllers

Chapter 2

How to Power CompactLogix 5380 Controllers

Chapter 3

How to Power Compact GuardLogix 5380 Controllers

Chapter 4

Safety Concept of Compact GuardLogix 5380 Controllers

Chapter 5

Connect to the Controller

Chapter 6

Start to Use the Controller

Chapter 7

Use the Secure Digital Card

Chapter 8

EtherNet/IP Network

Chapter 9

Use EtherNet/IP Modes

Chapter 10

Manage Controller Communication

Chapter 11

Standard I/O Modules

Chapter 12

Safety I/O Devices

Chapter 13

Develop Standard Applications

Chapter 14

Develop Safety Applications

Chapter 15

Develop Secure Applications

Chapter 16

Develop Motion Applications

Chapter 17

Troubleshoot the Controller

Appendix A

Status Indicators

Appendix B

Change Controller Type

Appendix C

History of Changes

Notes:

About This Publication

This manual provides information on how to design a system, operate a CompactLogix™ or Compact GuardLogix-based controllers system, and develop applications.

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

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

Download Firmware, AOP, EDS, and Other Files

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

Summary of Changes

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

Topic	Page
CompactLogix 5380 controllers support IEC-62443-4-2 SL 1 security requirements	throughout
Added the Secure Controller Systems section to Chapter 1	23
Revised the Safety Signature section in Chapter 4	45
Added 1784-SDHC8 and 1784-SDHC32 memory cards	91
Added Chapter 15, Develop Secure Applications	195
Updated Device Level Ring Network Topology section	106

Additional Resources

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

Resource		Description
Hardware installation	CompactLogix 5380 Controllers Installation Instructions, publication 5069-IN013	Provides installation instructions for CompactLogix™ 5380 controllers.
	Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014	Provides installation instructions for Compact GuardLogix® 5380 SIL 2 controllers.
	Compact GuardLogix 5380 SIL 3 Controllers Installation Instructions, publication 5069-IN023	Provides installation instructions for Compact GuardLogix 5380 SIL 3 controllers.
	Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Technical Data	Compact 5000 I/O Modules Specifications Technical Data, publication 5069-TD001	Provides specifications for Compact 5000™ I/O EtherNet/IP™ adapters and Compact 5000 I/O modules.
	CompactLogix 5380 and Compact GuardLogix 5380 Controllers Specifications Technical Data, publication 5069-TD002	Provides specifications for CompactLogix 5380 and Compact GuardLogix 5380 controllers.
Networks	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.
Safety Application Requirements	GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012	Provides requirements for achieving and maintaining Safety Integrity Level (SIL) 2 and Performance Level (PL) d and Safety Integrity Level (SIL) 3 and Performance Level (PL) e requirements with the GuardLogix 5580 and Compact GuardLogix 5380 controller system using the Studio 5000 Logix Designer® application.
Motion	Integrated Motion on the EtherNet/IP Network Reference Manual, publication MOTION-RM003	Provides descriptions of the AXIS_CIP_DRIVE attributes and the Logix Designer application Control Modes and Methods.
	Logix 5000 Controllers Motion Instructions Reference Manual, publication MOTION-RM002	Provides information on how to use Motion instructions.

Resource		Description
Design Considerations	Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides information on how to design and plan Logix 5000 controller systems.
	Ethernet Design Considerations Reference Manual, publication ENET-RM002	Provides additional information on network design for your system.
	Replacement Guidelines: Logix 5000 Controllers Reference Manual, publication 1756-RM100	Provides guidelines on how to replace the following: • ControlLogix® 5560/5570 controller with a ControlLogix 5580 controller • CompactLogix 5370 L3 controllers with a CompactLogix 5380 controller
Programming Tasks and Procedures	Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Provides access to the Logix 5000 Controllers set of programming manuals. The manuals cover such topics as how to manage project files, organize tags, program logic, test routines, handle faults, and more.
	Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Provides information on the programming instructions available to use in Logix Designer application projects.
	GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety application instruction set.
Product Certifications	Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

Chapter 1

CompactLogix 5380 and Compact GuardLogix 5380 Systems and Controllers

This chapter describes features of the following CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers.

Controller Type	Cat. No.
CompactLogix 5380 Standard controllers	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ERM, 5069-L310ERMK, 5069-L310ER-NSE, 5069-L320ER, 5069-L320ERM, 5069-L320ERMK, 5069-L330ER, 5069-L330ERM, 5069-L330ERMK, 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L350ERMK, 5069-L380ERM, 5069-L3100ERM
CompactLogix 5380 Process controllers	5069-L320ERP, 5069-L340ERP
Compact GuardLogix® 5380 SIL 2 controllers	5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2
Compact GuardLogix 5380 SIL 3 controllers	5069-L306ERMS3, 5069-L310ERMS3, 5069-L310ERMS3K, 5069-L320ERMS3, 5069-L320ERMS3K, 5069-L330ERMS3, 5069-L330ERMS3K, 5069-L340ERMS3, 5069-L350ERMS3, 5069-L350ERMS3K, 5069-L380ERMS3, 5069-L3100ERMS3

Minimum Requirements

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controllers have these minimum requirements:

- CompactLogix 5380 and Compact GuardLogix 5380 controllers have minimum hardware requirements. For more information on the hardware requirements, see Table 1 on page 18.
- The controller firmware revision must be compatible with the software version that you use. For more information, see Controller Firmware and Logix Designer Application Compatibility on page 55.
- Programming software

System	Cat. No.	Studio 5000 Logix Designer® Application[1]
CompactLogix	5069-L320ER, 5069-L340ERM	Version 28 or later
CompactLogix	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK, 5069-L320ERM, 5069-L320ERMK, 5069-L330ER, 5069-L330ERM, 5069-L330ERMK, 5069-L340ER	Version 29 or later
CompactLogix	5069-L350ERM, 5069-L350ERMK, 5069-L380ERM, 5069-L3100ERM	Version 30or later
Compact GuardLogix SIL 2 controllers[2]	5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L3100ERS2, 5069-L3100ERMS2	Version 31 or later
Compact GuardLogix SIL 3 controllers[2]	5069-L306ERMS3, 5069-L310ERMS3, 5069-L310ERMS3K, 5069-L320ERMS3, 5069-L320ERMS3K, 5069-L330ERMS3, 5069-L330ERMS3K, 5069-L340ERMS3, 5069-L350ERMS3, 5069-L350ERMS3K, 5069-L380ERMS3, 5069-L3100ERMS3	Version 32 or later
CompactLogix Process controllers	5069-L310ERxK, 5069-L320ERP, 5069-L340ERP	Version 33 or later

[1] For compatible Linx-based communication software and ControlFLASH™ software, see the Product Compatibility and Download Center (PCDC).

[2] For more information on safety ratings, see Safety Concept of Compact GuardLogix 5380 Controllers on page 43.

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

IMPORTANT This equipment is supplied as open-type equipment for indoor use. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that are present and appropriately designed to help prevent personal injury resulting from accessibility to live parts.

The enclosure must have suitable flame-retardant properties to help prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool.

For more information about enclosure type ratings that are required to comply with certain product safety certifications, see the following:

- Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014.
- Compact GuardLogix 5380 SIL 3 Controllers Installation Instructions, publication 5069-IN023.

Waste Electrical and Electronic Equipment (WEEE)

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

CompactLogix 5380 System

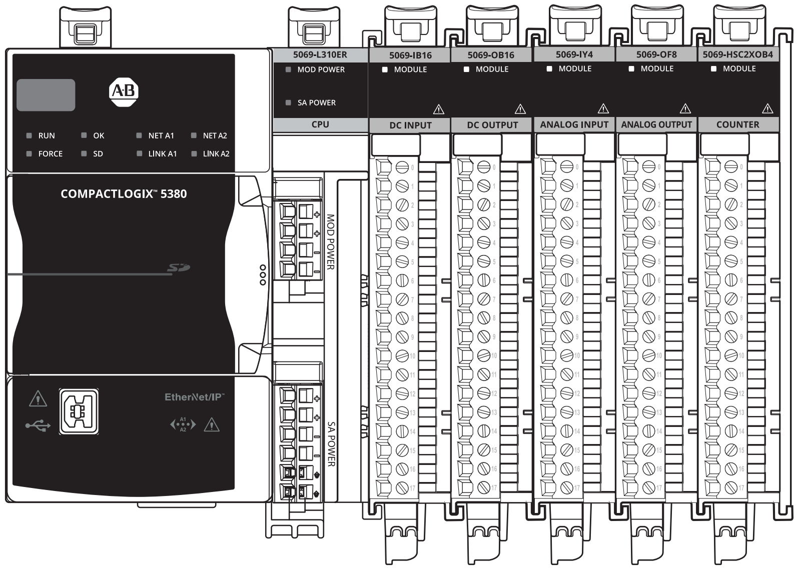
CompactLogix 5380 control systems are DIN rail-mounted systems that can operate in various applications.

One of the simplest controller configurations is a standalone controller with I/O assembled in one chassis, as shown in Figure 1.

Figure 1 - CompactLogix 5380 Controller in a Standalone System

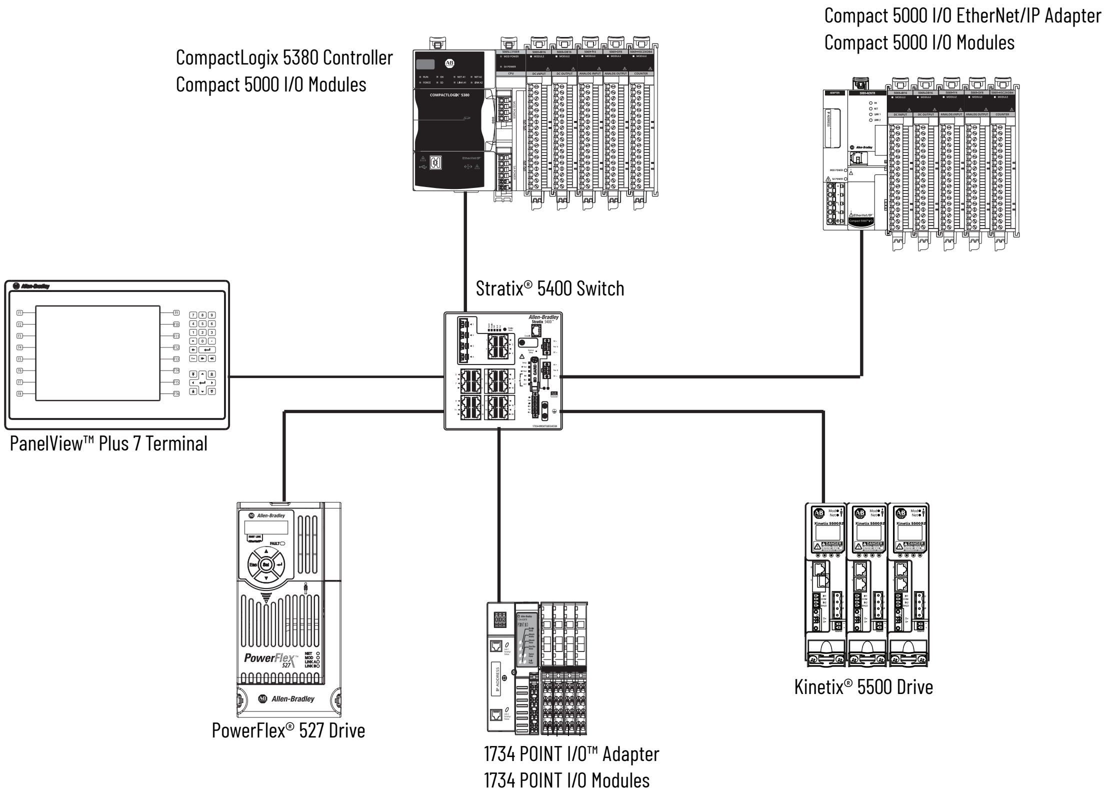
CompactLogix 5380 Controller

Compact 5000™ I/O Analog and Digital Modules



The controllers can also operate in more complex systems with devices that are connected to the controller via an EtherNet/IP™ network, as shown in Figure 2.

Figure 2 - CompactLogix 5380 Controller in a More Complex System



5069-L310ER-NSE No Stored Energy (NSE) Controller

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 400μJ or less in 40 seconds.

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

- 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.
- Wait at least **40 seconds** for the residual stored energy to decrease to 400 μJ or less before you remove the controller. There is no visual indication of when the 40 seconds has expired. **You must track that time period**.

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

CompactLogix 5380 Process Controllers

CompactLogix 5380 Process controllers (5069-L320ERP, 5069-L340ERP) are extensions of the Logix 5000 controller family that focus on plant-wide process control, and support motion.

The process controllers come configured with a default process tasking model and dedicated PlantPAx® process instructions that are optimized for process applications, and that improve design and deployment efforts.

The process controllers are conformal coated to add a layer of protection when exposed to harsh, corrosive environments.

Compact GuardLogix 5380 System

Compact GuardLogix 5380 SIL 2 and SIL 3 controllers are programmable automation controllers with integrated safety.

For SIL 3/PLe safety applications, the Compact GuardLogix 5380 SIL 3 controller system consists of a primary controller with an internal safety partner, that functions together in a 1oo2 architecture.

Compact GuardLogix 5380 SIL 2 Controller

Compact GuardLogix 5380 SIL 3 Controller

For more information on safety ratings, see Safety Concept of Compact GuardLogix 5380 Controllers on page 51.

The Compact 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).

With a Compact GuardLogix controller, you can interface to standard I/O via standard tasks while you interface with safety I/O via the safety task.

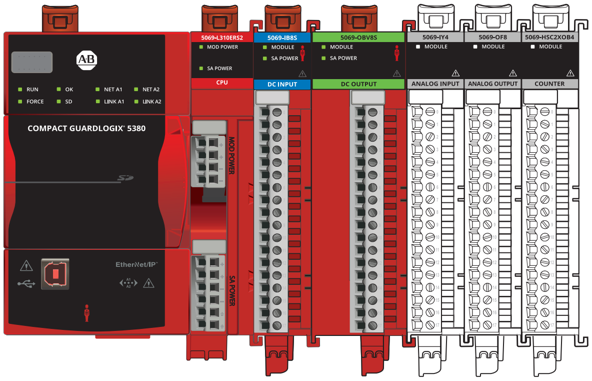
IMPORTANT For the safety task, Compact GuardLogix 5380 controllers support Ladder Diagram only.

For standard tasks, Compact GuardLogix 5380 controllers support:

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

The controllers can operate in various applications that range from standalone systems that contain local I/O modules, as shown in Figure 3.

Figure 3 - Compact GuardLogix 5380 Controller in a Standalone System

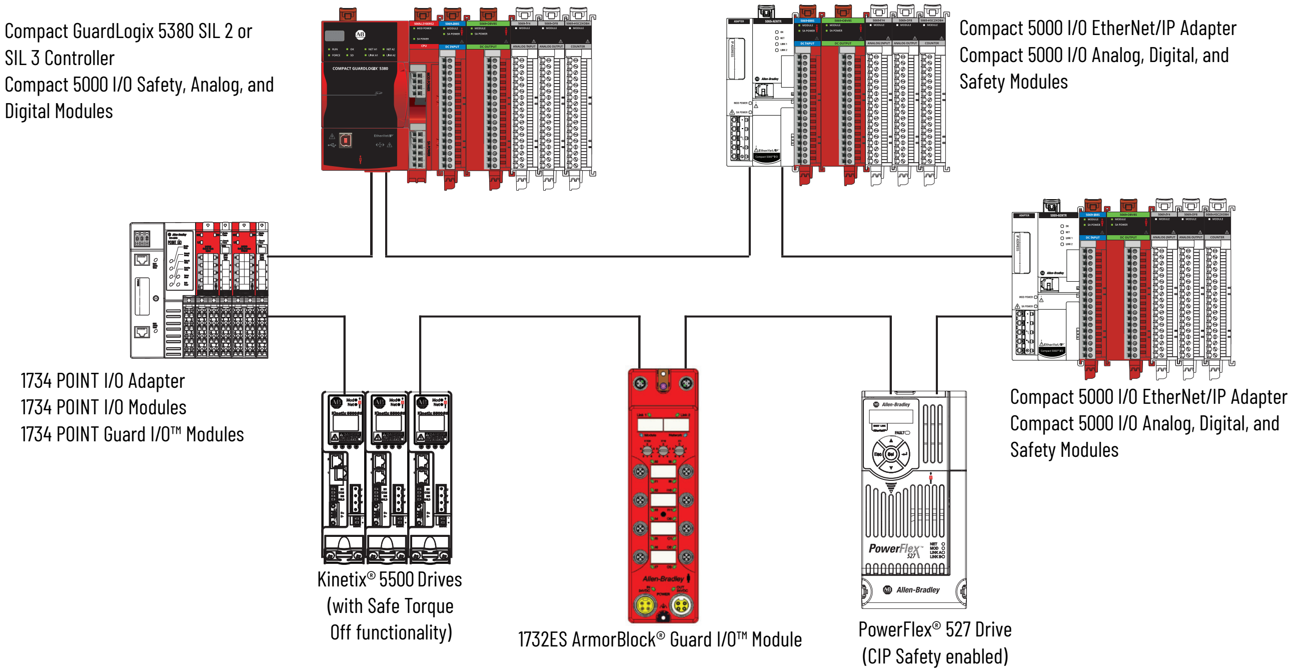


Compact GuardLogix 5380 Controller

Compact 5000 I/O Safety Digital, Standard Analog, and Standard Digital Modules

The controllers can also operate in more complex systems with devices that are connected to the controller via an EtherNet/IP network, as shown in Figure 4.

Figure 4 - Compact GuardLogix 5380 Controller on an EtherNet/IP DLR Network



Compact GuardLogix 5380 SIL 2 or SIL 3 Controller
Compact 5000 I/O Safety, Analog, and Digital Modules

Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Analog, Digital, and Safety Modules

1734 POINT I/O Adapter
1734 POINT I/O Modules
1734 POINT Guard I/O™ Modules

Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Analog, Digital, and Safety Modules

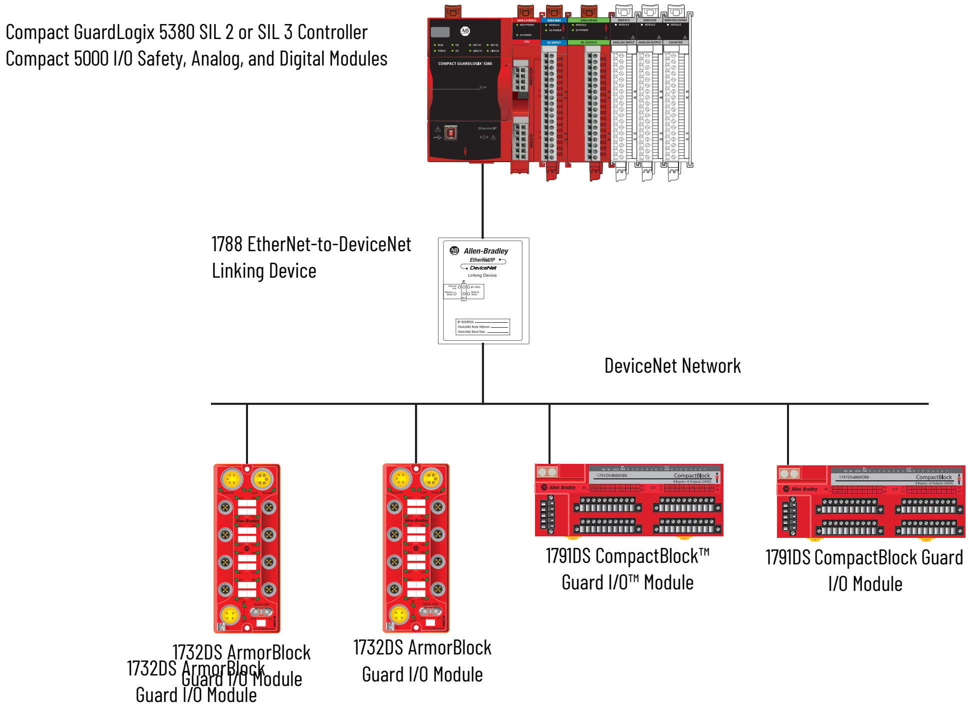
Kinetix® 5500 Drives (with Safe Torque Off functionality)

1732ES ArmorBlock® Guard I/O™ Module

PowerFlex® 527 Drive (CIP Safety enabled)

Compact GuardLogix 5380 controllers can communicate with safety devices on a DeviceNet® network via a 1788-EN2DN linking device, as shown in Figure 5

Figure 5 - Compact GuardLogix 5380 Controller Connected to Devices on a DeviceNet Network


Compact GuardLogix 5380 SIL 2 or SIL 3 Controller
Compact 5000 I/O Safety, Analog, and Digital Modules
1788 EtherNet-to-DeviceNet Linking Device
DeviceNet Network
1732DS ArmorBlock Guard I/O Module
1732DS ArmorBlock Guard I/O Module
1732DS ArmorBlock Guard I/O Module
1791DS CompactBlock™ Guard I/O™ Module
1791DS CompactBlock Guard I/O Module

Design the System

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

When you design a system, you must decide what system components your application needs. Table 1 describes components that are commonly used in CompactLogix 5380 and Compact GuardLogix 5380 control systems.

Table 1 - System Components

Component	Purpose	Required	For More Information
DIN rail	Mounting system	Yes	CompactLogix 5380 Controllers Installation Instructions, publication 5069-IN013 Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014 Compact GuardLogix 5380 SIL 3 Controllers Installation Instructions, publication 5069-IN023
End cap (5069-ECR) **IMPORTANT**: The end cap ships with the controller.	The end cap covers the exposed interconnections on the last module in the system. If you do not install the end cap before powering the system, equipment damage or injury from electric shock can result. **IMPORTANT**: You install the end cap after the last module is installed on the DIN rail. This design helps to prevent the end cap from going beyond the locked position. If you push the end cap beyond the locked position or insert it from the backwards direction, you can damage the MOD power bus and SA power bus connector.	Yes	
Removable terminal blocks (RTBs)	Connect these power types to the controller: MOD power SA power	Yes	

Table 1 - System Components (Continued)

Component	Purpose	Required	For More Information
External power supply[1]	Provides Module (MOD) Power to the system	Yes	Power the System on page 23
External power supply[1]	Provides Sensor/Actuator (SA) Power to the system	Yes - Only if the system requires SA power. If the system does not require SA power, the external power supply is not needed.	
Studio 5000 Logix Designer application	Configure the project that is used to define controller activity during system operation	Yes	Minimum Requirements on page 13 Create a Logix Designer Application Project on page 65
Linx-based communication software	Used as follows: Assign the controller an IP address Maintain communication over the EtherNet/IP network	Yes	For compatible Linx-based communication software and, see the Product Compatibility and Download Center (PCDC). Connect to the Controller on page 49
ControlFLASH software	Update controller firmware	Yes	For compatible ControlFLASH software, see the Product Compatibility and Download Center (PCDC). Update Controller Firmware on page 54
USB programming port	Complete tasks that only require a temporary connection to the controller, for example, when you download a project or update firmware	—	Connect a USB Cable on page 50
Ethernet port A1	Connects to these network types: Enterprise-level network Device-level network	—	Use EtherNet/IP Modes , on page 117
Ethernet port A2	Connect to device-level networks	—	
Secure Digital (SD) card **IMPORTANT**: The 1784-SD2 card ships with the controller.	Store data, such as the controller project and diagnostics that are required by technical support to obtain information if non-recoverable controller faults occur.	We recommend that you leave the SD card installed, so if a fault occurs, diagnostic data is automatically written to the card.	Use the Secure Digital Card on page 91
Ethernet cables	Used as follows: Access the controller from the workstation over an EtherNet/IP network to set IP address, update firmware, download, and upload projects Connect controller to an EtherNet/IP network and perform tasks that are required for normal operations	Yes	Connect an Ethernet Cable on page 50
USB Cable	Access the controller directly from the workstation to set IP address, update firmware, download, and upload projects. The USB port is intended for temporary local programming purposes only and not intended for permanent connection.	Yes - Only if you perform tasks that are listed in the previous column via the USB port. You can also perform the tasks via the controller Ethernet ports.	Connect a USB Cable on page 50
Integrated Safety I/O devices on an EtherNet/IP network	Connected to safety input and output devices, for example, Compact 5000 I/O safety modules or Guardmaster® Multifunctional Access Box. **IMPORTANT**: CompactLogix 5380 controllers cannot use safety devices.	Yes for Compact GuardLogix 5380 controllers.	Safety I/O Devices on page 161
Compact 5000 I/O modules	Used as follows: Local standard I/O modules that are installed in the CompactLogix 5380 system Remote standard I/O modules that are accessible via the EtherNet/IP network Local safety I/O modules that are installed in the CompactLogix 5380 system Remote safety I/O modules that are accessible via the EtherNet/IP network	Yes	Standard I/O Modules on page 141 Safety I/O Devices on page 161
Devices that are installed on an EtherNet/IP network	Dependent upon device type. Examples include: Remote standard I/O modules Remote safety I/O modules Ethernet switches Motion control devices, such as drives HMI devices	Yes	Standard I/O Modules on page 141 Safety I/O Devices on page 161 Develop Motion Applications on page 229

[1] We strongly recommend that you use separate external power supplies for MOD power and SA power, respectively.

Controller Features

CompactLogix 5380 and Compact GuardLogix 5380 Controller Features lists features available on the controllers. The features are described in detail in the rest of this manual.

Table 2 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Features

Feature	CompactLogix 5380 Controllers		Compact GuardLogix 5380 Controllers	
User memory	5069-L306ER, 5069-L306ERM	0.6 MB	5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3	0.6 MB
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK	1 MB	5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	1 MB
	5069-L320ER, 5069-L320ERM, 5069-L320ERP	2 MB	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	2 MB
	5069-L330ER, 5069-L330ERM	3 MB	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	3 MB
	5069-L340ER, 5069-L340ERM, 5069-L340ERP	4 MB	5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3	4 MB
	5069-L350ERM	5 MB	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K	5 MB
	5069-L380ERM	8 MB	5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3	8 MB
	5069-L3100ERM	10 MB	5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	10 MB
Safety memory	—		5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3	0.3 MB
	—		5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK	0.5 MB
	—		5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	1 MB
	—		5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	1.5 MB
	—		5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3	2 MB
	—		5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K	2.5 MB
	—		5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3	4 MB
	—		5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	5 MB
Controller tasks	32 tasks 1000 programs/task Event tasks; all event triggers		32 tasks 31 standard tasks 1 safety task 1000 programs/task Event tasks; all event triggers	
Communication ports	1 - USB port, 2.0 full-speed, Type B 2 - Embedded Ethernet ports, 10 Mbps, 100 Mbps, 1 Gbps			
CIP Security™	See CIP Security on page 23.			
EtherNet/IP network topologies supported	Device Level Ring (DLR) Star Linear			

Table 2 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Features (Continued)

Feature	CompactLogix 5380 Controllers		Compact GuardLogix 5380 Controllers	
EtherNet/IP modes	Linear/DLR mode Dual-IP mode - Available with the Logix Designer application, version 29 or later.			
EtherNet/IP nodes supported, max[1]	5069-L306ER, 5069-L306ERM	16 nodes	5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3	16 nodes
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK	24 nodes	5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	24 nodes
	5069-L320ER, 5069-L320ERM, 5069-L320ERP	40 nodes	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K 5069-L320ERMS3, 5069-L320ERMS3K	40 nodes
	5069-L330ER, 5069-L330ERM	60 nodes	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	60 nodes
	5069-L340ER, 5069-L340ERM, 5069-L340ERP	90 nodes	5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3	90 nodes
	5069-L350ERM	120 nodes	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K	120 nodes
	5069-L380ERM	150 nodes	5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3	150 nodes
	5069-L3100ERM	180 nodes	5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	180 nodes
Integrated motion axes supported Only controllers with an 'M' or 'P' in the catalog number support motion.	5069-L306ERM	2 axes	5069-L306ERMS2, 5069-L306ERMS3	2 axes
	5069-L310ERM, 5069-L310ERMK	4 axes	5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	4 axes
	5069-L320ERM, 5069-L320ERP	8 axes	5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	8 axes
	5069-L330ERM	16 axes	5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	16 axes
	5069-L340ERM, 5069-L340ERP	20 axes	5069-L340ERMS2, 5069-L340ERMS3	20 axes
	5069-L350ERM	24 axes	5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K	24 axes
	5069-L380ERM	28 axes	5069-L380ERMS2, 5069-L380ERMS3	28 axes
	5069-L3100ERM	32 axes	5069-L3100ERMS2, 5069-L3100ERMS3	32 axes
Local I/O modules, max	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK	8 modules	5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3, 5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	8 modules
	5069-L320ER, 5069-L320ERM, 5069-L320ERP	16 modules	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	16 modules
	5069-L330ER[2], 5069-L330ERM[2], 5069-L340ER, 5069-L340ERM, 5069-L340ERP, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	31 modules	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3, 5069-L350ERS2, 5069-L350ERS2K,5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3, 5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	31 modules
Programming languages	• Ladder Diagram (LD) • Structured Text (ST) • Function Block Diagram (FBD) • Sequential Function Chart (SFC)		• For the safety task, Compact GuardLogix controllers support Ladder Diagram only. • For standard tasks, Compact GuardLogix controllers support: – Ladder Diagram (LD) – Structured Text (ST) – Function Block Diagram (FBD) – Sequential Function Chart (SFC)	
Supported controller Features	• Data access control • Firmware Supervisor • Secure Digital (SD) card • Standard Connections		• Data access control • Firmware Supervisor • Secure Digital (SD) card • Standard Connections • Safety Connections	

[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 page 104.

[2] When you use this controller with the Logix Designer application, version 29, the application limits the number of local I/O modules in the project to 16. For more information, see Knowledgebase Article *5380 CompactLogix controllers limited to 16 local Compact 5000 I/O modules in V29 of Studio 5000.®*
With the Logix Designer application, version 30 or later, the controller supports as many as 31 local I/O modules.

IMPORTANT When you use a CompactLogix 5380 or Compact GuardLogix 5380 controller, you do not need to configure a System Overhead Time Slice value.

Features Supported by Compact GuardLogix 5380 Controllers via the Safety Task

You can use the Compact GuardLogix 5380 controllers in safety applications via the Safety task in the Logix Designer application.

In the Logix Designer application, 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[1]	
	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[2]	—	X
Function Block Diagrams (FBD)	—	X
Integrated motion	X[3]	X
Drive Safety Instructions	X	—
Ladder Diagram (LD)	X	X
Language switching	X	X
License-based source protection	—	X
Import program components	—	X
Export program components	X	X
Sequential Function Chart (SFC) routines	—	X
Structured Text (ST)	—	X

[1] Compact GuardLogix 5380 SIL 2 controllers are compatible with Studio 5000 Logix Designer Application, version 31 or later. Compact GuardLogix 5380 SIL 3 controllers are compatible with Studio 5000 Logix Designer Application, Version 32 or later

[2] 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.

[3] Limited to the use of Drive Safety Instructions with Kinetix 5700 ERS4 drives.

IMPORTANT Safety Consideration

Compact GuardLogix 5380 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 GuardLogix 5560 controller, or a Compact GuardLogix 5370 controller, the safety consumed tag can be configured as either unicast or multicast. A GuardLogix 5560 controller requires Studio 5000 Logix Designer application version 19 or later for unicast produce/consume safety tags.

CIP Security

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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

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

Rockwell Automation uses the following products to implement CIP Security:

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

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

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

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

Secure Controller Systems

The CompactLogix 5380 controller, firmware revision 32, supports IEC-62443-4-2 SL 1 requirements. For security features and system requirements, see Develop Secure Applications on page 195.

Power the System

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controller provides power to the system as follows:

- MOD Power—System-side power that powers the system and lets modules transfer data and execute logic.

  System-side power is provided through the MOD Power RTB.
- SA Power—Field-side power that powers some Compact 5000 I/O modules and field-side devices that are connected to them.

  Field-side power is provided through the SA Power RTB.

There are specific considerations and restrictions that you must be aware of before you connect MOD power and SA power to a CompactLogix 5380 system or to a Compact GuardLogix 5380 system.

For more information on how to connect MOD power and SA power to the different systems, see the following:

- How to Power CompactLogix 5380 Controllers—Chapter 2 on page 25
- How to Power Compact GuardLogix 5380 Controllers—Chapter 3 on page 31

Real-time Clock

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

CompactLogix 5380 controllers can retain the date and time of the real-time clock (RTC) for a number of days, depending on the temperature of the controller.

Table 3 - RTC- Hold-up Time Duration

Ambient Temperature	Hold-up Time (Typical)
40 °C (104 °F)	7 days
60 °C (140 °F)	5 days

Notes:

How to Power CompactLogix 5380 Controllers

This chapter explains how to power standard CompactLogix™ 5380 controllers.

For information on how to power Compact GuardLogix® 5380 controllers, see Chapter 3, How to Power Compact GuardLogix 5380 Controllers on page 31.

Two Types of Power

Applies to these controllers:
CompactLogix 5380

The CompactLogix 5380 controllers provide power to the system as follows:

- MOD Power—System-side power that powers the system and lets modules transfer data and execute logic.

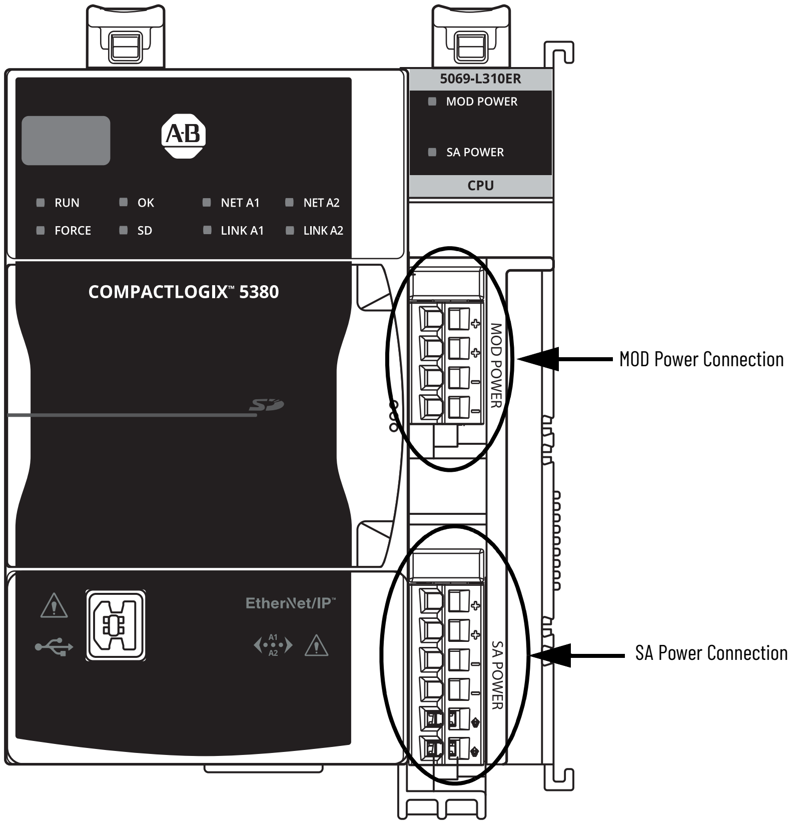
  System-side power is provided through the MOD Power RTB.

- SA Power—Field-side power that powers some Compact 5000™ I/O modules and field-side devices that are connected to them.

  Field-side power is provided through the SA Power RTB.

Connect external power supplies to the RTBs to provide MOD power and SA power. Figure 6 shows the RTBs on a CompactLogix 5380 controller.

Figure 6 - MOD Power and SA Power RTBs on a CompactLogix 5380 Controller



Power begins at the controller and passes across the Compact 5000 I/O module internal circuitry via power buses.

MOD power passes across a MOD power bus, and SA power passes across a SA power bus. The MOD power bus and SA power bus are isolated from each other.

IMPORTANT We **recommend** that you use separate external power supplies for MOD power and SA power, respectively. This practice can help prevent unintended consequences that can result if you use one supply.

If you use separate external power supplies, the loss of power from one external power supply does not affect the availability of power from the other supply. For example, if separate MOD and SA external power supplies are used and SA power is lost, MOD power remains available for the CompactLogix 5380 controller and Compact 5000 I/O modules. As such, data transfer continues in the system.

For more information on how to connect MOD power and SA power, see the CompactLogix 5380 Controllers Installation Instructions, publication 5069-IN013

MOD Power

Applies to these controllers:
CompactLogix 5380

MOD power is a DC power source that is required to operate a CompactLogix 5380 system.

IMPORTANT You can only use DC power on the MOD power bus. Do not connect AC power to the MOD power bus.

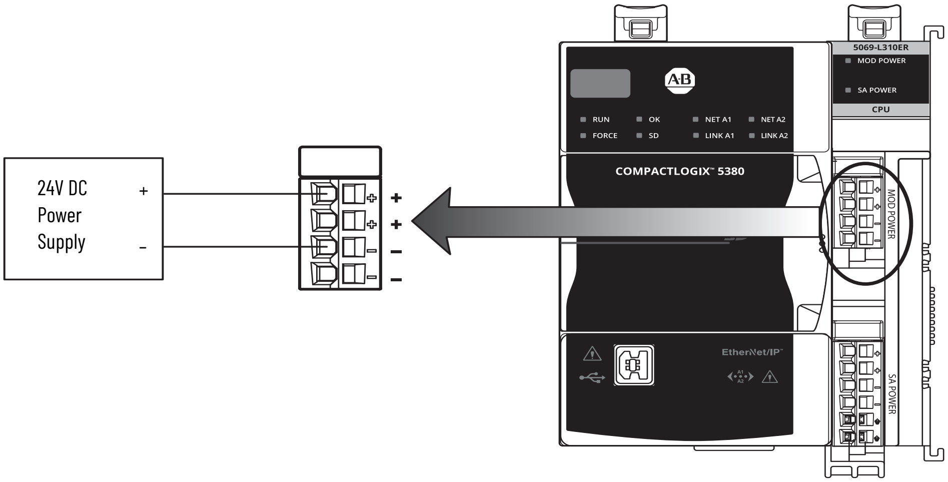
When external power is disconnected, the 5380 controller stores enough power to save the project to the on-board NVS memory.

Remember the following:

- Every module in the CompactLogix 5380 system draws current from the MOD power bus and passes the remaining current to the next module.
- MOD power lets Compact 5000 I/O modules transfer data and the controller execute logic.
- A CompactLogix 5380 system uses only one MOD power bus.
- The total continuous current draw across the MOD power bus must not be more than 10 A, max, at 18…32V DC.
- We recommend that you use an external power supply that is adequately sized for the total MOD power bus current draw in the system.

  You must consider **inrush current requirements** when you calculate the total MOD power bus current draw in the system.

Figure 7 - External Power Supply Provides MOD Power



MOD Power Bus

When the MOD power source is turned on, the following occurs.

1. The CompactLogix 5380 controller draws current from the MOD power bus and passes the remaining current through to the next module.
2. The next module draws MOD power bus current and passes the remaining current through to the next module.
3. The process continues until MOD power bus current needs are met for all modules in the system.

For more information on the current that the Compact 5000 I/O modules draw from the MOD power bus, see the Compact 5000 I/O Modules Specifications Technical Data, publication 5069-TD001.

SA Power

Applies to these controllers:
CompactLogix 5380

SA power provides power to devices that are connected to some of the Compact 5000 I/O modules in the CompactLogix 5380 system. SA power is connected to the controller via an SA power RTB.

Remember the following:

- Some Compact 5000 I/O modules draw current from the SA power bus and pass the remaining current to the next module.
- Some Compact 5000 I/O modules only pass current along the SA power bus to the next module.
- A CompactLogix 5380 system can have multiple SA power buses. The first SA power bus starts at the controller and passes across the I/O modules that are installed to the right of the controller.

  You use a 5069-FPD field potential distributor to establish a new SA power bus. The new SA power bus is isolated from the SA power bus to its left in the system.

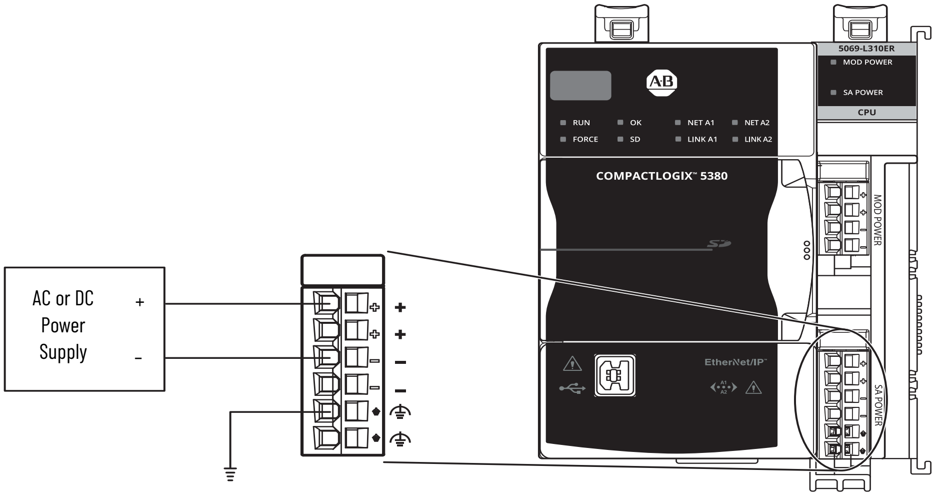
  For more information on how to use a 5069-FPD field potential distributor in a CompactLogix 5380 system, see page 29.
- If the SA power source uses DC voltage, the total continuous current draw across the SA power bus must not be more than to 10 A, max at 18…32V DC.
- We recommend that you use an external power supply that is adequately sized for the total SA power bus current draw on an individual bus.

  You must consider **inrush current requirements** when you calculate the total SA power bus current draw in the system.
- Connections to an SA power bus use a shared common. All inputs that draw current from an SA power bus to power field-side devices have a return through circuitry to the SA - terminal on the SA power connector.

IMPORTANT Each SA power bus has a shared common unique to that bus because SA power buses are completely isolated from each other.

The SA power bus that the CompactLogix 5380 controller establishes has a shared common. If you use a 5069-FPD field potential distributor to establish a new SA power bus in the system, that second bus has its own shared common for modules that draw current from it.

Figure 8 - External Power Supply Provides SA Power



When the SA power source is turned on, the following occurs.

1. The CompactLogix 5380 controller draws current from the SA power bus and passes the remaining current through to the next module.

IMPORTANT	The level of current that the CompactLogix 5380 controller draws from the SA power bus is negligible. It draws 10 mA (DC Power), 25 mA (AC power).

2. The next module completes one of these tasks.
   - If the module uses SA power, the module draws current from the SA power bus and passes the remaining current through to the next module.
   - If the module does not use SA power bus current, the module passes the remaining current through to the next module.
3. The process continues until all SA power bus current needs are met for the modules on the SA power bus.

If your system includes AC and DC modules that require SA power, you must use a 5069-FPD field potential distributor to establish a separate SA power bus and separate the module types on the isolated SA power buses.

For more information on the current that the Compact 5000 I/O modules draw from the SA power bus, see the Compact 5000 I/O Modules Specifications Technical Data, publication 5069-TD001.

Track SA Power Bus Current Draw

We recommend that you track the SA power bus current draw, max, per module, and collectively for the CompactLogix 5380 system.

You must make sure that the Compact 5000 I/O modules that are installed on an SA power bus do not consume more than 10 A. If so, you must establish another SA power bus.

Consider the following with this example:

- The values in this example represent a worst-case calculation. That is, all modules that draw SA power bus current, draw the maximum available on the module.
- Not all modules that are shown in Figure 9 use SA power bus current. For example, the 5069-ARM and 5069-OW4I modules only pass SA power bus current to the next module.

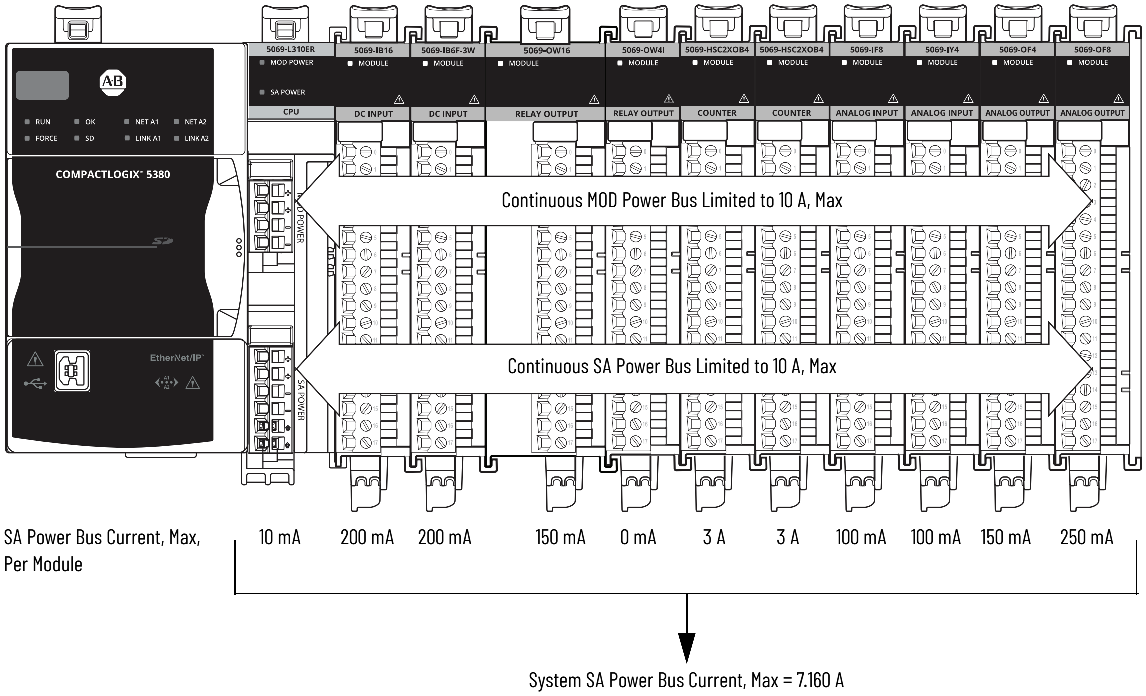
  Other modules that do not use SA power bus current, but are not shown in the graphic, include the 5069-OB16, 5069-OB16F, 5069-OX4I, and 5069-SERIAL modules.

- System SA power bus current, max, is calculated as each module draws SA power bus current. The calculation begins with the controller. The controller SA power bus current draw used for the calculation is 10 mA for DC power

  In Figure 9, after the 5069-IB16 module in slot 1 draws SA power bus current, the system SA power bus current, max, is 210 mA.

  After the 5069-IB16 module in slot 2 draws SA power bus current, the system SA power bus current draw is 410 mA. This process continues until the system SA power bus current, max, is 7.160 A.

Figure 9 - CompactLogix 5380 System - Calculate SA Power Bus Current Draw



Use a 5069-FPD Field Potential Distributor to Create a New SA Power Bus

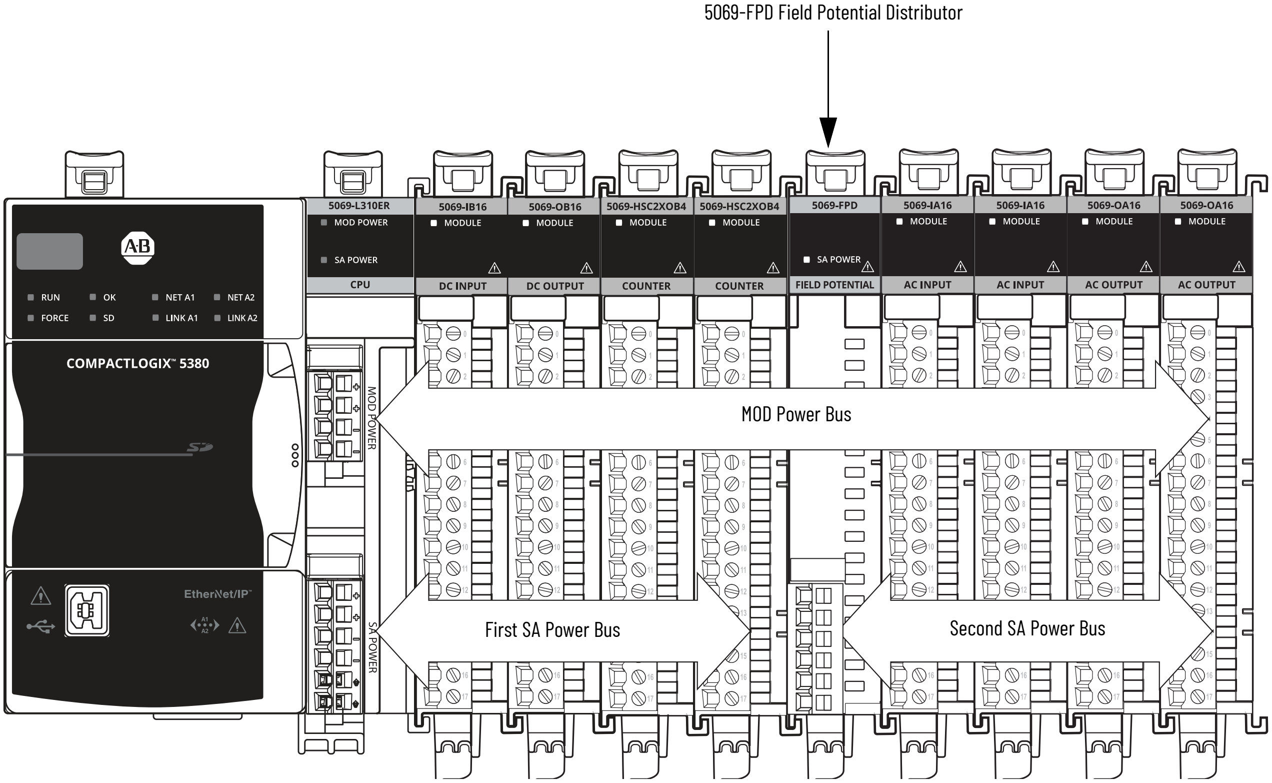
You can use a 5069-FPD field potential distributor to establish a new SA power bus in a CompactLogix 5380 system.

The field potential distributor blocks the current that passes across the SA power bus to its left. At that point, the field potential distributor establishes a new SA power bus for modules to the right. The new SA power bus is isolated from the SA power bus to its left in the system.

You can connect either a 24V DC or 120/240V AC external power supply to a 5069-FPD field potential distributor in a CompactLogix 5380 system.

Figure 10 shows a CompactLogix 5380 system that uses a 5069-FPD field potential distributor to create a second SA power bus.

Figure 10 - CompactLogix 5380 System - Create a New SA Power Bus



You can install multiple 5069-FPD field potential distributors in the same system, if necessary.

SA Power—Additional Notes

- Other examples of system configurations that use multiple SA power buses include:
  - The modules in the system collectively draw more than 10 A of SA power. That is, the maximum current that one SA power bus can provide.
  - The modules in the system must be isolated according to module types, such as digital I/O and analog I/O modules.
  - The modules in the system are isolated according to the type of field-side device to which they are connected.

    For example, you can separate modules that are connected to field-side devices that use DC voltage from modules that are connected to field-side devices that require AC voltage.
- The actual current in CompactLogix 5380 system changes based on the operating conditions at a given time.

  For example, the SA power bus current draw on some modules is different if all channels power field devices or half of the channels power field devices.
- Some Compact 5000 I/O modules use field-side power but do not draw it from a SA power bus. The modules receive field-side power from an external power supply that is connected directly to the I/O module.

  For example, the 5069-OB16 and 5069-OB16F modules use Local Actuator (LA) terminals on the module RTB, that is, LA+ and LA– terminals for all module channels.

  In this case, you can use the same external power supply that is connected to the SA power RTB on the controller to the LA+ and LA– terminals.

IMPORTANT	You must consider the current limit of an external power supply if you use it to provide power to the SA power RTB on the controller and the LA+ and LA– terminals on a 5069-OB16 or 5069-OB16F module.

Chapter 3

How to Power Compact GuardLogix 5380 Controllers

This chapter explains how to power Compact GuardLogix® 5380 controllers.

For information on how to power standard CompactLogix™ 5380 controllers, see Chapter 2, How to Power CompactLogix 5380 Controllers on page 25.

Two Types of Power

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The Compact GuardLogix 5380 controllers provide power to the system as follows:

- MOD Power - System-side power that powers the system and lets modules transfer data and execute logic.

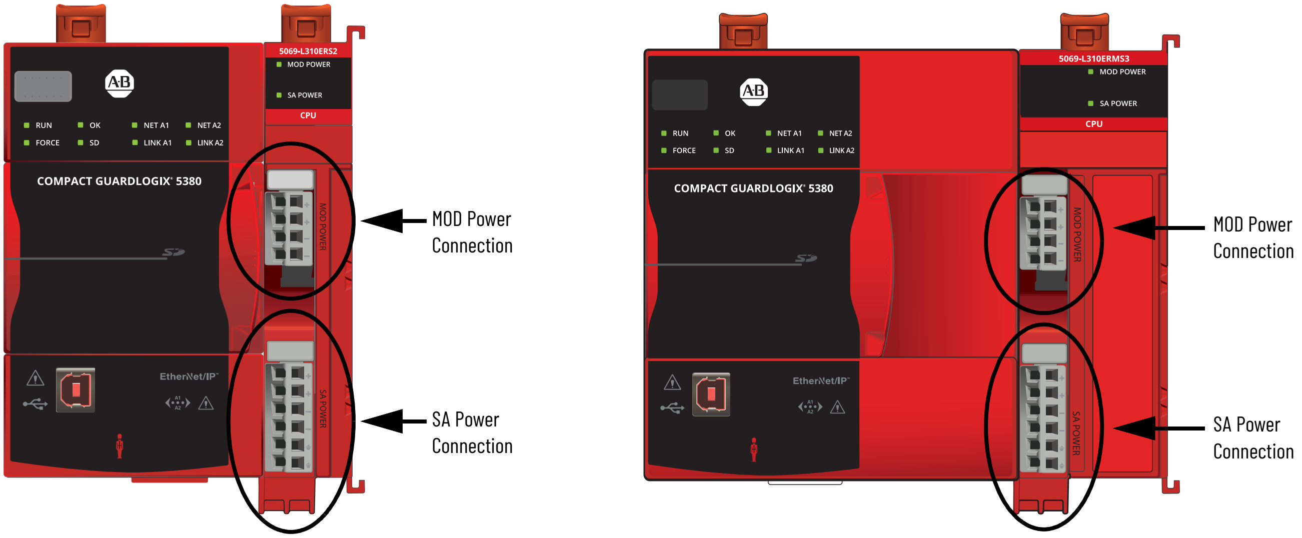
  System-side power is provided through the MOD Power RTB.
- SA Power - Field-side power that powers some Compact 5000™ I/O modules and field-side devices that are connected to them.

  Field-side power is provided through the SA Power RTB.

IMPORTANT	Both the MOD and SA Power must be DC power on the controller side. DC power for the Compact GuardLogix controllers must come from an SELV/PELV-rated power source. If you use an AC voltage for local I/O modules, then you must connect through a 5069-FPD field potential distributor module. An AC voltage cannot be terminated on the controller.

Connect external power supplies to the RTBs to provide MOD power and SA power. Figure 11 shows the RTBs on a Compact GuardLogix 5380 controller.

Figure 11 - MOD and SA Power RTBs on Compact GuardLogix 5380 SIL2 and SIL 3 Controllers



Power begins at the controller and passes across the Compact 5000 I/O module internal circuitry via power buses.

MOD power passes across a MOD power bus, and SA power passes across a SA power bus. The MOD power bus and SA power bus are isolated from each other.

IMPORTANT	We recommend that you use separate external power supplies for MOD power and SA power, respectively. This practice can help prevent unintended consequences that can result if you use one supply. If you use separate external power supplies, the loss of power from one external power supply does not affect the availability of power from the other supply. For example, if separate MOD and SA external power supplies are used and SA power is lost, MOD power remains available for the Compact GuardLogix 5380 controller and Compact 5000 I/O modules. As such, data transfer continues in the system.

For more information on how to connect MOD power and SA power, see these publications:

- Compact GuardLogix 5380 SIL2 Controllers Installation Instructions, publication 5069-IN014.
- Compact GuardLogix 5380 SIL3 Controllers Installation Instructions, publication 5069-IN023.

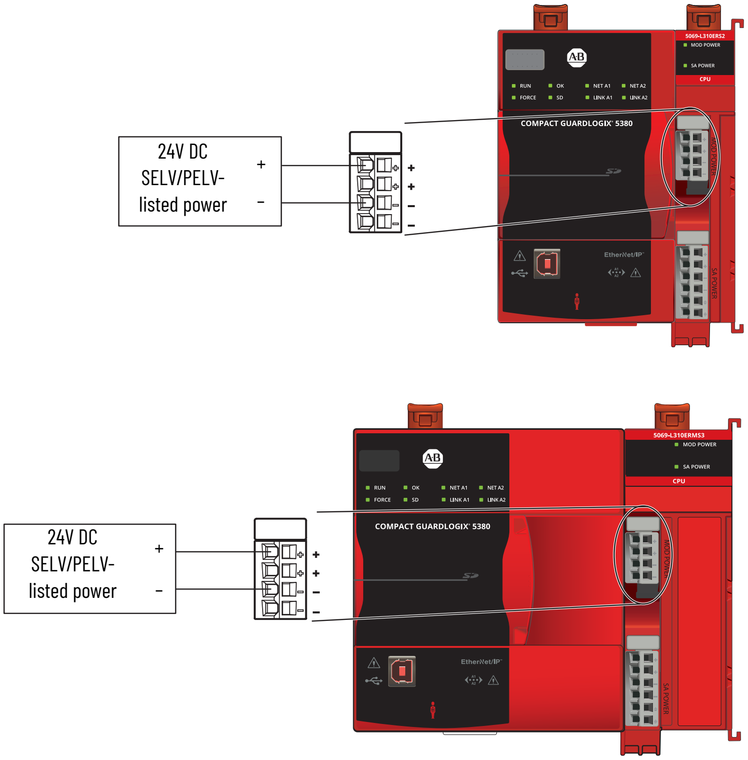
MOD Power

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

MOD power is a DC power source that is required to operate a Compact GuardLogix 5380 system. Remember the following:

- You must use SELV or PELV power supplies to provide MOD power to Compact GuardLogix 5380 controllers.
- Every module in the Compact GuardLogix 5380 system draws current from the MOD power bus and passes the remaining current to the next module.
- MOD power lets Compact 5000 I/O modules transfer data and the controller execute logic.
- A Compact GuardLogix 5380 system uses only one MOD power bus.
- You must limit the MOD power source to 5 A, max, at 18…32V DC.
- We recommend that you use an external SELV/PELV rated power supply that is adequately sized for the total MOD power bus current draw in the system. You must consider **current inrush requirements** when you calculate the total MOD power bus current draw in the system.

Figure 12 - External Power Supply Provides MOD Power



MOD Power Bus

When the MOD power source is turned on, the following occurs.

1. The Compact GuardLogix 5380 controller draws current from the MOD power bus and passes the remaining current through to the next module.
2. The next module draws MOD power bus current and passes the remaining current through to the next module.
3. The process continues until MOD power bus current needs are met for all modules in the system.

For more information on the current that the Compact 5000 I/O modules draw from the MOD power bus, see the Compact 5000 I/O Modules Specifications Technical Data, publication 5069-TD001.

SA Power

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

SA power provides power to devices that are connected to some of the Compact 5000 I/O modules in the Compact GuardLogix 5380 system. SA power is connected to the controller via an SA power RTB.

Remember the following:

IMPORTANT More specific restrictions apply when you connect SA power to a Compact GuardLogix 5380 controller or 5069-FPD field potential distributor.

For more information, see page 38.

- You must use SELV or PELV power supplies to provide SA power to Compact GuardLogix 5380 controllers.
- If the SA power source uses DC voltage, you must limit the SA power source to 10 A, max at 18...32V DC.
- Some Compact 5000 I/O modules draw current from the SA power bus and pass the remaining current to the next module.

- Some Compact 5000 I/O modules only pass current along the SA power bus to the next module.
- If the SA power source is an AC power supply, or non-SELV/PELV DC source, then you must terminate from an FPD before consuming the power on the SA power bus.
- A Compact GuardLogix 5380 system can have multiple SA power buses. The first SA power bus starts at the controller and passes across the I/O modules that are installed to the right of the controller.

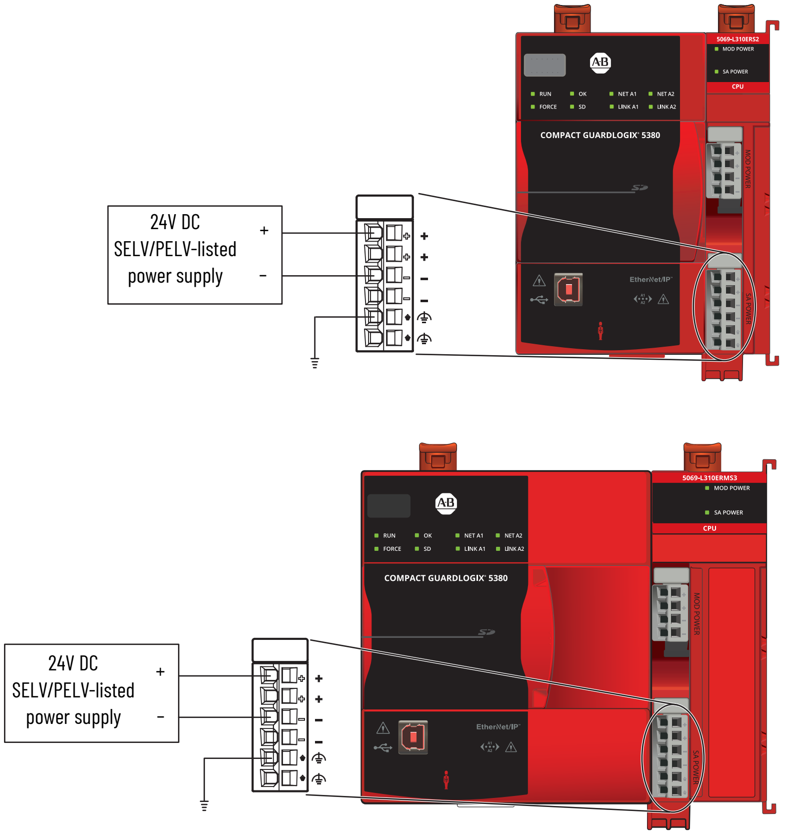
  You can use a 5069-FPD field potential distributor to establish a new SA power bus. The new SA power bus is isolated from the SA power bus to its left in the system.

  For more information on how to use a 5069-FPD field potential distributor in a CompactLogix 5380 system, see page 36.
- We recommend that you use an external power supply that is adequately sized for the total SA power bus current draw on an individual bus. You must consider **current inrush requirements** when you calculate the total SA power bus current draw on a specific bus.
- Connections to an SA power bus use a **shared common**. All inputs that draw current from an SA power bus to power field-side devices have a return through circuitry to the SA - terminal on the SA power connector.

IMPORTANT Each SA power bus has a shared common unique to that bus because SA power buses are completely isolated from each other.

The SA power bus that the controller establishes has a shared common. If you use a 5069-FPD field potential distributor to establish a new SA power bus in the system, that second bus has its own shared common for modules that draw current from it.

Figure 13 - External Power Supply Provides SA Power



When the SA power source is turned on, the following occurs.

1. The controller draws current from the SA power bus and passes the remaining current through to the next module.

IMPORTANT	The level of current that the Compact GuardLogix 5380 controller draws from the SA power bus is negligible. It draws 10 mA.

2. The next module completes one of these tasks.
   - If the module uses SA power, the module draws current from the SA power bus and passes the remaining current through to the next module.
   - If the module does not use SA power bus current, the module passes the remaining current through to the next module.
3. The process continues until all SA power bus current needs are met for the modules on the SA power bus.

For more information on the current that the Compact 5000 I/O modules draw from the SA power bus, see the Compact 5000 I/O Modules and EtherNet/IP Adapters Technical Data, publication 5069-TD001.

Track SA Power Bus Current Draw

We recommend that you track the SA power bus current draw, max, per module, and collectively for the Compact GuardLogix 5380 system. You must make sure that the Compact 5000 I/O modules that are installed on an SA power bus do not consume more than 10 A. If so, you must establish another SA power bus.

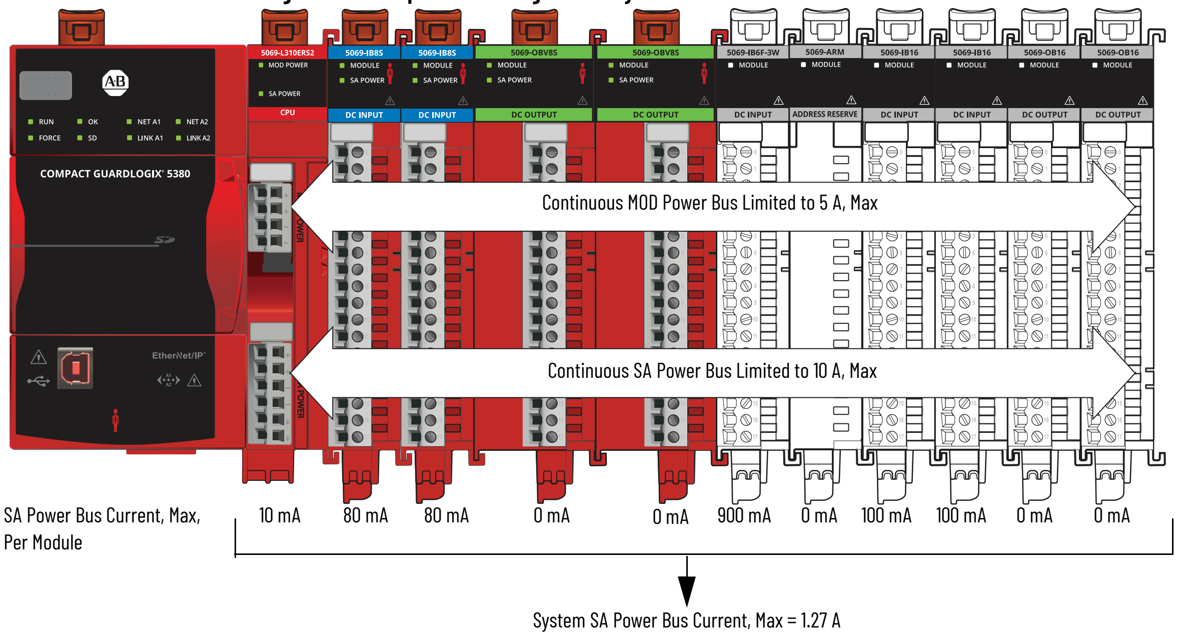
Consider the following with this example:

- The values in this example represent a worst-case calculation. That is, all modules that draw SA power bus current, draw the maximum available on the module.
- Not all modules that are shown in Figure 14 on page 36 use SA power bus current. For example, the 5069-OBV8S, 5069-ARM and 5069-OB16 modules only pass SA power bus current to the next module. Other modules that do not use SA power bus current, but are not shown in the graphic, include the 5069-OB16F and 5069-OX4I modules.
- System SA power bus current, max, is calculated as each module draws SA power bus current. The calculation begins with the controller. The controller SA power bus current draw used for the calculation is 10 mA for DC power

  In Figure 14, after the 5069-IB8S module in slot 1 draws SA power bus current, the system SA power bus current, max, is 90 mA.

  After the 5069-IB8S module in slot 2 draws SA power bus current, the system SA power bus current draw is 170 mA. This process continues until the system SA power bus current, max, is 1.27 A.

Figure 14 - Compact GuardLogix 5380 System - Calculate SA Power Bus Current Draw[1]



Use a 5069-FPD Field Potential Distributor to Create a New SA Power Bus

IMPORTANT	If you use local Compact 5000 I/O relay modules, or an AC voltage for locl Compact 5000 I/O modules, then you must connect through a 5069-FPD field potential distributor module. An AC voltage cannot be terminated on the controller.

You can use a 5069-FPD field potential distributor to establish a new SA power bus in a Compact GuardLogix 5380 system.

The field potential distributor blocks the current that passes across the SA power bus to its left. At that point, the field potential distributor establishes a new SA power bus for modules to the right. The new SA power bus is isolated from the SA power bus to its left in the system.

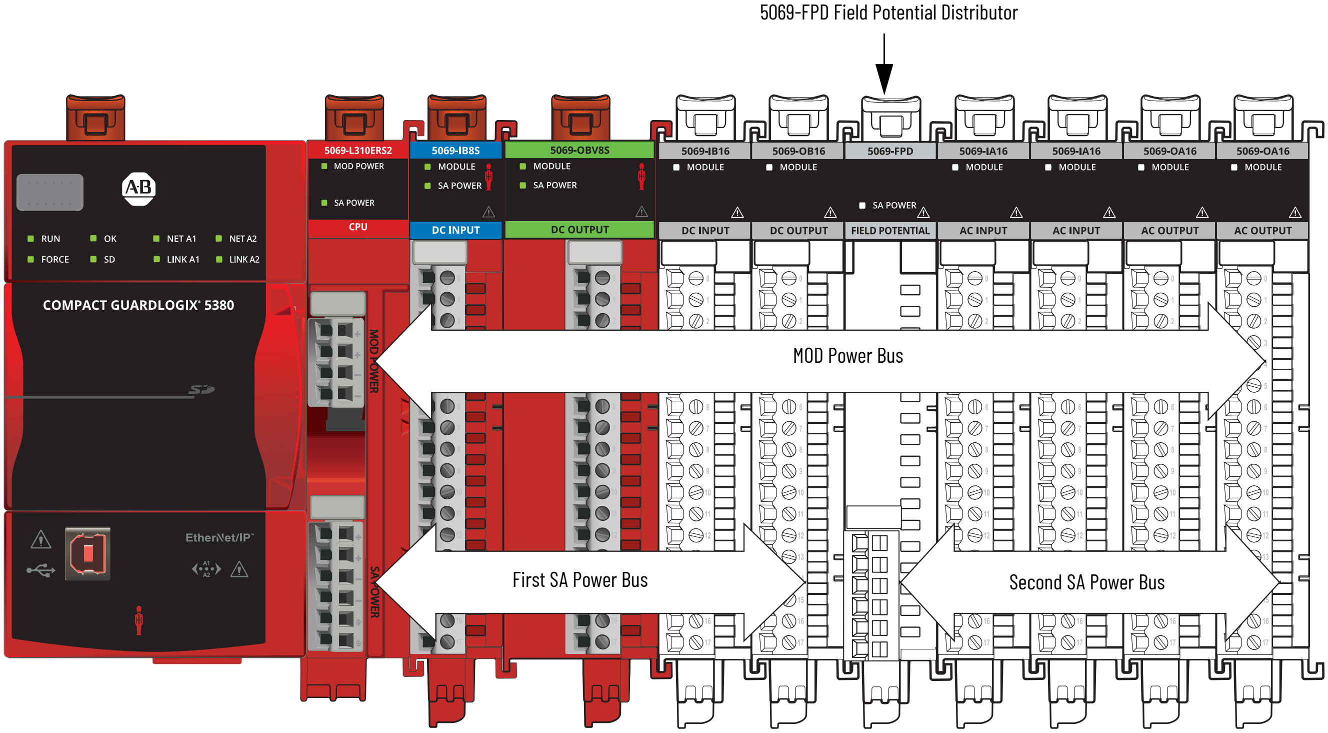
You can connect either a 24V DC or 120/240V AC external power supply to a 5069-FPD field potential distributor in a Compact GuardLogix 5380 system.

IMPORTANT	Some restrictions apply when you connect SA power to a 5069-FPD field potential distributor. For more information, see page 38.

Figure 15 shows a Compact GuardLogix 5380 system that uses a 5069-FPD field potential distributor to create a second SA power bus.

[1] Although a Compact GuardLogix 5380 SIL2 controller is shown, this example also applies to Compact GuardLogix 5380 SIL 3 controllers.

Figure 15 - Compact GuardLogix 5380 System - Create a New SA Power Bus[1]



You can install multiple 5069-FPD field potential distributors in the same system, if necessary.

[1] Although a Compact GuardLogix 5380 SIL2 controller is shown, this example also applies to Compact GuardLogix 5380 SIL 3 controllers.

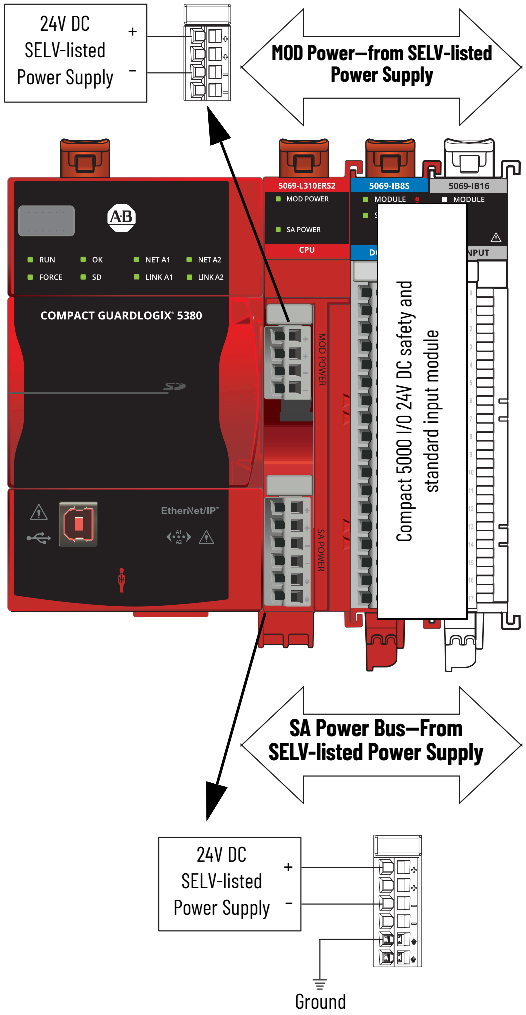
Restrictions When You Connect SA Power to a Compact GuardLogix 5380 System

Remember these restrictions in Table 4 hen you connect SA power to a Compact GuardLogix 5380 system.

Table 4 - SA Power Restrictions - Compact GuardLogix 5380 System

Component to Which SA Power Is Connected	Restrictions
Compact GuardLogix 5380 SIL 2 or SIL 3 Controller	• You must use SELV/PELV-listed power supplies to provide SA power to Compact GuardLogix 5380 controllers. • You can only connect a 24V DC SELV/PELV-listed power supply. • The total continuous current draw across the SA power bus must not be more than 10 A, max at 0…32V DC.

Example Compact GuardLogix System

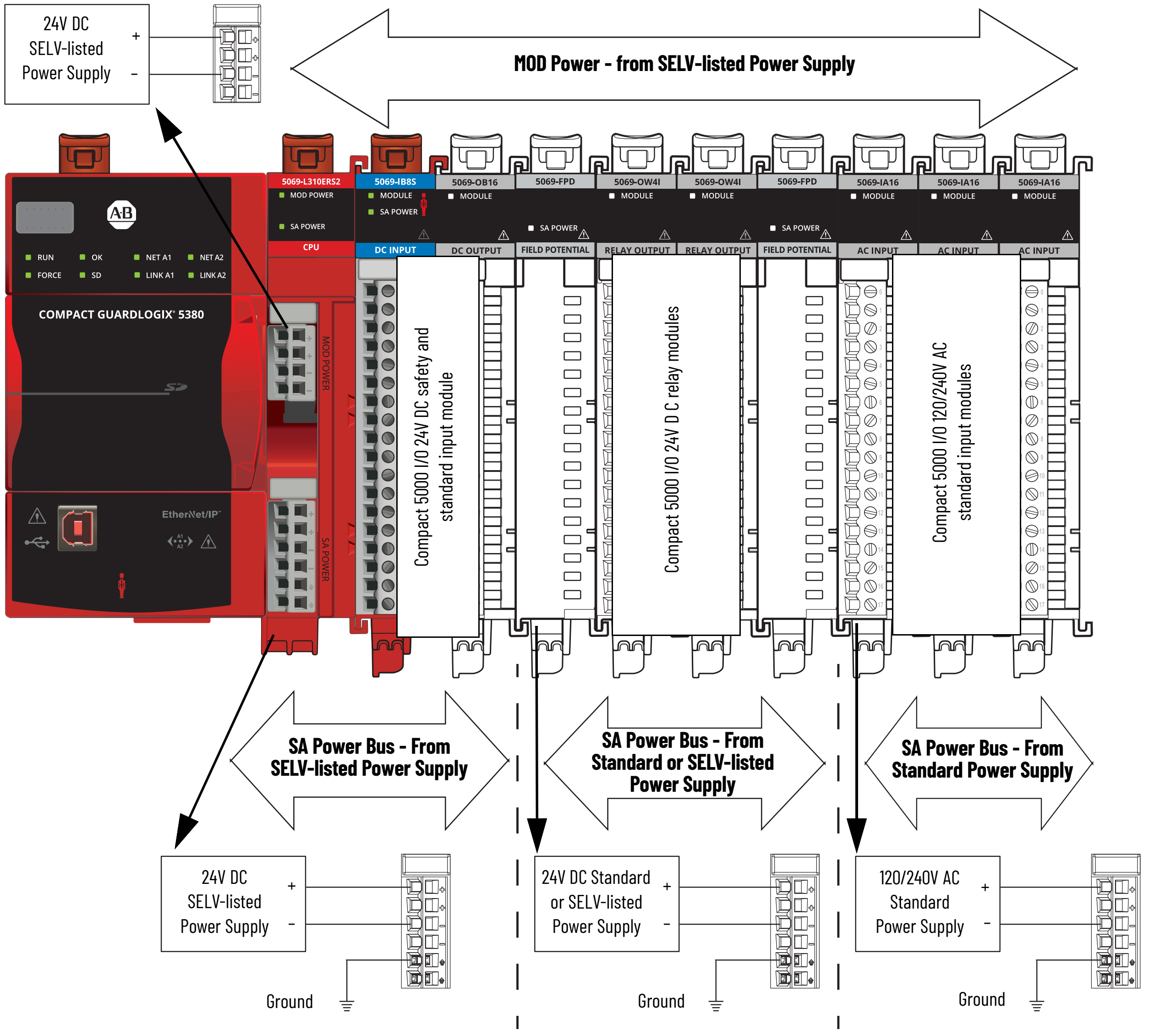


*Although a Compact GuardLogix 5380 SIL2 controller is shown, this example also applies to Compact GuardLogix 5380 SIL 3 controllers.

Table 4 - SA Power Restrictions - Compact GuardLogix 5380 System (Continued)

Component to Which SA Power Is Connected	Restrictions
5069-FPD Field Potential Distributor With Compact 5000 I/O Standard Modules Only	In addition to the restrictions on page 38, these restrictions also apply: • You can use non-SELV or PELV power supplies if only Compact 5000 I/O standard modules are installed to the right of the 5069-FPD field potential distributor. • You can connect a 24V DC or 120/240V AC power supply. The example uses a 120/240V AC power supply. – If the SA power that is connected to the 5069-FPD field potential distributor is **DC voltage**, the total continuous current draw across the SA power bus must not be more than 10 A, max at 0…32V DC. – If a Compact GuardLogix 5380 system includes Compact 5000 I/O relay modules (5069-OW4I, 5069-OX4I, 5069-OW16), or I/O modules that require SA power that is **AC voltage**, you must install these modules to the right of a 5069-FPD field potential distributor, as shown. **IMPORTANT**: This requirement applies even if it means that you must install the 5069-FPD field potential distributor immediately to the right of the Compact GuardLogix 5380 controller. • If a Compact GuardLogix 5380 system includes Compact 5000 I/O standard modules that use SA power that is provided by a power supply that is not SELV/PELV-listed, the I/O modules must be installed to the right of a 5069-FPD field potential distributor. **IMPORTANT**: The SA power bus that the 5069-FPD field potential distributor establishes cannot include any Compact 5000 I/O safety modules.

Example Compact GuardLogix System

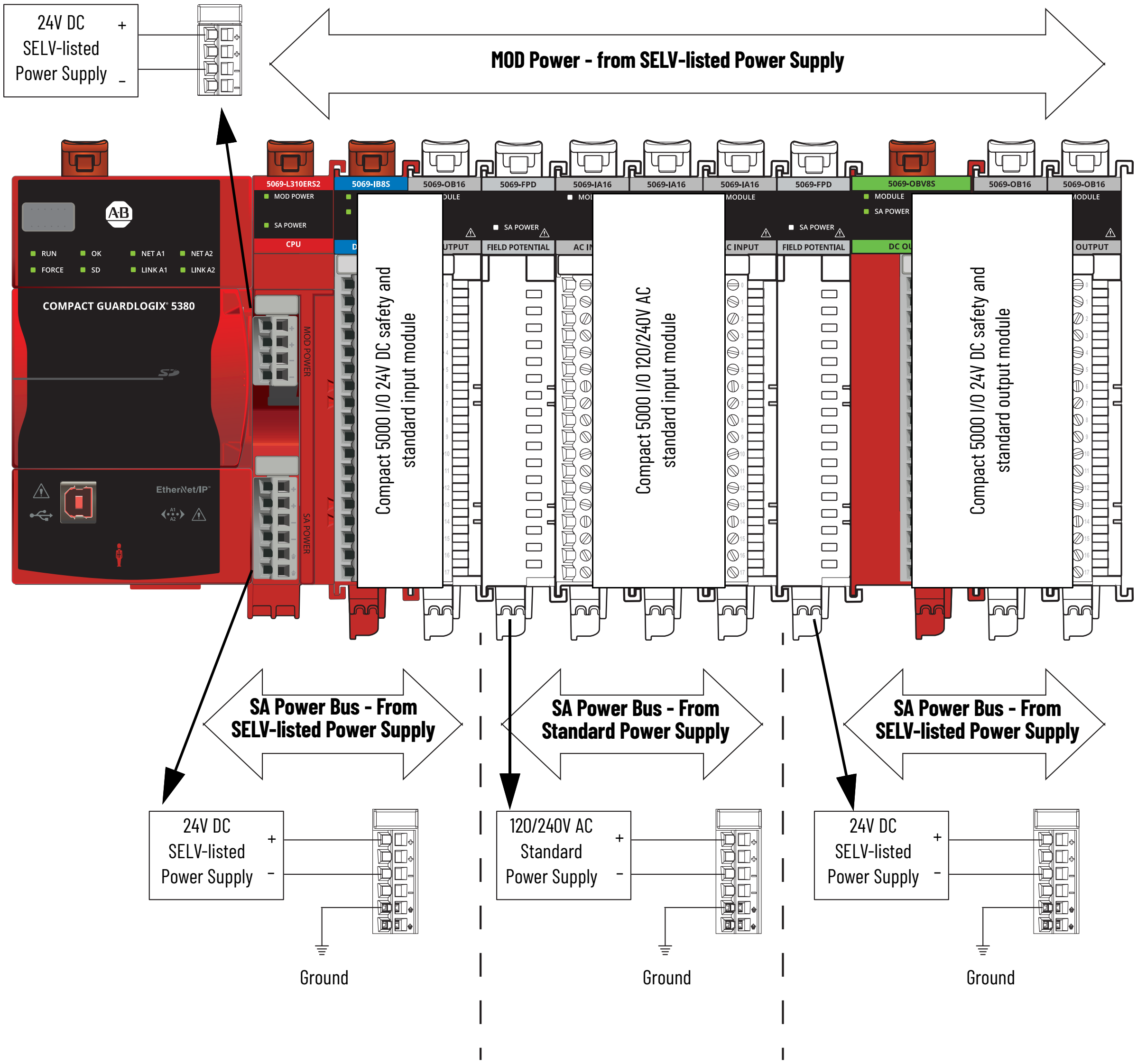

24V DC SELV-listed Power Supply
+
–
MOD Power - from SELV-listed Power Supply
5069-L310ERS2
5069-IB8S
5069-OB16
5069-FPD
5069-OW4I
5069-OW4I
5069-FPD
5069-IA16
5069-IA16
5069-IA16
MOD POWER
SA POWER
MODULE
CPU
DC INPUT
DC OUTPUT
FIELD POTENTIAL
RELAY OUTPUT
RELAY OUTPUT
FIELD POTENTIAL
AC INPUT
AC INPUT
AC INPUT
RUN
OK
FORCE
SD
NET A1
NET A2
LINK A1
LINK A2
COMPACT GUARDLOGIX 5380
EtherNet/IP
Compact 5000 I/O 24V DC safety and standard input module
Compact 5000 I/O 24V D C relay modules
Compact 5000 I/O 120/240V AC standard input modules
SA Power Bus - From SELV-listed Power Supply
SA Power Bus - From Standard or SELV-listed Power Supply
SA Power Bus - From Standard Power Supply
24V DC SELV-listed Power Supply
24V DC Standard or SELV-listed Power Supply
120/240V AC Standard Power Supply
Ground
Ground
Ground

*Although a Compact GuardLogix 5380 SIL2 controller is shown, this example also applies to Compact GuardLogix 5380 SIL 3 controllers.

Table 4 - SA Power Restrictions - Compact GuardLogix 5380 System (Continued)

Component to Which SA Power Is Connected	Restrictions
5069-FPD Field Potential Distributor With Compact 5000 I/O Safety and Standard Modules	In addition to the restrictions on page 38 and page 39, this restriction also applies: • You must use SELV or PELV power supplies to provide SA power to Compact 5000 I/O safety modules that are installed to the right of the 5069-FPD field potential distributor.

Example Compact GuardLogix 5380 System



*Although a Compact GuardLogix 5380 SIL2 controller is shown, this example also applies to Compact GuardLogix 5380 SIL 3 controllers.

SA Power—Additional Notes

- Other examples of system configurations that use multiple SA power buses include:
  - The modules in the system collectively draw more than 10 A of SA power. That is, the maximum current that one SA power bus can provide.
  - The modules in the system must be isolated according to module types, such as digital I/O and analog I/O modules.
  - The modules in the system are isolated according to the type of field-side device to which they are connected.

    For example, you can separate modules that are connected to field-side devices that use DC voltage from modules that are connected to field-side devices that require AC voltage.
- The actual current in a Compact GuardLogix 5380 system changes based on the operating conditions at a given time.

  For example, the SA power bus current draw on some modules is different if all channels power field devices or half of the channels power field devices.
- Some Compact 5000 I/O modules use field-side power but do not draw it from a SA power bus. The modules receive field-side power from an external power supply that is connected directly to the I/O module.

  For example, the 5069-OB16, 5069-OB16F, and 5069-OBV8S modules use Local Actuator (LA) terminals on the module RTB, that is, LA+ and LA– terminals for all module channels.

  In this case, you can use the same external power supply that is connected to the SA power RTB on the controller to the LA+ and LA– terminals.

IMPORTANT	You must consider the current limit of an external power supply if you use it to provide power to the SA power RTB on the controller and the LA+ and LA– terminals on a 5069-OB16, 5069-OB16F, or 5069-OBV8S module. The 5069-OBV8S module requires a SELV/PELV-rated power supply.

Notes:

Safety Concept of Compact GuardLogix 5380 Controllers

Functional Safety Capability

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The Compact GuardLogix® 5380 controller systems are 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.

Controller System	IEC 61508	IEC 62061	ISO 13849-1
	Type-approved and certified for use in safety applications up to and including:	Suitable for use in safety applications up to and including:	Suitable for use in safety applications up to and including:
Compact GuardLogix 5380 SIL 2 controller systems [1]	SIL 2	SIL CL2	Performance Level PLd (Cat. 3)
Compact GuardLogix 5380 SIL 3 controller systems[2][3]	SIL 3	SIL CL3	Performance Level PLe (Cat. 4)

[1] Compact GuardLogix 5380 SIL 2 controller catalog numbers have a '2' at the end, for example, 5069-L3*xxxxx*S2, and are for use in safety applications up to and including SIL 2.

[2] Compact GuardLogix 5380 SIL 3 controller catalog numbers have a '3' at the end, for example, 5069-L3*xxxxx*S3, and are for use in safety applications up to and including SIL 3.

[3] For SIL 3/PLe safety applications, the Compact GuardLogix® 5380 SIL 3 controller system consists of a primary controller with an internal 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 to 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 Compact GuardLogix safety system.

Safety Network Number

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

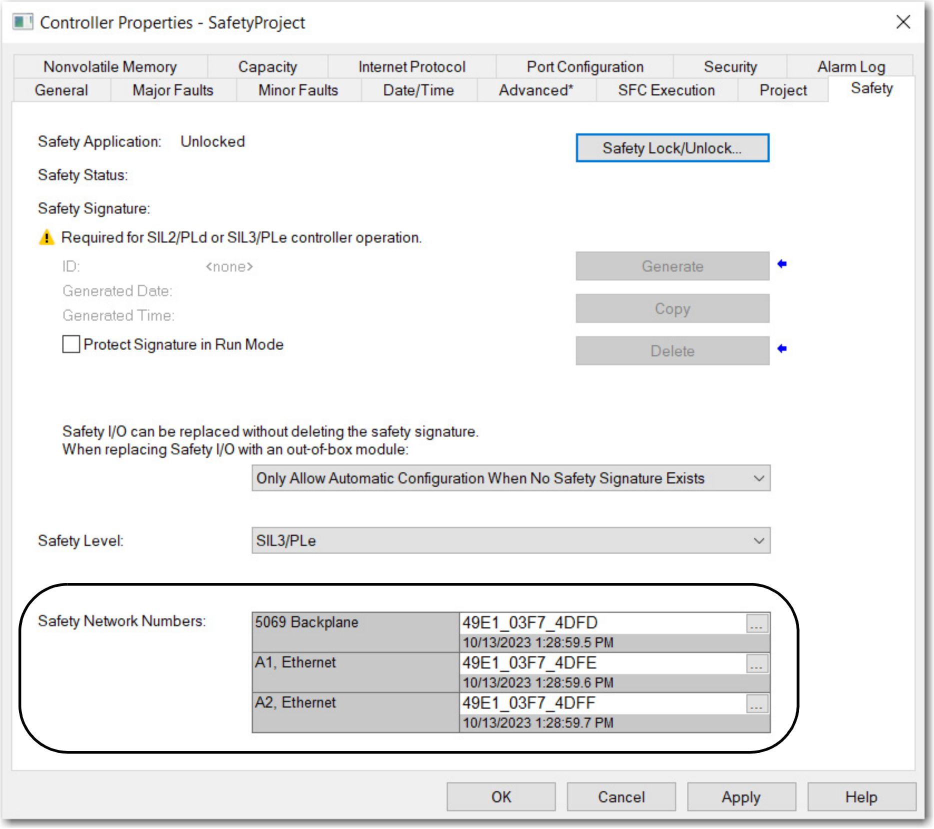
The safety network number (SNN) uniquely identifies CIP Safety™ subnets within a routable safety network. The combination of SNN + Node Address uniquely identifies each CIP Safety port on each device in the routable safety network.

The application assigns an SNN to each CIP Safety subnet attached to a Compact GuardLogix 5380 controller, including the backplane. If there are other Logix Safety controllers on an attached Ethernet network, assign the same SNN for this network in each controller application. This allows you to use Logix Designer's automatic assignment of safety network numbers for devices added to the application.

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

To assign SNNs, see Assign the Safety Network Number (SNN) on page 67.

Figure 16 - Safety Network Numbers



Safety Application: Unlocked

Safety Status:

Safety Signature:

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

ID: <none>

Generated Date:

Generated Time:

□ Protect Signature in Run Mode

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

Only Allow Automatic Configuration When No Safety Signature Exists

Safety Level: SIL3/PLe

Safety Network Numbers:

5069 Backplane	49E1_03F7_4DFD 10/13/2023 1:28:59.5 PM
A1, Ethernet	49E1_03F7_4DFE 10/13/2023 1:28:59.6 PM
A2, Ethernet	49E1_03F7_4DFF 10/13/2023 1:28:59.7 PM

Safety Signature

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The GuardLogix® system uses a safety signature to verify the integrity of a safety application:

- The safety signature applies to the entire safety portion of the controller project. The ability to create, record, and verify the safety signature is a mandatory part of the safety-application development process. The safety signature must be present to operate as a SIL 2/PLd or SIL 3/PLe safety controller. Nothing in the standard application is included in the safety signature.
- The safety signature is a hierarchy of multiple safety signature elements. For example, the safety task, programs, and routines are examples of safety signature elements.

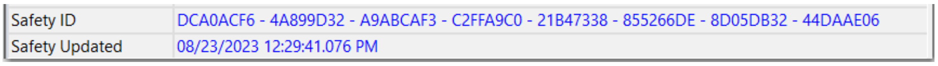
  Safety signature elements can help you during impact analysis by identifying the individual changes within a controller project. If your validation plan does not require revalidation of unchanged elements, your certification effort can be reduced.

  All safety signature elements are created at the time that you generate the safety signature for the project. To view all safety signature elements for a project, you can run the Safety Signature report.

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

- Safety signature ID--A unique 64-character alphanumeric identification number.
- Time stamp—The date and time that the safety signature was generated. For a safety signature element, the time stamp changes whenever its signature ID changes.

Figure 17 - Safety Signature



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

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

Distinguish Between Standard and Safety Components

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Slots of a Compact GuardLogix 5380 system chassis that are not used by the safety function can be populated with other Compact 5000™ I/O modules that are certified to the Low Voltage and EMC Directives. See http://www.rockwellautomation.com/rockwellautomation/certification/ce.page to find the CE certificate for the CompactLogix™ 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.

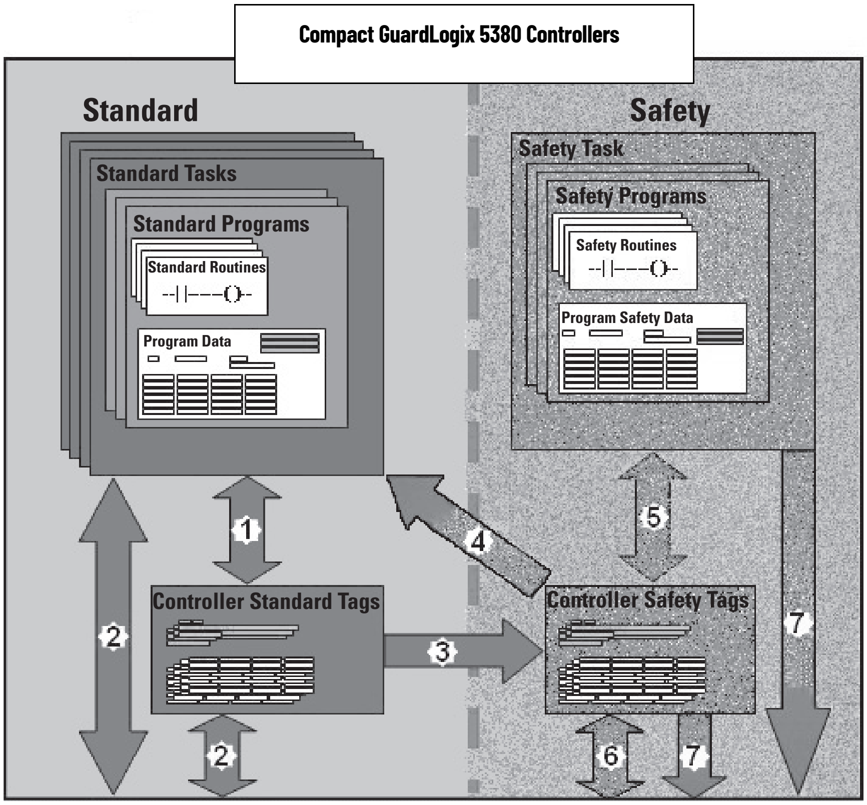
In addition, the Logix Designer application displays a safety class attribute whenever safety task, safety programs, safety routine, safety tag, or safety Add-On Instruction properties are displayed.

Controller Data-flow Capabilities

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

This illustration explains the standard and safety data-flow capabilities of the Compact GuardLogix 5380 controllers.

Figure 18 - Data-flow Capabilities



No.	Description
1	Standard tags and logic behave the same way that they do in a standard CompactLogix 5380 controller.
2	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.
3	Compact GuardLogix 5380 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 networks, including 1756 GuardLogix controllers and 5069 Compact 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 safety data.

Safety Terminology

The following table defines terms that are used in this manual.

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 a dangerous failure on demand	The average probability of a dangerous failure on demand.
PFH	Probability of dangerous failure per hour	The average frequency of a dangerous failure per hour.
PL	Performance Level	ISO 13849-1 safety rating.
SIL	Safety Integrity Level	A relative level of risk-reduction that is 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:

Connect to the Controller

Before You Begin

Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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

The EtherNet/IP driver:

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

USB driver:

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

For information on how to configure EtherNet/IP or USB drivers, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

Connection Options

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Before you can begin using your controller, you must make a connection to the controller. Make sure that you have already configured the EtherNet/IP or USB communication drivers. See the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

Connection options with the controller include:

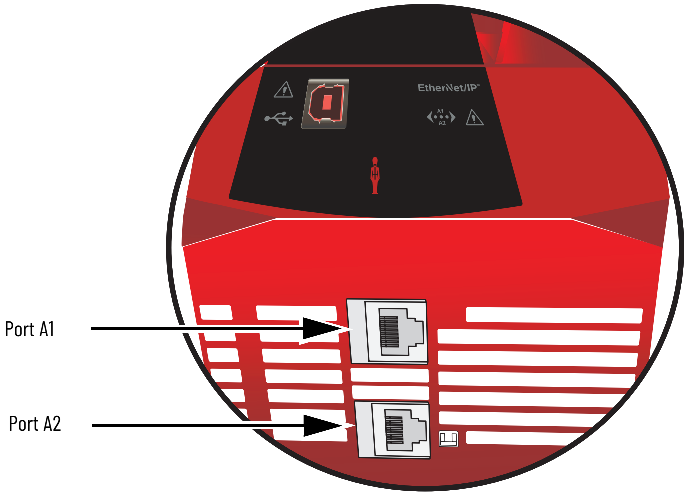
- Ethernet cable to an Ethernet port - The controller Ethernet ports support communication rates of 10 Mbps, 100 Mbps, and 1 Gbps. See Connect an Ethernet Cable on page 50.
- USB cable to the USB port - The controller USB port uses a Type B receptacle and is USB 2.0 compatible. The port runs at 12 Mbps. See Connect a USB Cable on page 50.

Connect an Ethernet Cable

The example graphic shows a Compact GuardLogix 5380 controller. You perform the same task to connect an Ethernet cable to a CompactLogix 5380 controller.

WARNING: If you connect or disconnect the communications cable with power applied to this module or any device on the network, 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.

If you are connecting a controller directly to an EtherNet/IP network, connect a CAT 5e or CAT 6 Ethernet cable with an RJ45 connector to an Ethernet port on the bottom of the controller.



For information on how to select the proper cable, see Guidance for Selecting Cables for EtherNet/IP Networks, publication ENET-WP007-EN-P.

Connect a USB Cable

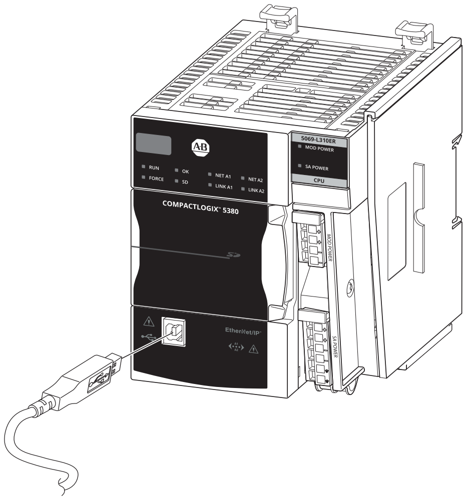
Use the USB connection to update firmware and download programs.

The example graphic shows a CompactLogix 5380 controller. You perform the same task to connect an Ethernet cable to a Compact GuardLogix 5380 controller.

The USB port is intended only for temporary local programming purposes and not intended for permanent connection. The USB cable is not to exceed 3.0 m (9.84 ft) and must not contain hubs.

WARNING: Do not use the USB port in hazardous locations.

Figure 19 - USB Connection



Set the IP Address

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

- The controller embedded Ethernet ports are 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.
- The controller is configured so that you must set the IP address each time that power is cycled.

  You can configure your controller so that you are not required to set an IP address each time that power is cycled.
- The controller is configured to use Dual-IP mode. As a result, you must set a unique IP address for port A1 and port A2.

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 Devices User Manual, publication ENET-UM006.

IMPORTANT	The EtherNet/IP mode in which the controller operates affects the setting and use of IP addresses on the controller. For example, if the controller operates in Dual-IP mode, you must set an IP address for each controller Ethernet port. That is, you must complete the steps that are described in this section twice–once for each port. For more information on how the EtherNet/IP modes affect the controller IP address, see Use EtherNet/IP Modes on page 117.

Use a Secure Digital Card to Set the Controller IP Address

You can use an SD card to set the controller IP address. The SD card can set the IP address when it loads a project onto the controller.

For more information on how to use an SD card, see Use the Secure Digital Card on page 91.

Duplicate IP Address Detection

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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 controller 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 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
• Both devices support duplicate IP address detection. • Second device is added to the network after the first device is operating on the network.	1. The device that began operation first uses the IP address and continues to operate without interruption. 2. The device that begins operation second detects the duplication and enters Conflict mode.
• Both devices support duplicate IP address detection. • Both devices were powered up at approximately the same time.	Both EtherNet/IP devices enter Conflict mode. To resolve this conflict, follow these steps. 1. Assign a new IP address to the controller. 2. Cycle power to the other device.
One device supports duplicate IP address detection and a second device does not.	1. Regardless of which device obtained the IP address first, the device that does not support IP address detection uses the IP address and continues to operate without interruption. 2. The device that supports duplicate IP address detection detects the duplication and enters Conflict mode.

DNS Addressing

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

IMPORTANT Safety Considerations

- Safety connections are not allowed to use host names (this requires DNS lookup, which is not allowed for Safety I/O). Safety devices on EtherNet/IP networks do not present the host name parameter. Standard devices do present the host name parameter, regardless of whether the project is safety or standard.
- Compact GuardLogix 5380 controllers can have safety connections or standard connections. When used in a standard project, GuardLogix 5580 controllers are considered standard devices (the only connections are standard consumed tags), so the controller presents the host name parameter.
- When Compact GuardLogix 5380 controllers are used in a safety project, it is assumed to be a safety device, and the host name parameter is not presented.

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

To use DNS addressing, follow these steps.

1. Assign a host name to the controller.

   A network administrator can assign a host name. Valid host names must be IEC-1131-3 compliant.
2. Configure the controller parameters.
3. Configure the IP address, subnet mask, gateway address, a host name for the controller, domain name, and primary/secondary DNS server addresses.

   In the DNS server, the host name must match the IP address of the controller.
4. In the Logix Designer application, add the controller to the I/O configuration tree.

IMPORTANT Remember the following:

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

Update Controller Firmware

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can use these tools to update the controller firmware:

- ControlFLASH™ or ControlFLASH Plus™ software
- AutoFlash feature of the Logix Designer application

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 Compact 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	Compact GuardLogix 5380 controllers have a different compiler than earlier controllers. You must re-validate that applications on earlier controllers compile correctly on Compact GuardLogix 5380 controllers.

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

Example:

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

Controller Firmware and Logix Designer Application Compatibility

In Logix 5000™ control systems, the controller firmware and the Logix Designer application must be of the same major revision level. For example, if the controller firmware revision is 31.xxx, you must use the Logix Designer application, version 31.

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

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

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

In the PCDC:

- The Download section has the firmware for your controller.
- The Compare section has software compatibility information for software applications that are used in a CompactLogix 5380 and Compact GuardLogix 5380 control system.

Determine Required Controller Firmware

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

In Logix 5000™ control systems, the controller firmware and the Logix Designer application must be of the same major revision level. For example, if the controller firmware revision is 31.xxx, you must use the Logix Designer application, version 31.

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

Obtain Controller Firmware

You can obtain controller firmware in these ways:

- Firmware is packaged as part of the Studio 5000 Logix Designer environment 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 may be released during a product's life. 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.

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

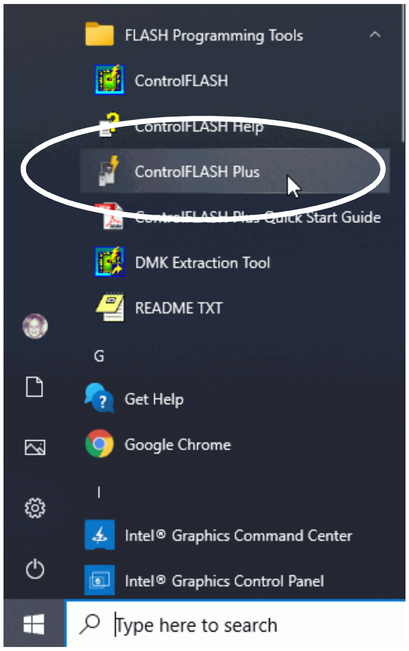
Use ControlFLASH Plus Software to Update Firmware

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

To update your controller firmware with ControlFLASH Plus software, complete the following steps.

If your application network cannot access the PCDC during operation, make sure that you download controller firmware revision to which you want to update the controller before beginning these steps.

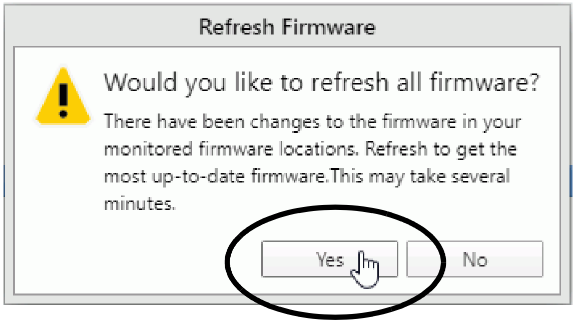
1. Verify that the network connection is made.
2. From the Windows Start Menu, click FLASH Programming Tools > ControlFLASH Plus.



When the software starts, it automatically browses the network to which the workstation and the controllers are connected.

If the devices on the network have changed since the last time you connected, the Refresh Firmware dialog box appears and asks if you want to refresh all firmware.

3. Click Next.

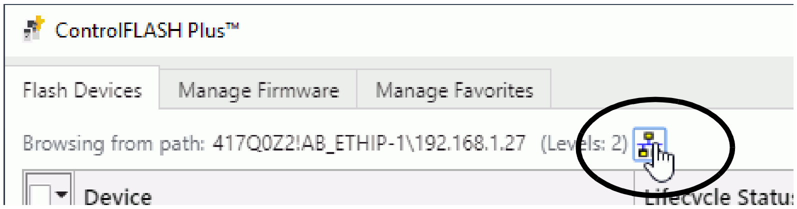


Refresh Firmware

Would you like to refresh all firmware?

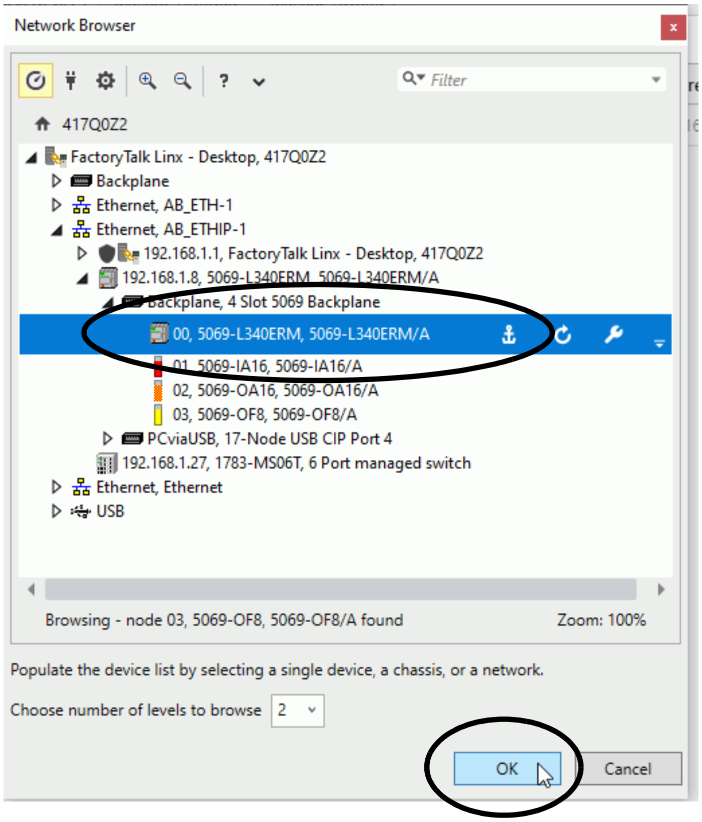
There have been changes to the firmware in your monitored firmware locations. Refresh to get the most up-to-date firmware.This may take several minutes.

4. If the controller appears on the Flash Device tab in the ControlFLASH Plus dialog box, click the controller and move to step 7.
5. If the controller does not appear on the Flash Devices tab in the ControlFLASH Plus dialog box, click the browse button.



Browsing from path: 417Q0Z2!AB_ETHIP-1\192.168.1.27 (Levels: 2)

6. On the Network Browser dialog box, complete the following steps.
   a. Drill down to the controller.
   b. Select the controller.
   c. Click OK.



- FactoryTalk Linx - Desktop, 417Q0Z2
  - Backplane
  - Ethernet, AB_ETH-1
  - Ethernet, AB_ETHIP-1
    - 192.168.1.1, FactoryTalk Linx - Desktop, 417Q0Z2
    - 192.168.1.8, 5069-L340ERM, 5069-L340ERM/A
      - Backplane, 4 Slot 5069 Backplane
        - 00, 5069-L340ERM, 5069-L340ERM/A
        - 01, 5069-IA16, 5069-IA16/A
        - 02, 5069-OA16, 5069-OA16/A
        - 03, 5069-OF8, 5069-OF8/A
      - PCviaUSB, 17-Node USB CIP Port 4
    - 192.168.1.27, 1783-MS06T, 6 Port managed switch
  - Ethernet, Ethernet
  - USB

Browsing - node 03, 5069-OF8, 5069-OF8/A found Zoom: 100%

Populate the device list by selecting a single device, a chassis, or a network.

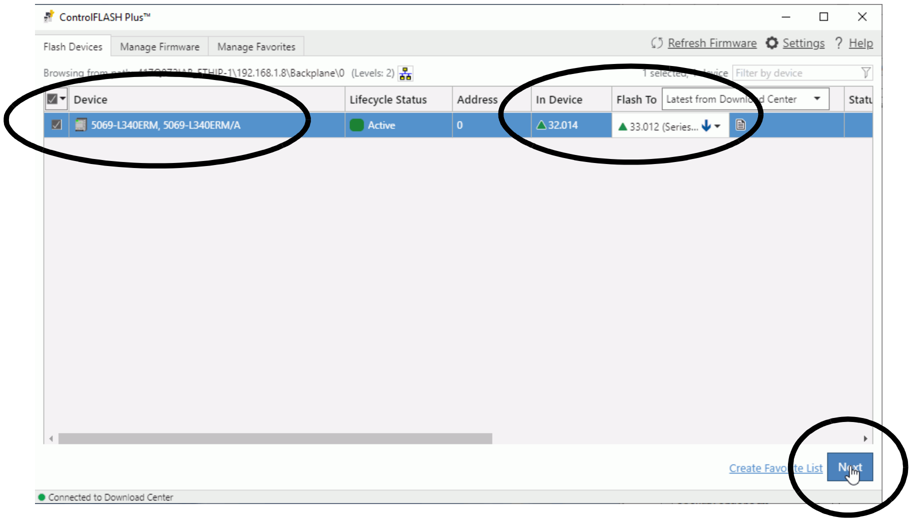
Choose number of levels to browse 2

7. On the Flash Devices tab, complete the following steps.
   a. To select the controller, click the check box to the left of the controller Device Name.
   b. Confirm the current controller firmware revision and the revision to which you want to upgrade.

      The Flash To column gives you the option to the latest revision available at the PCDC, as shown in the example. You must have access to the PCDC to use this option, however.

      Otherwise, ControlFLASH Plus flashes to the latest revision on the computer.
   c. Click Next.

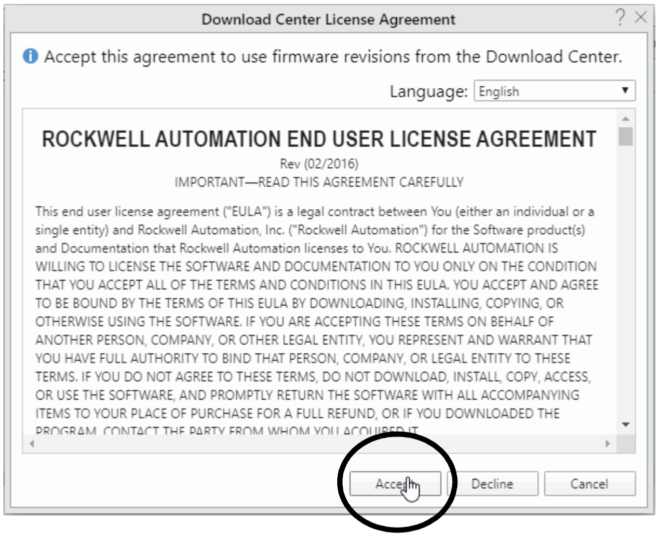
      If you are not logged into the Rockwell Automation Technical Support site, you are prompted to do so.



☑ Device	Lifecycle Status	Address	In Device	Flash To Latest from Download Center	Statu
☑ 5069-L340ERM, 5069-L340ERM/A	Active	0	32.014	33.012 (Series...	

8. If the Download Center License Agreement dialog box appears, click Accept.

   This dialog box only appears if you choose to flash to the latest revision at the PCDC.


Download Center License Agreement

Accept this agreement to use firmware revisions from the Download Center.

Language: English

ROCKWELL AUTOMATION END USER LICENSE AGREEMENT

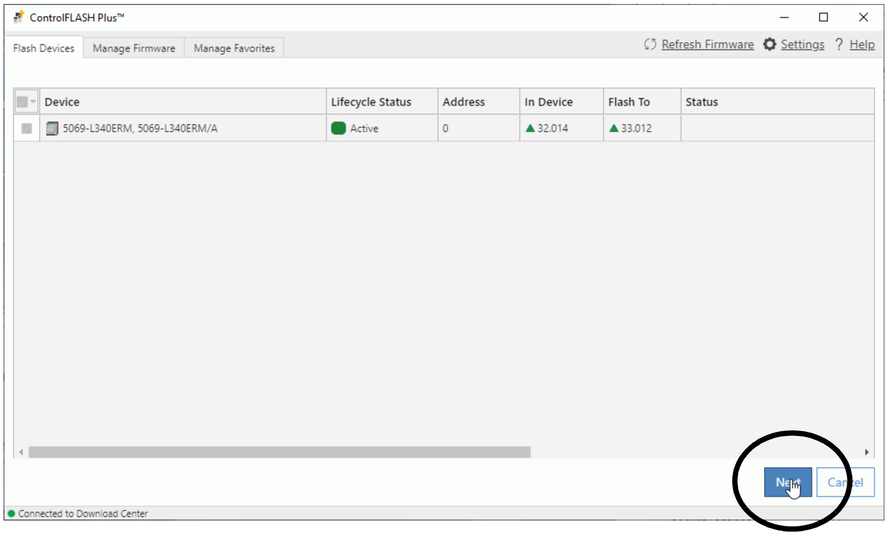
Rev (02/2016)

IMPORTANT—READ THIS AGREEMENT CAREFULLY

This end user license agreement ("EULA") is a legal contract between You (either an individual or a single entity) and Rockwell Automation, Inc. ("Rockwell Automation") for the Software product(s) and Documentation that Rockwell Automation licenses to You. ROCKWELL AUTOMATION IS WILLING TO LICENSE THE SOFTWARE AND DOCUMENTATION TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS IN THIS EULA. YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY DOWNLOADING, INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON, COMPANY, OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE SOFTWARE, AND PROMPTLY RETURN THE SOFTWARE WITH ALL ACCOMPANYING ITEMS TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, OR IF YOU DOWNLOADED THE PROGRAM, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT

The firmware installation file is downloaded to your workstation.

9. Click Next.



ControlFLASH Plus™

Flash Devices | Manage Firmware | Manage Favorites

Refresh Firmware Settings ? Help

☐	Device	Lifecycle Status	Address	In Device	Flash To	Status
☐	5069-L340ERM, 5069-L340ERM/A	🟩 Active	0	▲ 32.014	▲ 33.012	

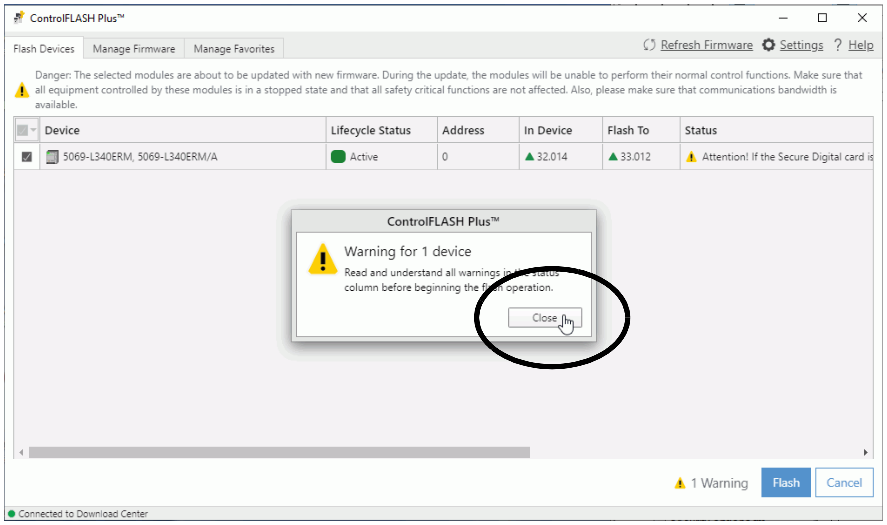
Next Cancel

● Connected to Download Center

You can receive an alert to read and understand all warnings before the flash operation begins.

10. Click Close and read the warnings.

The warning is describes in the Status column.



ControlFLASH Plus™

Flash Devices | Manage Firmware | Manage Favorites

Refresh Firmware Settings ? Help

Danger: The selected modules are about to be updated with new firmware. During the update, the modules will be unable to perform their normal control functions. Make sure that all equipment controlled by these modules is in a stopped state and that all safety critical functions are not affected. Also, please make sure that communications bandwidth is available.

☐	Device	Lifecycle Status	Address	In Device	Flash To	Status
☑	5069-L340ERM, 5069-L340ERM/A	🟩 Active	0	▲ 32.014	▲ 33.012	⚠ Attention! If the Secure Digital card is

ControlFLASH Plus™

Warning for 1 device

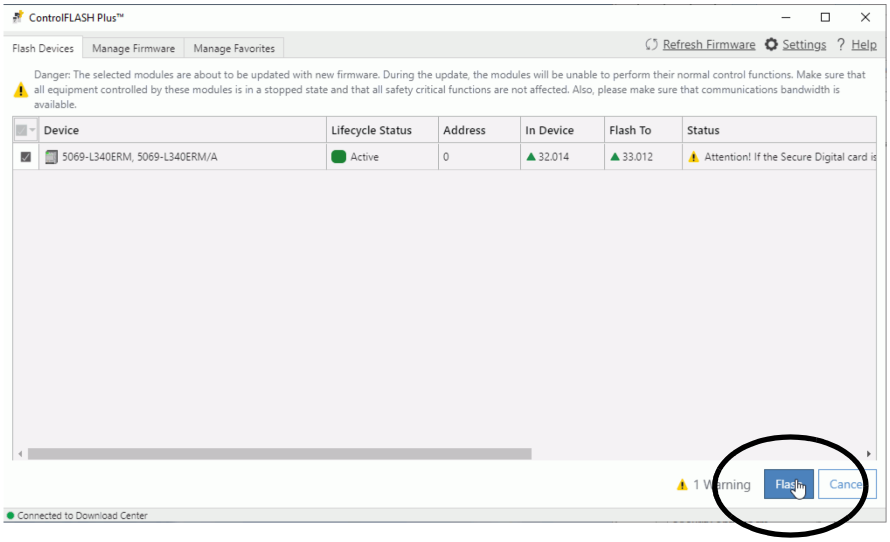
Read and understand all warnings in the status column before beginning the flash operation.

Close

⚠ 1 Warning Flash Cancel

● Connected to Download Center

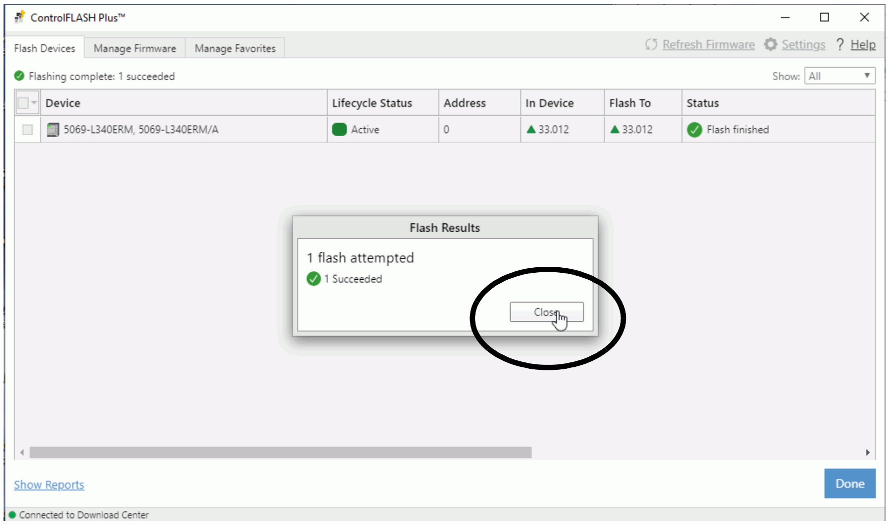
11. Click Flash.



Danger: The selected modules are about to be updated with new firmware. During the update, the modules will be unable to perform their normal control functions. Make sure that all equipment controlled by these modules is in a stopped state and that all safety critical functions are not affected. Also, please make sure that communications bandwidth is available.

☑	Device	Lifecycle Status	Address	In Device	Flash To	Status
☑	5069-L340ERM, 5069-L340ERM/A	Active	0	▲32.014	▲33.012	⚠ Attention! If the Secure Digital card is

12. When ControlFLASH Plus indicates that the update was successful, click Close.



Flashing complete: 1 succeeded

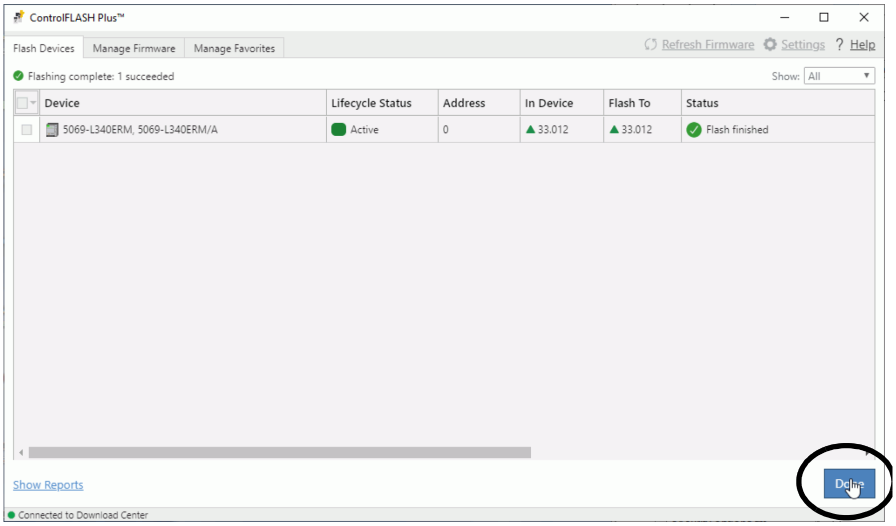
□	Device	Lifecycle Status	Address	In Device	Flash To	Status
□	5069-L340ERM, 5069-L340ERM/A	Active	0	▲33.012	▲33.012	✓ Flash finished

Flash Results

1 flash attempted

✓ 1 Succeeded

13. Click Done.



Flashing complete: 1 succeeded

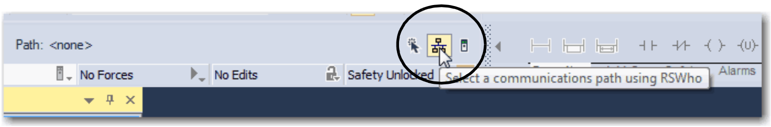
□	Device	Lifecycle Status	Address	In Device	Flash To	Status
□	5069-L340ERM, 5069-L340ERM/A	Active	0	▲33.012	▲33.012	✓ Flash finished

Use AutoFlash to Update Firmware

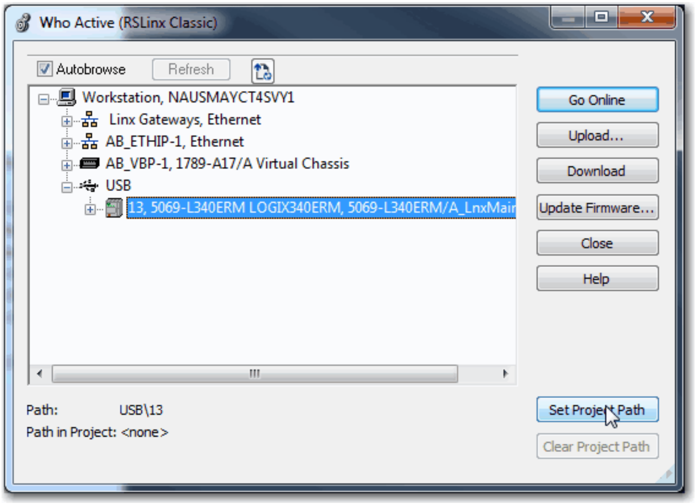
To update the controller firmware with the AutoFlash feature, complete these steps.

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

1. Verify that the network connection is made and the network driver has been configured in Linx-based communication software.
2. Start the Logix Designer application, and create a project.
3. In the project, click RSWho.



4. Expand the communication path and select the controller.


Who Active (RSLinx Classic)

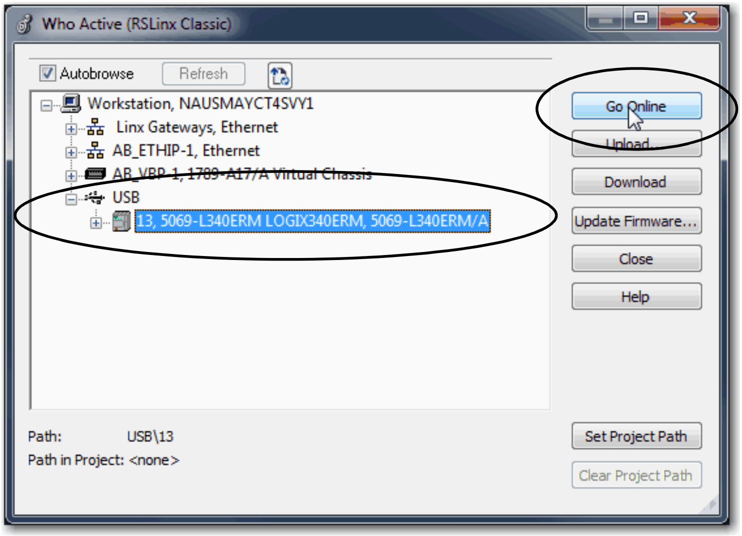
☑ Autobrowse

- Workstation, NAUSMAYCT4SVY1
  - Linx Gateways, Ethernet
  - AB_ETHIP-1, Ethernet
  - AB_VBP-1, 1789-A17/A Virtual Chassis
  - USB
    - 13, 5069-L340ERM LOGIX340ERM, 5069-L340ERM/A_LnxMair

Path: USB\13

Path in Project: <none>

5. Select the controller and click Go Online.


Who Active (RSLinx Classic)

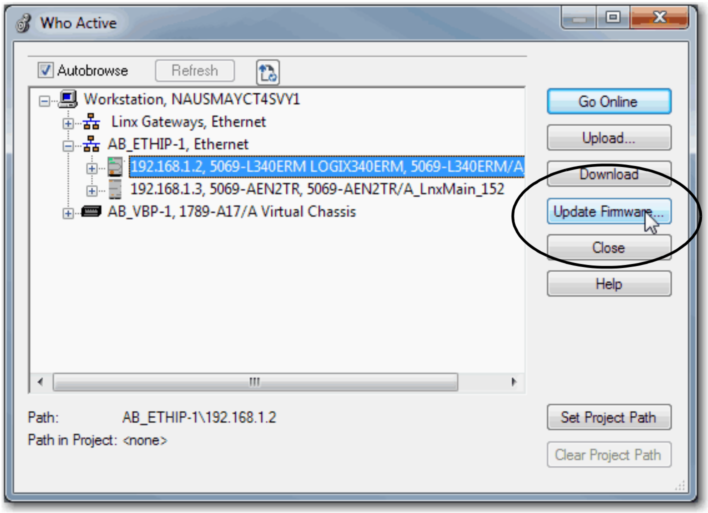
☑ Autobrowse

- Workstation, NAUSMAYCT4SVY1
  - Linx Gateways, Ethernet
  - AB_ETHIP-1, Ethernet
  - AB_VBP-1, 1789-A17/A Virtual Chassis
  - USB
    - 13, 5069-L340ERM LOGIX340ERM, 5069-L340ERM/A

Path: USB\13

Path in Project: <none>

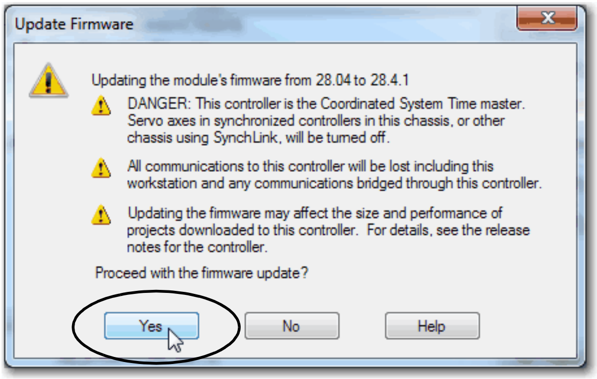
6. On the Who Active dialog box, select the controller under the communication driver you want to use, and click Update Firmware.



Workstation, NAUSMAYCT4SVY1
Linx Gateways, Ethernet
AB_ETHIP-1, Ethernet
192.168.1.2, 5069-L340ERM LOGIX340ERM, 5069-L340ERM/A
192.168.1.3, 5069-AEN2TR, 5069-AEN2TR/A_LnxMain_152
AB_VBP-1, 1789-A17/A Virtual Chassis

Path: AB_ETHIP-1\192.168.1.2
Path in Project: <none>

7. On the Choose Firmware Revision dialog, browse to the location of the firmware files (C:\Program Files (x86)\ControlFlash).
8. Select the firmware revision, and click Update.
9. On the Confirmation dialog, click Yes.



Updating the module's firmware from 28.04 to 28.4.1

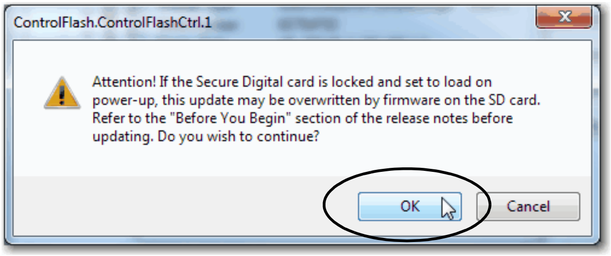
DANGER: This controller is the Coordinated System Time master. Servo axes in synchronized controllers in this chassis, or other chassis using SynchLink, will be turned off.

All communications to this controller will be lost including this workstation and any communications bridged through this controller.

Updating the firmware may affect the size and performance of projects downloaded to this controller. For details, see the release notes for the controller.

Proceed with the firmware update?

10. On the ControlFLASH Attention dialog, click OK.



Attention! If the Secure Digital card is locked and set to load on power-up, this update may be overwritten by firmware on the SD card. Refer to the "Before You Begin" section of the release notes before updating. Do you wish to continue?

A progress dialog box indicates the progress of the firmware update. The controllers indicate progress in updates and blocks.

IMPORTANT	Let the firmware update complete before you cycle power or otherwise interrupt the update. If the ControlFLASH update of the controller is interrupted, the controllers revert to boot firmware, that is, revision 1.*xxx*.

When the update is complete, the Update Status dialog box indicates that the update is complete.

11. Click OK on the Who Active dialog box.

Controllers with Firmware Earlier than Revision 31

Applies to these controllers:
CompactLogix 5380

For controllers with firmware revisions earlier than revision 31, you must be aware of the following before you set the IP address and update the controller firmware:

- Controller state before you make changes
- Firmware revision to which you are updating the controller
- Order in which you set the IP address and update the firmware revision

Controller State Before Making Changes	Description	Firmware Revision of Update/Change	Task Completion Order	Result of Completing Tasks in Order Indicated
Out-of-box	• No IP address set • Unique MAC addresss are used for port A1 and port A2, respectively • Each port on the controller is DHCP-enabled • Firmware revision 1.xxx	Revision 29.011 or later	1. Change the EtherNet/IP mode from Dual-IP mode to Linear/ DLR mode. 2. Set IP address on port A1/A2. 3. Install controller firmware.	• The controller EtherNet/IP mode is automatically set to Dual-IP mode. • The port A1/A2 IP address, network mask, default gateway settings are applied to port A2. • Other port A1/A2 settings, for example, DNS servers and Domain Name, are lost. • The port A1/A2 MAC address is applied to port A1, and a separate MAC address is applied to Port A2. • You must set the IP address configuration
			1. Install controller firmware. 2. Set IP addresses on port A1 and port A2.	• The controller EtherNet/IP mode remains set to Dual-IP mode after the firmware is installed. • The controller EtherNet/IP mode is set to Dual-IP mode when it is in the out-of-box state. • A unique MAC address is assigned to each controller port. • You must set the IP address and related parameters for port A1 (enterprise port) and port A2 (device-level port).
	• No IP address is set • One MAC address is used for port A1/A2 • Port A1/A2 is DHCP-enabled • Firmware revision 1.xxx	Revision 28.xxx **IMPORTANT**: Only the 5069-L320ER and 5069-L340ERM controllers support revision 28.xxx.	1. Set IP address on port A1/A2. 2. Install controller firmware.	• The controller EtherNet/IP mode is automatically set to Linear/DLR mode. • The IP address settings on port A1/A2 remain the same.
			1. Install controller firmware. 2. Set IP address on port A1/A2.	
Operating	• IP address set on port A1/ A2 • Firmware revision 28.xxx is installed	Revision 29.011 or later	Update controller firmware	• EtherNet/IP mode changes to Dual-IP mode. • The port A1/A2 IP address, network mask, default gateway settings are applied to port A2. • Other port A1/A2 settings, for example, DNS servers and Domain Name, are lost. • The port A1/A2 MAC address is applied to port A1. A separate MAC address is applied to Port A2. • The I/O Configuration section in the Logix Designer application project is automatically assigned to port A1. • You can change the I/O configuration in the Logix Designer application project to assign it to port A2. • If necessary, you can change to DLR/Linear mode after the firmware revision update.
	• Controller operates in Linear/DLR mode • IP address set on port A1/ A2 • Firmware revision 29.011 or later is installed	Downgrade to revision 28.xxx **IMPORTANT**: You can perform this download only on the 5069-L320ER and 5069-L340ERM controllers.	Downgrade controller firmware	• EtherNet/IP mode remains in Linear/DLR mode • IP address settings remain the same
	• Controller operates in Dual-IP mode • IP addresses are set on port A1 and port A2 • Firmware revision 29.011 or later is installed		Downgrade controller firmware	• EtherNet/IP mode automatically changes from Dual-IP mode to Linear/DLR mode • After the change is made, the port A2 Internet Protocol configuration is applied to the A1/A2 port.

Notes:

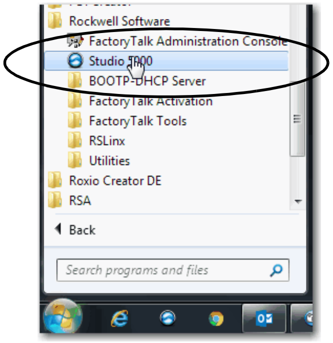
Start to Use the Controller

Create a Logix Designer Application Project

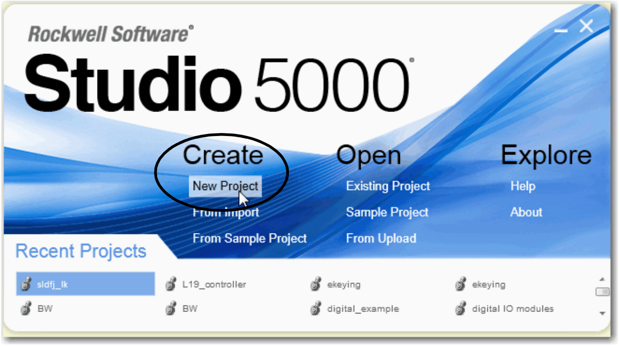
Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Out-of-the-box, the controller does not contain a Studio 5000 Logix Designer® application project. To create a Logix Designer application project, complete these steps.

1. Start the application. The Logix Designer application is part of the Studio 5000® environment.

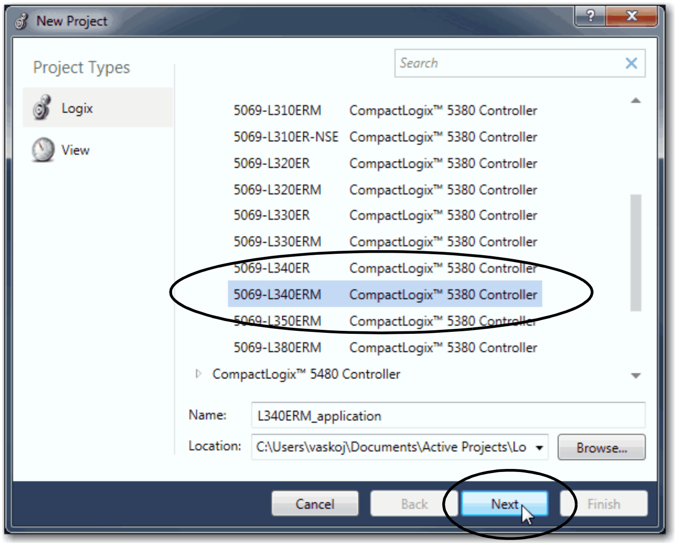


2. Click New Project.



3. On the New Project dialog box, complete these steps:
   a. Select the controller.
   b. Name the project.
   c. Browse to the location where the project file is created.

d. Click Next.



New Project

Project Types

- Logix
- View

Search

5069-L310ERM	CompactLogix™ 5380 Controller
5069-L310ER-NSE	CompactLogix™ 5380 Controller
5069-L320ER	CompactLogix™ 5380 Controller
5069-L320ERM	CompactLogix™ 5380 Controller
5069-L330ER	CompactLogix™ 5380 Controller
5069-L330ERM	CompactLogix™ 5380 Controller
5069-L340ER	CompactLogix™ 5380 Controller
5069-L340ERM	CompactLogix™ 5380 Controller
5069-L350ERM	CompactLogix™ 5380 Controller
5069-L380ERM	CompactLogix™ 5380 Controller

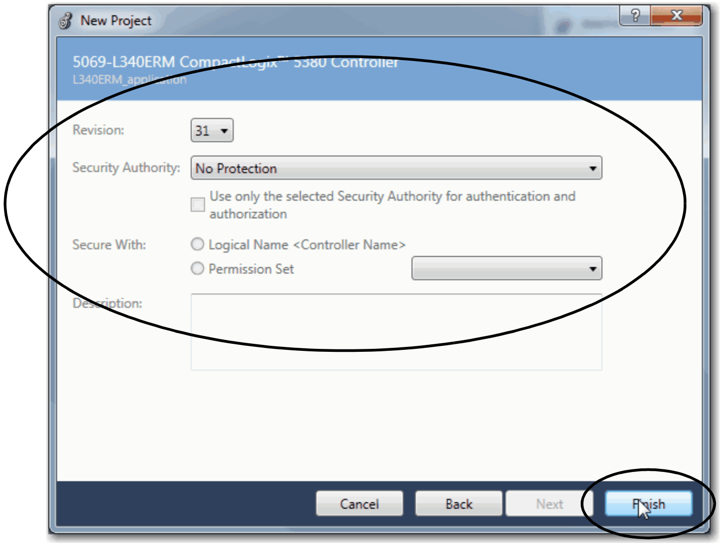
CompactLogix™ 5480 Controller

Name: L340ERM_application

Location: C:\Users\vaskoj\Documents\Active Projects\Lo

4. Select the following:
   - Revision
   - Security Authority (optional)
   - Secure With (only available if Security Authority is used)

   For information on security, refer to the Logix 5000™ Controllers Security Programming Manual, publication 1756-PM016.



New Project

5069-L340ERM CompactLogix™ 5380 Controller

L340ERM_application

Revision: 31

Security Authority: No Protection

☐ Use only the selected Security Authority for authentication and authorization

Secure With: ○ Logical Name <Controller Name>

○ Permission Set

Description:

5. Click Finish.

Additional Configuration for a Compact GuardLogix Controller

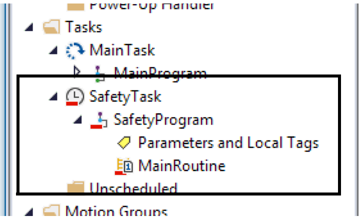
Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Compact GuardLogix 5380 controllers require additional configuration after you create the project. These topics describe how to configure the additional parameters.

Topic	Page
Assign the Safety Network Number (SNN)	67
Go Online with the Controller	72

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

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



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 Compact GuardLogix 5380 controllers have up to three safety network numbers: a separate SNN for each Ethernet port, and one SNN for the backplane.
- If a bridge or adapter device is in the I/O tree and a child CIP Safety device is added, the subnet that is created by the bridge or adapter is assigned an SNN.

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

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

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

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

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

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

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

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

- Automatic Assignment of Time-based SSN
- Manual Assignment of SSN

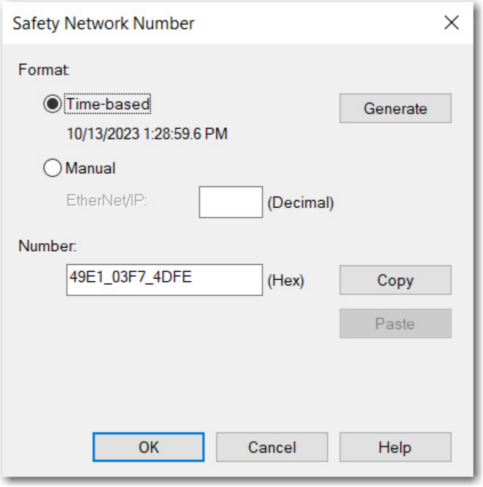
Automatic Assignment of Time-based SSN

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 20 - Time-based Format



Safety Network Number

Format

● Time-based

10/13/2023 1:28:59.6 PM

○ Manual

EtherNet/IP: (Decimal)

Number: 49E1_03F7_4DFE (Hex)

Manual Assignment of SSN

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

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

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

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

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

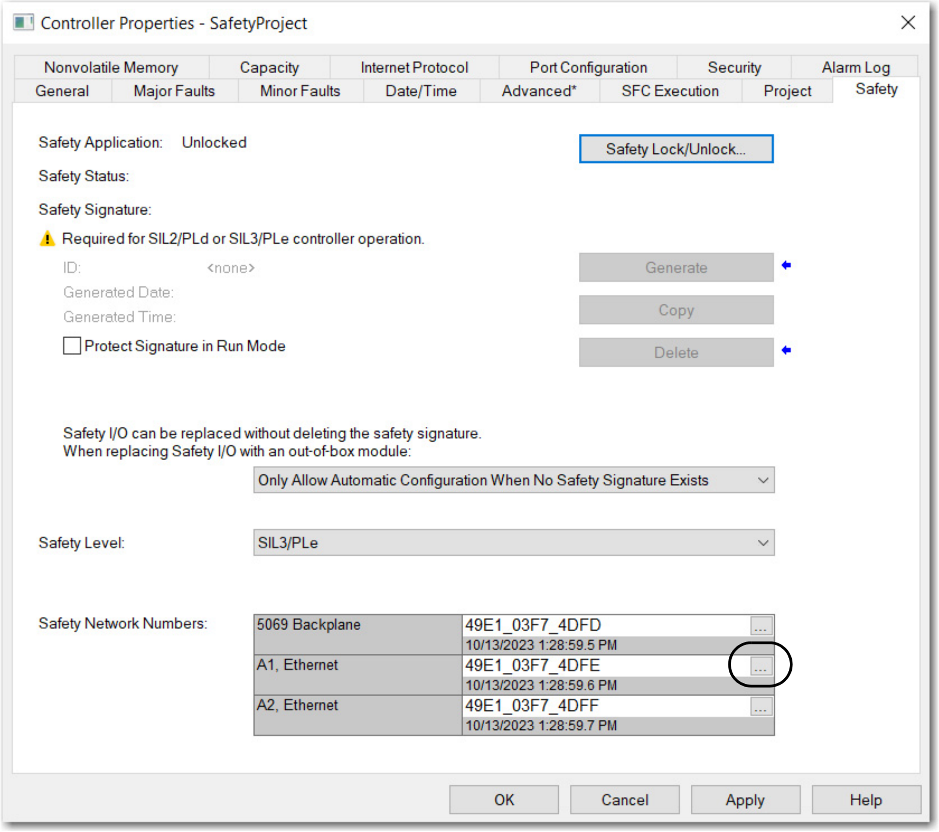
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

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

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

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

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



Safety Application: Unlocked

Safety Status:

Safety Signature:

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

ID: <none>

Generated Date:

Generated Time:

□ Protect Signature in Run Mode

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

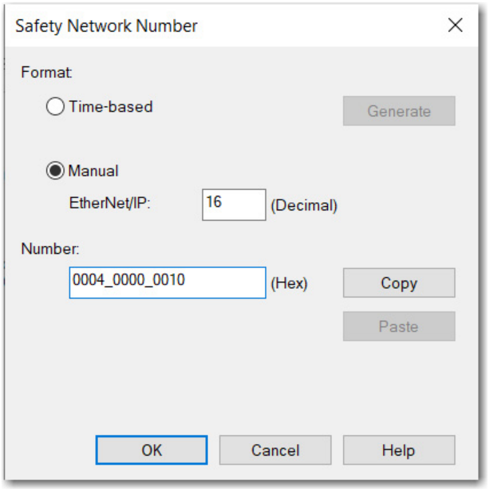
Only Allow Automatic Configuration When No Safety Signature Exists

Safety Level: SIL3/PLe

Safety Network Numbers:

5069 Backplane	49E1_03F7_4DFD 10/13/2023 1:28:59.5 PM
A1, Ethernet	49E1_03F7_4DFE 10/13/2023 1:28:59.6 PM
A2, Ethernet	49E1_03F7_4DFF 10/13/2023 1:28:59.7 PM

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



Safety Network Number

Format:

○ Time-based

● Manual

EtherNet/IP: 16 (Decimal)

Number:

0004_0000_0010 (Hex)

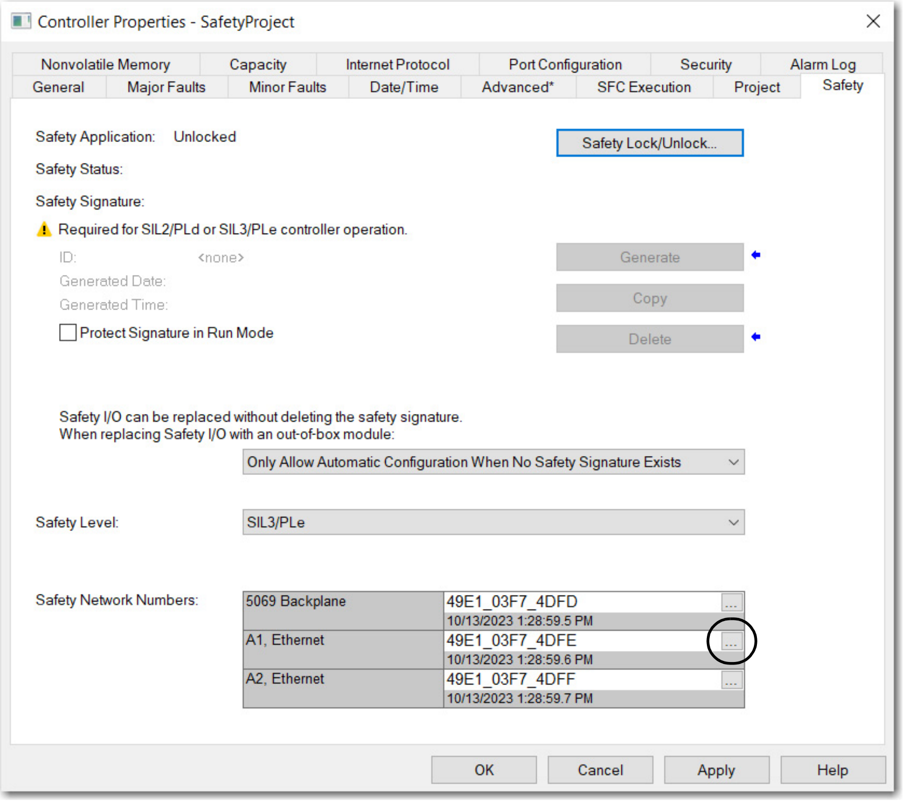
6. Click OK.

Copy and Paste a Safety Controller Safety Network Number

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

Copy a Safety Controller SNN

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



Controller Properties - SafetyProject

Safety Application: Unlocked

Safety Status:

Safety Signature:

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

ID: <none>

Generated Date:

Generated Time:

□ Protect Signature in Run Mode

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

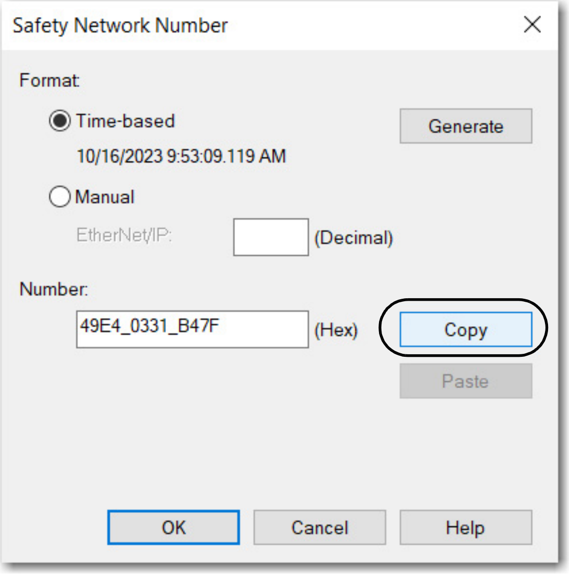
Only Allow Automatic Configuration When No Safety Signature Exists

Safety Level: SIL3/PLe

Safety Network Numbers:

5069 Backplane	49E1_03F7_4DFD 10/13/2023 1:28:59.5 PM
A1, Ethernet	49E1_03F7_4DFE 10/13/2023 1:28:59.6 PM
A2, Ethernet	49E1_03F7_4DFF 10/13/2023 1:28:59.7 PM

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



Safety Network Number

Format:

● Time-based

10/16/2023 9:53:09.119 AM

○ Manual

EtherNet/IP: (Decimal)

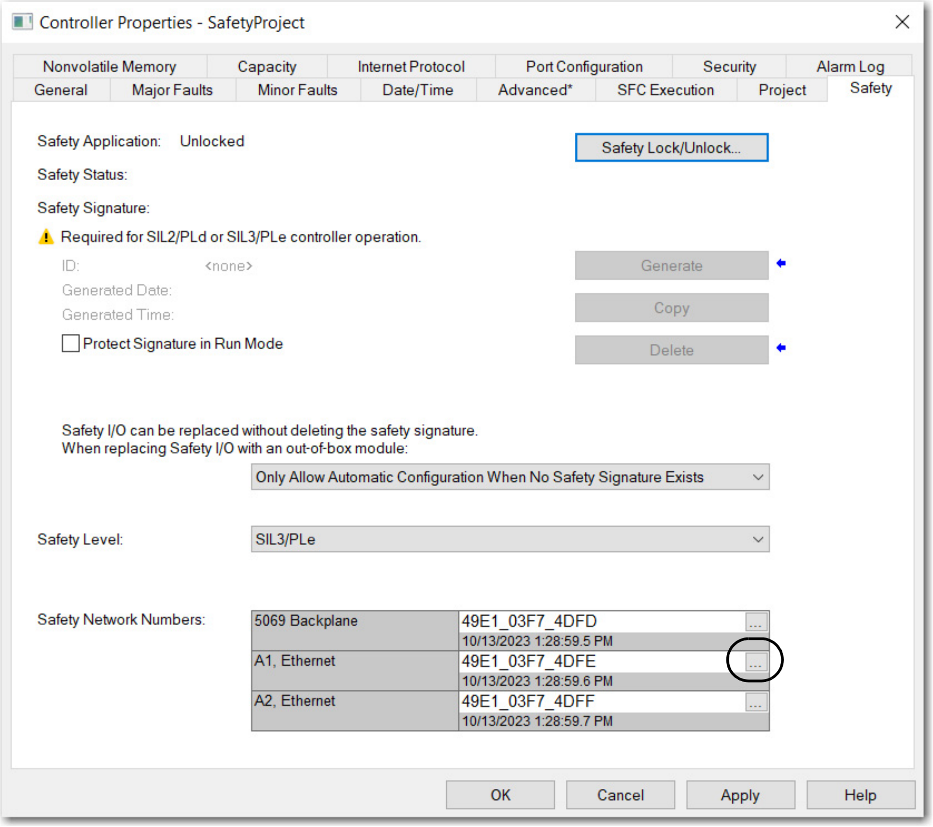
Number:

49E4_0331_B47F (Hex)

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

Paste a Safety Controller SNN

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.



Controller Properties - SafetyProject

Safety Application: Unlocked

Safety Status:

Safety Signature:

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

ID: <none>

Generated Date:

Generated Time:

□ Protect Signature in Run Mode

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

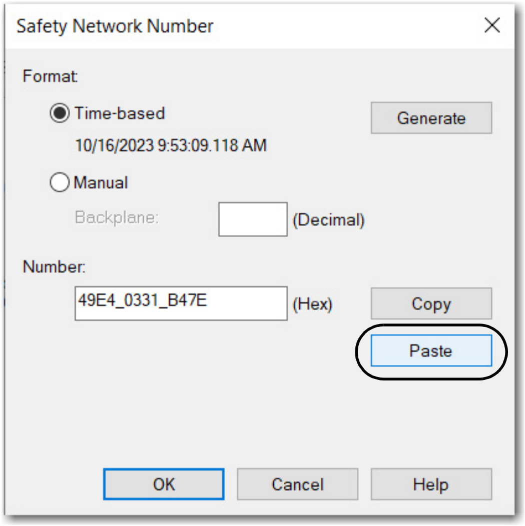
Only Allow Automatic Configuration When No Safety Signature Exists

Safety Level: SIL3/PLe

Safety Network Numbers:

5069 Backplane	49E1_03F7_4DFD 10/13/2023 1:28:59.5 PM
A1, Ethernet	49E1_03F7_4DFE 10/13/2023 1:28:59.6 PM
A2, Ethernet	49E1_03F7_4DFF 10/13/2023 1:28:59.7 PM

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



Safety Network Number

Format:

● Time-based

10/16/2023 9:53:09.118 AM

○ Manual

Backplane: (Decimal)

Number:

49E4_0331_B47E (Hex)

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

Go Online with the Controller

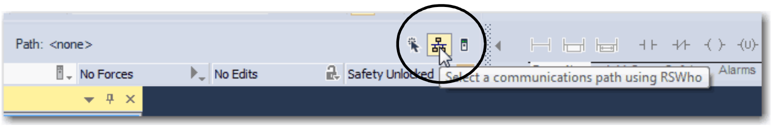
Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

For this section, the USB port was chosen as the communication path. Another path through the embedded Ethernet ports is also possible.

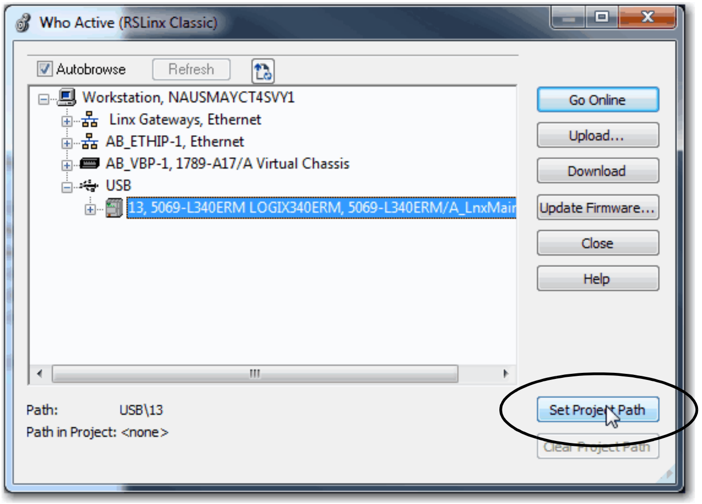
Use RSWho

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



Path: <none>

3. Expand the communication path and select the controller.



Who Active (RSLinx Classic)

☑ Autobrowse

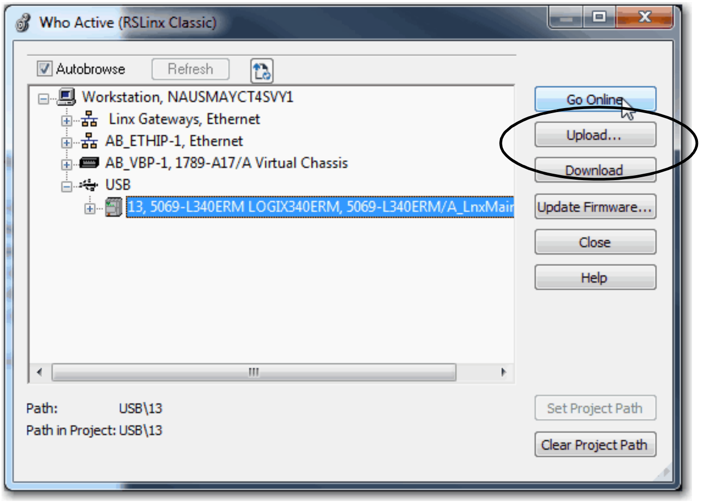
Workstation, NAUSMAYCT4SVY1
- Linx Gateways, Ethernet
- AB_ETHIP-1, Ethernet
- AB_VBP-1, 1789-A17/A Virtual Chassis
- USB
  - 13, 5069-L340ERM LOGIX340ERM, 5069-L340ERM/A_LnxMain

Path: USB\13

Path in Project: <none>

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, you do not have to choose the path each time you go online.
5. After you choose the communication path, click Go Online in the Who Active dialog box.



Workstation, NAUSMAYCT4SVY1
Linx Gateways, Ethernet
AB_ETHIP-1, Ethernet
AB_VBP-1, 1789-A17/A Virtual Chassis
USB
13, 5069-L340ERM LOGIX340ERM, 5069-L340ERM/A_LnxMair

Path: USB\13
Path in Project: USB\13

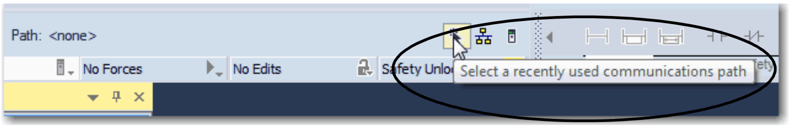
Go Online uses the highlighted node in the Who Active tree, regardless of the setting for Path in Project. For more information on the Who Active dialog box, see the Logix Designer Online Help.

See Additional Considerations for Going Online with a Controller on page 75.

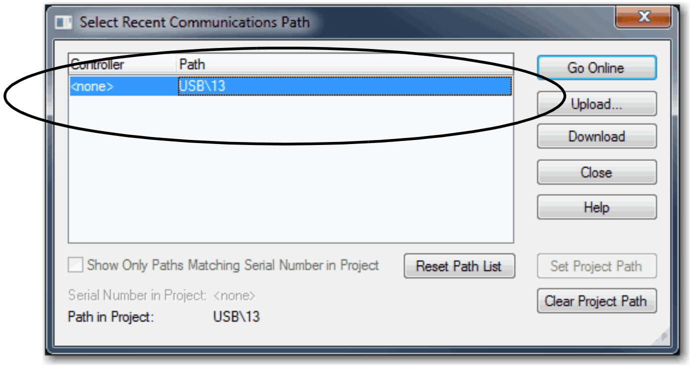
Use a Recent Communications Path

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

1. Click the Recent Communication Path button next to the Path bar.



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

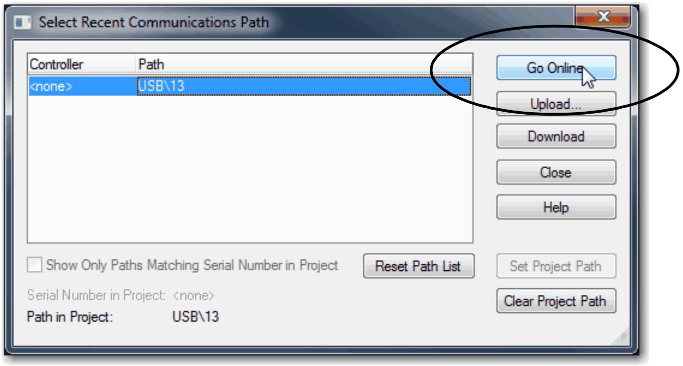


Select Recent Communications Path
Go Online
Upload...
Download
Close
Help
□ Show Only Paths Matching Serial Number in Project
Reset Path List
Set Project Path
Clear Project Path

Controller	Path
<none>	USB\13

Serial Number in Project: <none>
Path in Project: USB\13

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



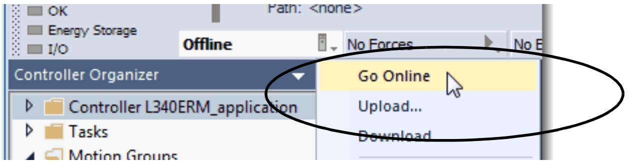
Select Recent Communications Path
Go Online
Upload...
Download
Close
Help
□ Show Only Paths Matching Serial Number in Project
Reset Path List
Set Project Path
Clear Project Path

Controller	Path
<none>	USB\13

Serial Number in Project: <none>
Path in Project: USB\13

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 Controller on page 75.

Additional Considerations for Going Online with a Controller

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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.

For information on uploading a project, downloading a project, and the upload and download dialog boxes, see the Logix Designer Online Help.

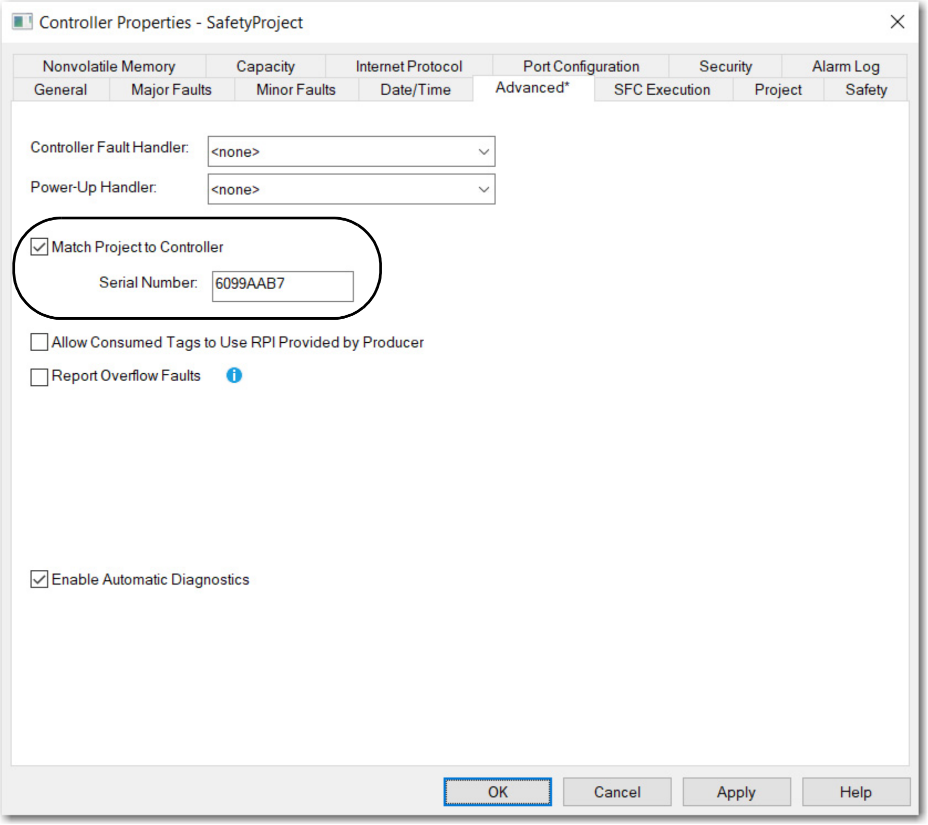
A number of factors affect these processes, including the Match Project to Controller feature and the Firmware Revision Match feature.

For Compact GuardLogix controllers, additional considerations include the safety status and faults, the existence of a safety signature, and the safety-lock/-unlock status of the project and the controller. See Additional Considerations for Going Online with a Compact GuardLogix Controller on page 76.

Match Project to Controller

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

Figure 21 - Match Project to Controller



Controller Fault Handler: <none>

Power-Up Handler: <none>

☑ Match Project to Controller

Serial Number: 6099AAB7

☐ Allow Consumed Tags to Use RPI Provided by Producer

☐ Report Overflow Faults

☑ Enable Automatic Diagnostics

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

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

Additional Considerations for Going Online with a Compact GuardLogix Controller

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can upload program logic and go online regardless of safety status. Safety status and faults only affect the download process.

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

Safety Signature and Safety-locked and -unlocked Status

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

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

Following an upload, the safety signature in the offline project matches the controller 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 safety-lock status, determines if a download can proceed.

Table 5 - 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.	The entire application downloads. Safety lock status matches the status in the offline project. The safety signature does not change.
	Safety signatures do not match.	If the controller had a safety signature, it is automatically deleted, and the entire project is downloaded. Safety lock status matches the status in the offline project.
Controller safety-locked	Safety signatures match.	If the offline project and the controller are safety-locked, all standard project components are downloaded. If the offline project is not safety-locked, but the controller is, the download is blocked and you must first unlock the controller to allow the download to proceed.
	Safety signatures do not match.	You must first safety-unlock the controller to allow the download to proceed. If the controller had a safety signature, it is automatically deleted, and the entire project is downloaded. Safety lock status matches the status in the offline project.

Checks for Going Online with a 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 6 - 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 can 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 firmware are not compatible.	Choose one of the following options: Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection. **IMPORTANT:** The online project is deleted. To preserve the online project, cancel the online process and install a version of the Studio 5000 environment that is compatible with the firmware revision of your controller.
You must upload or download to go online by using the open project.	Choose one of the following options: Upload to update the offline project. Download to update the controller project. Choose File to select another offline project.
Unable to connect in a manner that preserves safety signature. The firmware minor revision on the controller is not compatible with safety signature in offline project.	To preserve the safety signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller. To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to connect to controller. Incompatible safety signature cannot be deleted while project is safety-locked.	Cancel the online process. You must safety-unlock the offline project before attempting to go online.

When the controller and the Logix Designer application are online, the safety-locked status and safety signature of the controller match the controller 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:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

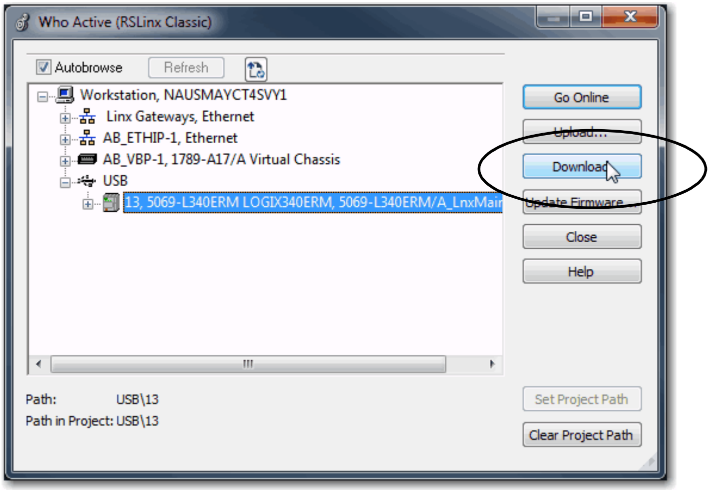
When you download a project to the controller, it copies the project from the Logix Designer application onto the controller. You can download a project in two ways:

- Use Who Active on page 78
- Use the Controller Status Menu on page 78

Use Who Active

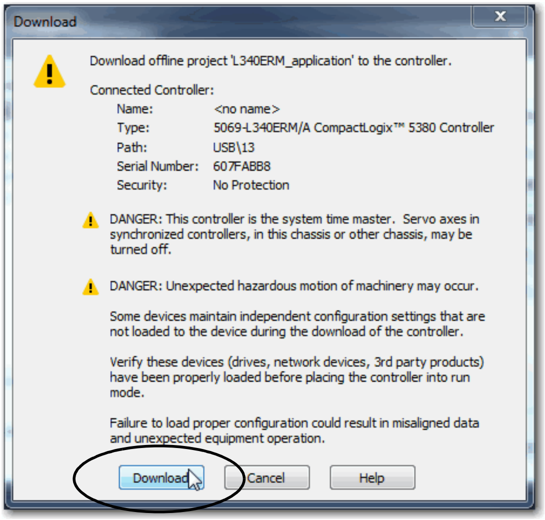
You can use the features of the Who Active dialog box to download to the controller after you have set the communication path. Complete these steps to download to the controller.

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



Path: USB\13
Path in Project: USB\13

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



Download offline project 'L340ERM_application' to the controller.

Connected Controller:

Name: <no name>
Type: 5069-L340ERM/A CompactLogix™ 5380 Controller
Path: USB\13
Serial Number: 607FABB8
Security: No Protection

DANGER: This controller is the system time master. Servo axes in synchronized controllers, in this chassis or other chassis, may be turned off.

DANGER: Unexpected hazardous motion of machinery may occur.

Some devices maintain independent configuration settings that are not loaded to the device during the download of the controller.

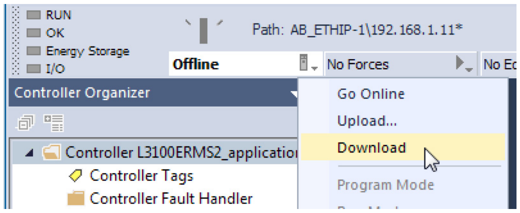
Verify these devices (drives, network devices, 3rd party products) have been properly loaded before placing the controller into run mode.

Failure to load proper configuration could result in misaligned data and unexpected equipment operation.

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 22 - Download Via the Controller Status Menu



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

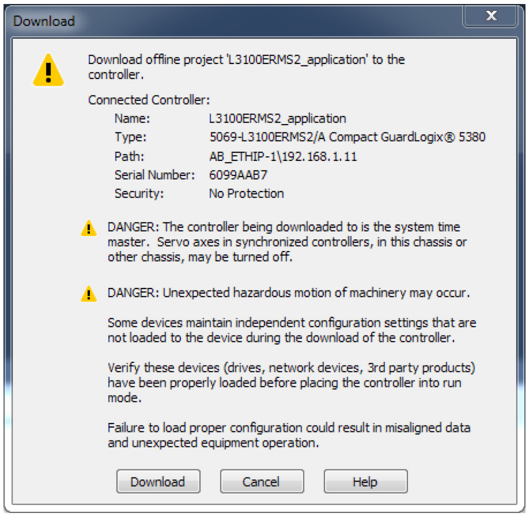
Additional Considerations for Download to a Compact GuardLogix Controller

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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



Download

Download offline project 'L3100ERMS2_application' to the controller.

Connected Controller:
Name: L3100ERMS2_application
Type: 5069-L3100ERMS2/A Compact GuardLogix® 5380
Path: AB_ETHIP-1\192.168.1.11
Serial Number: 6099AAB7
Security: No Protection

DANGER: The controller being downloaded to is the system time master. Servo axes in synchronized controllers, in this chassis or other chassis, may be turned off.

DANGER: Unexpected hazardous motion of machinery may occur.

Some devices maintain independent configuration settings that are not loaded to the device during the download of the controller.

Verify these devices (drives, network devices, 3rd party products) have been properly loaded before placing the controller into run mode.

Failure to load proper configuration could result in misaligned data and unexpected equipment operation.

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 can 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 firmware are not compatible.	Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.
Unable to download to controller. The internal safety partner hardware has failed.	Replace the Compact GuardLogix SIL 3 controller.
Unable to download to the controller. Safety partnership has not been established.	Cancel the download process and attempt a new download to the Compact GuardLogix SIL 3 controller.
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 firmware minor revision is not compatible with safety signature in offline project.	If the firmware minor revision is incompatible, to preserve the safety signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project. To proceed with the download despite the safety signature incompatibility, click Download. The safety signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to download to controller. Controller is locked. Controller and offline project safety signatures do not match.	Choose Unlock. The Safety Unlock for Download dialog box appears. If the Delete Signature checkbox is selected and you choose Unlock, click Yes to confirm the deletion. **IMPORTANT:** The safety system requires revalidation.
Downloading safety signature…	The safety signature is present in the offline project and is downloading.

Following a successful download, the safety-locked status and safety signature of the controller match the project that was downloaded.

Upload from the Controller

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

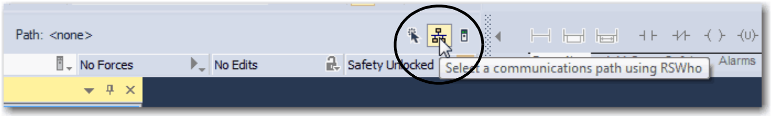
When you upload a project from the controller, it copies the project from the controller to the Logix Designer application. To upload a project, use one of these methods:

- Use Who Active on page 80
- Use the Controller Status Menu on page 81

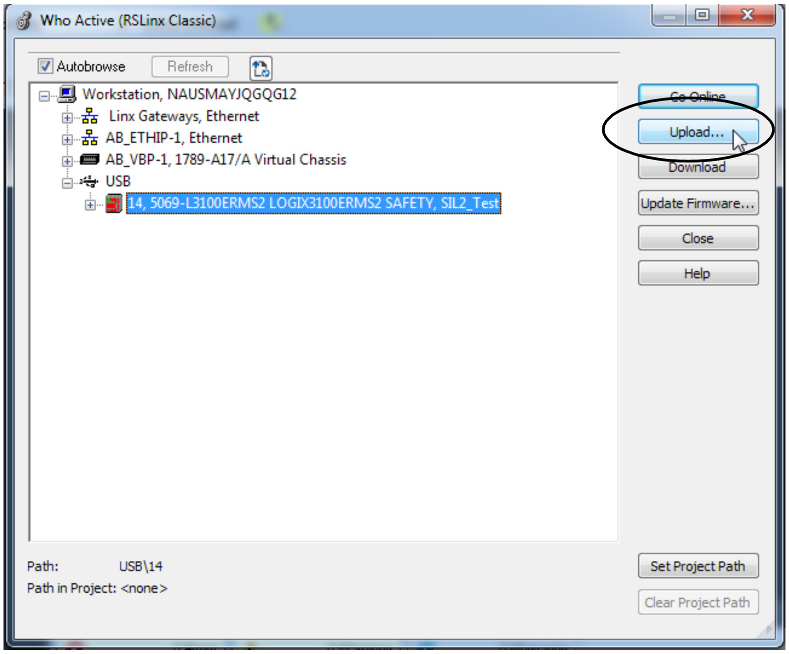
Use Who Active

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. In the Logix Designer application project, click RSWho.

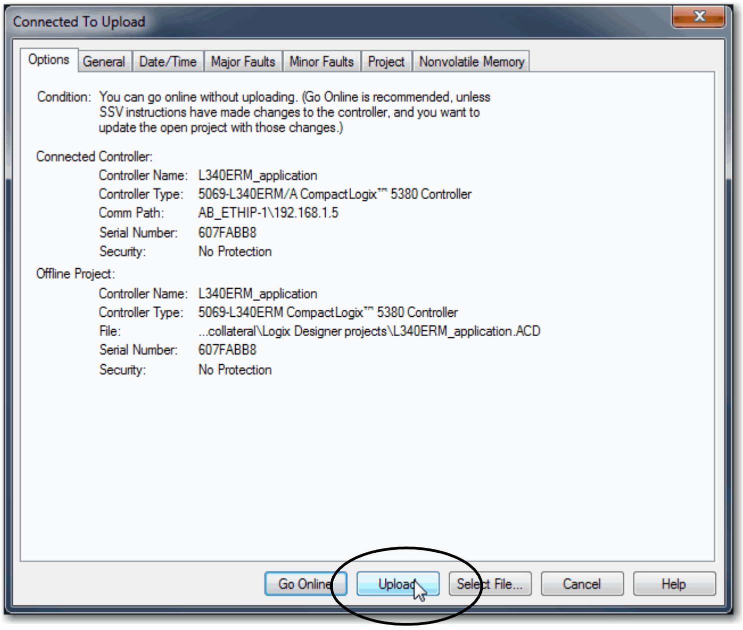


2. Expand the communication path and select the controller.
3. Click Upload on the Who Active dialog box.



Path: USB\14
Path in Project: <none>

4. On the Connected to Upload dialog box, verify that the project is the one you want to upload and click Upload.
5. Click Upload.



Condition: You can go online without uploading. (Go Online is recommended, unless SSV instructions have made changes to the controller, and you want to update the open project with those changes.)

Connected Controller:
Controller Name: L340ERM_application
Controller Type: 5069-L340ERM/A CompactLogix™ 5380 Controller
Comm Path: AB_ETHIP-1\192.168.1.5
Serial Number: 607FABB8
Security: No Protection

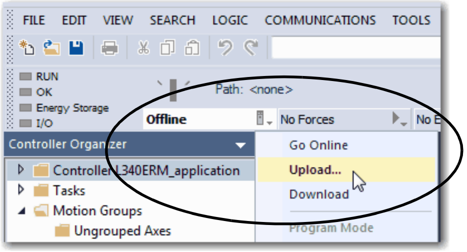
Offline Project:
Controller Name: L340ERM_application
Controller Type: 5069-L340ERM CompactLogix™ 5380 Controller
File: ...collateral\Logix Designer projects\L340ERM_application.ACD
Serial Number: 607FABB8
Security: No Protection

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

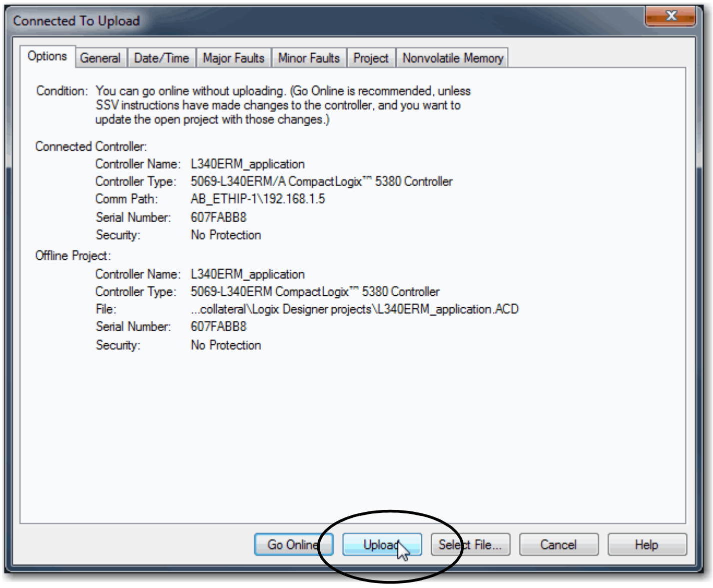
Use the Controller Status Menu

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 pull-down menu, choose Upload.



2. On the Connected to Upload dialog box, verify the project to upload.
3. Click Upload.



Condition: You can go online without uploading. (Go Online is recommended, unless SSV instructions have made changes to the controller, and you want to update the open project with those changes.)

Connected Controller:
Controller Name: L340ERM_application
Controller Type: 5069-L340ERM/A CompactLogix™ 5380 Controller
Comm Path: AB_ETHIP-1\192.168.1.5
Serial Number: 607FABB8
Security: No Protection

Offline Project:
Controller Name: L340ERM_application
Controller Type: 5069-L340ERM CompactLogix™ 5380 Controller
File: ...collateral\Logix Designer projects\L340ERM_application.ACD
Serial Number: 607FABB8
Security: No Protection

Additional Considerations for Upload to a Compact GuardLogix Controller

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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.

Table 7 - Upload Behavior

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

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

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

Choose the Controller Operation Mode

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

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Mode Switch 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.	• 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	• 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.	• 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	• 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.	• 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	• 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).	• 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	• 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.	• 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	• 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 mode switch 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 mode switch alone, it is only available via the Logix Designer application.

Use the Mode Switch to Change the Operation Mode

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

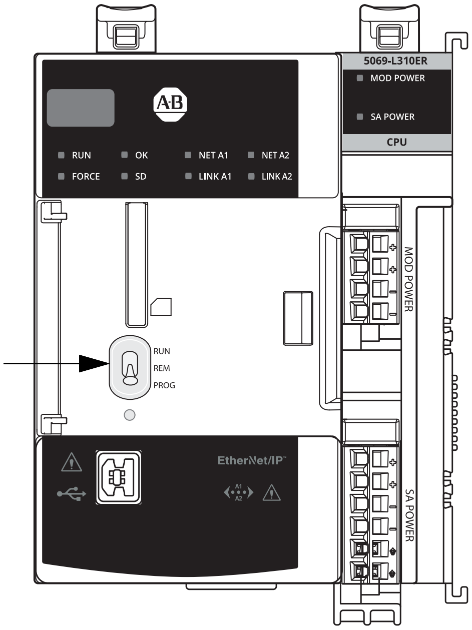
When the mode switch on the controller is set to RUN mode, features like online editing, program downloads, and firmware updates are prohibited. See Choose the Controller Operation Mode on page 83 for a list of prohibited features.

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

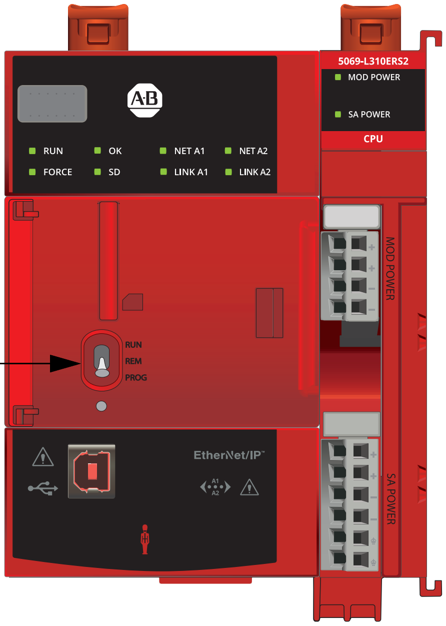
IMPORTANT	During runtime, we recommend that you place the controller mode switch in RUN mode. This can help discourage unauthorized access to the controller or potential tampering with the program of the controller, configuration, or device firmware. Place the mode switch in REM or PROG mode during controller commissioning and maintenance and whenever temporary access is necessary to change the program, configuration, or firmware of the product.

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

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



Mode Switch



Mode Switch on both Compact GuardLogix SIL 2 and SIL 3 controllers.

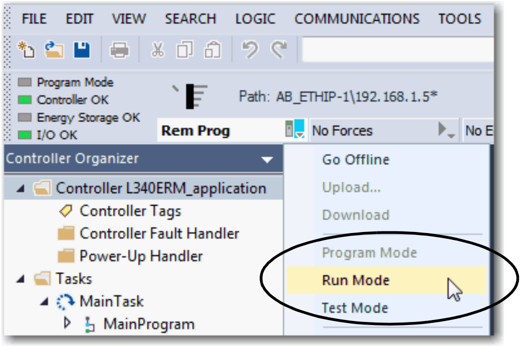
Use the Logix Designer Application to Change the Operation Mode

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

The Controller Status menu in the upper-left corner of the application window lets you specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

1. From the Controller Status pull-down menu, choose the operation mode.



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

Change Controller Configuration

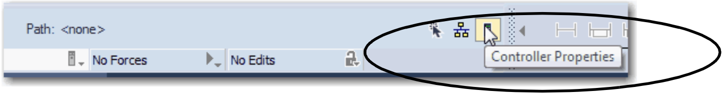
Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

After the project is created, you can change some configuration parameters on the Controller Properties dialog box while the **controller is offline**. Examples of configurable parameter that you can change offline include the following:

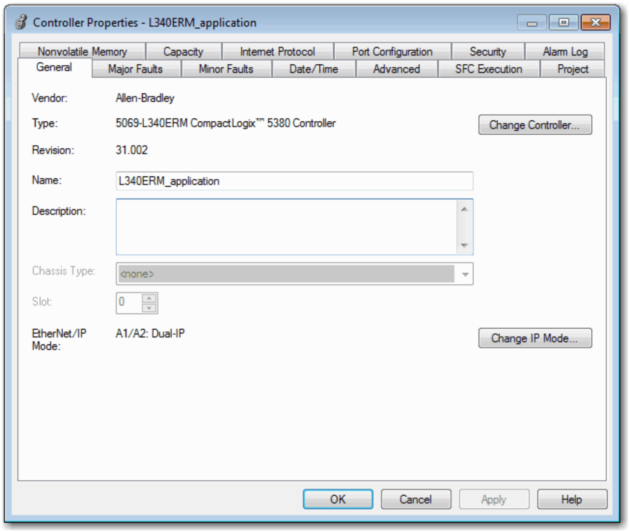
- EtherNet/IP™ Mode on the General tab
- Enable Time Synchronization on the Date/Time tab
- Execution Control on the SFC Execution tab

To change the controller configuration while the project is offline, complete these steps.

1. On the Online toolbar, click the Controller Properties button.



2. On the Controller Properties dialog box, click the General tab.



Vendor: Allen-Bradley

Type: 5069-L340ERM CompactLogix™ 5380 Controller

Revision: 31.002

Name: L340ERM_application

Description:

Chassis Type: <none>

Slot: 0

EtherNet/IP Mode: A1/A2: Dual-IP

Reset Button

You can reset the CompactLogix and Compact GuardLogix controllers 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 Compact 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.

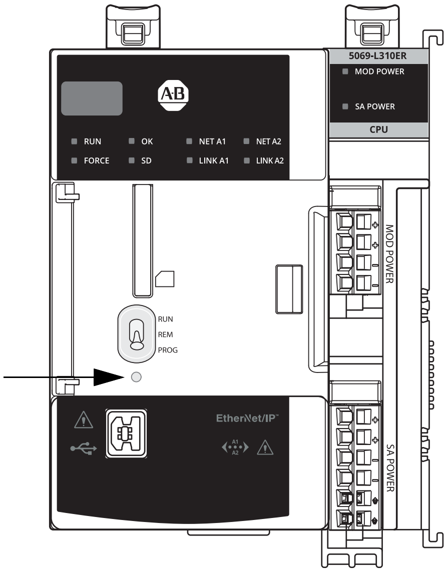
For a Compact GuardLogix SIL 3 controller, the reset button resets both the primary safety controller and the safety partner.

A controller has two stages of reset:

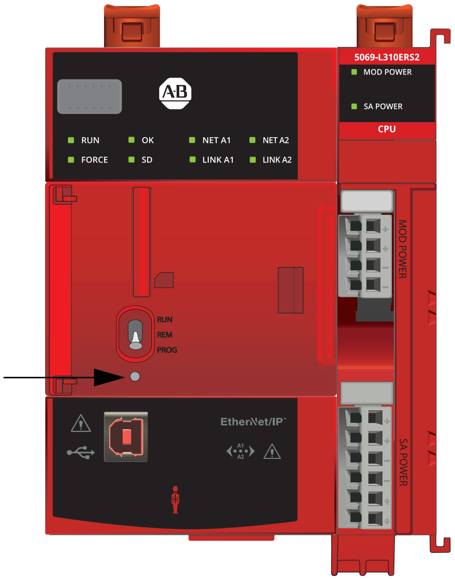
- A Stage 1 reset clears the application program and memory, but retains the IP address, all network settings, and firmware revision. A stage 1 reset occurs only if the controller contains a user application. See Stage 1 Reset on page 87.
- A Stage 2 reset returns the controller to out-of box settings (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.

IMPORTANT Because port enable/disable status is associated with the application program, the 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.



Reset Button



Reset Button on both Compact GuardLogix SIL 2 and SIL 3 controllers.

Stage 1 Reset

IMPORTANT	A stage 1 reset occurs only if the controller contains a user application.

The stage 1 reset completes the following:

- 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 reloads (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. Open the front door on the controller.
3. To press and hold the reset button, use a small tool with a diameter of a paper clip.
4. While holding in the reset button, power up the controller.
5. Continue to hold the reset button while the 4-character display cycles through CLR, 4, 3, 2, 1, Project Cleared.
6. After Project Cleared appears, release the reset button.

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

After a Stage 1 reset is performed, load a 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

IMPORTANT	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 revision.

The stage 2 reset completes the following:

- Returns the module to revision 1.x firmware, that is, the out-of-box firmware revision.
- Clears all user settings, including network and time synchronization settings.

  If the controller uses firmware revision 29.011 or later, the EtherNet/IP mode is reset to Dual-IP mode, that is, the default mode.
- Resets the controller to begin the controller start up process.
- There are no entries in the controller log after a Stage 2 reset, but saved logs on the SD card remain.

To perform a Stage 2 reset, complete these steps. This process assumes that an SD card is installed in the controller.

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

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 Set the IP Address on page 51.
- Update the firmware revision—For more information, see Update Controller Firmware on page 54.
- 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.

Notes:

Use the Secure Digital Card

Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controllers ship with an 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:

- 1784-SD2 card—2 GB card that ships with the controller
- 1784-SD1 card—1 GB card
- 1784-SDHC8—8 GB card
- 1785-SDHC32—32 GB card
- 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 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 without storing them, 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.

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, its content appears 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 content of the SD card.

Figure 23 - Nonvolatile Memory Tab

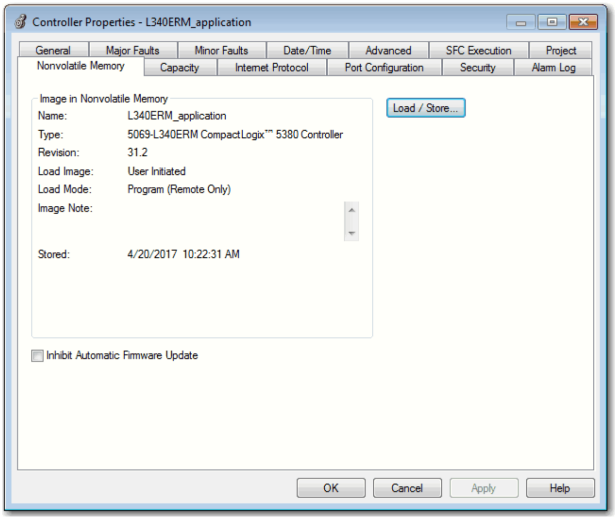


Image in Nonvolatile Memory

Name: L340ERM_application

Type: 5069-L340ERM CompactLogix™ 5380 Controller

Revision: 31.2

Load Image: User Initiated

Load Mode: Program (Remote Only)

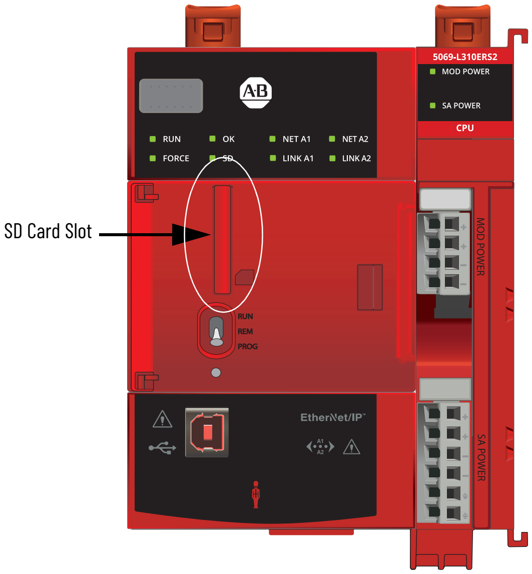
Image Note:

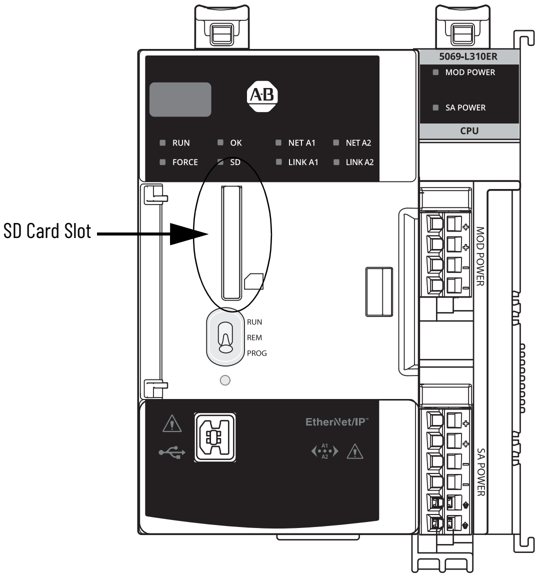
Stored: 4/20/2017 10:22:31 AM

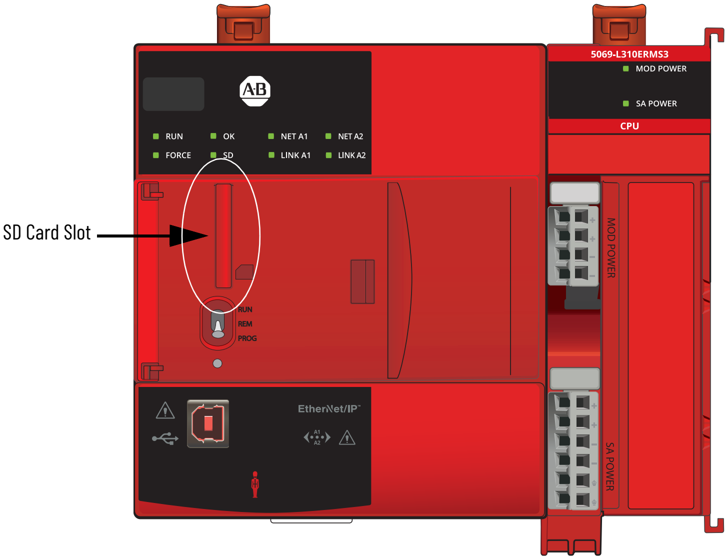
□ Inhibit Automatic Firmware Update

Remember the following:

- An SD card slot is on the front of the controller behind the door.







- If the card is installed and a fault occurs, diagnostic data is automatically written to the card. Diagnostic data helps the investigation and correction of the fault cause.
- The controller detects the presence of an SD card at power-up or if a card is inserted during controller operation.
- The SD card can store all configuration data that is stored in nonvolatile memory, for example, the controller IP address.
- The SD card can store the back-up program.

IMPORTANT	Rockwell Automation recommends that you back up your Studio 5000 Logix Designer® program to an SD card regularly. If a major non-recoverable fault occurs that removes the program from the controller memory, the backup copy on the SD card can be automatically restored to the controller and quickly resume normal controller operation.

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

Considerations for Storing and Loading a Safety Project

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Only Compact GuardLogix 5380 controllers support safety projects. CompactLogix 5380 controllers do not support safety projects.

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

For a Compact GuardLogix 5380 SIL 3 controller, if no application exists in the controller but a valid safety partnership exists, you can save only the firmware of the internal safety partner.

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

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

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

IMPORTANT To help prevent the firmware that is 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

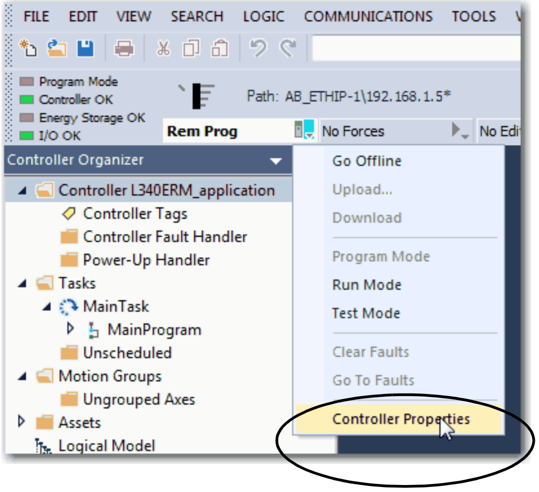
Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

We recommend that you back up your Studio 5000 Logix Designer® application to an SD card regularly.

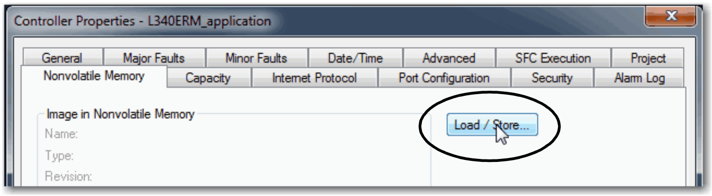
If a major non-recoverable fault occurs that removes the program from the controller memory, the backup copy on the SD card can be automatically restored to the controller to quickly resume normal controller operation.

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

1. Make sure that the controller is online and in Program mode or Remote Program mode.
2. From the Controller Status pull-down menu, click Controller Properties.



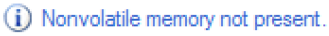
3. On the Nonvolatile Memory tab, click Load/Store.



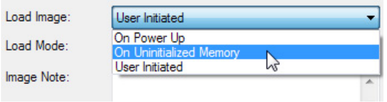
If Load/Store is dimmed (unavailable), verify the following:

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

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


Nonvolatile memory not present.

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


Load Image: User Initiated

The following table describes the Load Image options.

Table 8 - Load Image Options

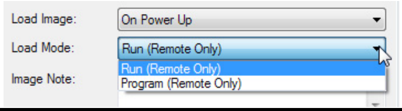
If You Want to Load the Project	Then Select This Load Image Option	Notes	Safety Considerations
Whenever you turn on or cycle power	On Power Up	• During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory. • The controller loads the stored project and firmware at every powerup regardless of the firmware or application project on the controller. • You can always use the Studio 5000 Logix Designer application to load the project.	• For a safety application, On Power Up loads whether or not the controller is safety-locked or there is a safety signature. • If the application is configured to load from the SD card on power up, then the application in the controller is overwritten even if the controller is safety locked.
Whenever there is no project in the controller and you turn on or cycle chassis power	On Uninitialized Memory	• If the project has been cleared from memory, this option loads the project back into the controller on power-up. • The controller updates the firmware on the controller, if necessary. The application project that is stored in nonvolatile memory is also loaded and the controller enters the selected mode, either Program or Run. • You can always use the Logix Designer application to load the project.	• The controller also updates the firmware on the safety partner, if necessary.
Only through the Logix Designer application	User Initiated	• If the controller type and the major and minor revisions of the project in nonvolatile memory match the controller type and major and minor revisions of the controller, you can initiate a load.	• You can initiate a load, regardless of the safety status. • You can load a project to a safety-locked controller only when the safety signature of the project that is stored in nonvolatile memory matches the project on the controller. • If the signatures do not match or the controller is safety-locked without a safety signature, you are prompted to first unlock the controller. • **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 necessary, the application that is stored in nonvolatile memory is loaded so that the safety status becomes Safety Task Operable and the controller enters the Program mode.

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

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

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

5. 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)	 Load Image: On Power Up Load Mode: Run (Remote Only) Run (Remote Only) Program (Remote Only) Image Note:
Run	Run (remote only)	

IMPORTANT **Safety Consideration**

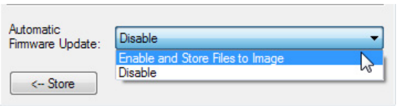
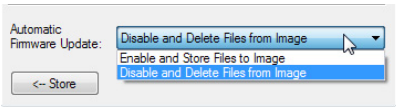
Rockwell Automation recommends that you use Program (Remote Only), when you set the Load Mode for a safety application project.

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

IMPORTANT **Safety Consideration**

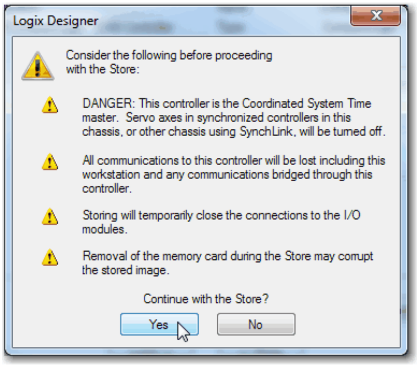
Some Safety I/O devices do not support the Firmware Supervisor feature. For example, Safety I/O devices on DeviceNet® networks and POINT Guard I/O™ modules do not support the Firmware Supervisor feature.

The following 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.	 Automatic Firmware Update: Disable Enable and Store Files to Image Disable <- Store
Enable and Store Files to Image	Enables automatic firmware updates for I/O devices in the configuration tree of the controller. Saves I/O device firmware and controller firmware to the image. Only I/O devices that are configured for Exact Match Keying participate in the Automatic Firmware Update process.[1]	 Automatic Firmware Update: Disable and Delete Files from Image Enable and Store Files to Image Disable and Delete Files from Image <- Store
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.

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



Logix Designer

Consider the following before proceeding with the Store:

DANGER: This controller is the Coordinated System Time master. Servo axes in synchronized controllers in this chassis, or other chassis using SynchLink, will be turned off.

All communications to this controller will be lost including this workstation and any communications bridged through this controller.

Storing will temporarily close the connections to the I/O modules.

Removal of the memory card during the Store may corrupt the stored image.

Continue with the Store?

If you enabled Automatic Firmware Update, a dialog box informs 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:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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 these ways:

- Controller Power-up
- User-initiated Action

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

Controller Power-up

The following table shows what happens at power-up when the SD card in the controller contains an image.

Image Setting	Controller Is in Out-of-box Condition (v1.*xxx* Firmware)	Firmware > 1.*xxx* and Internal Nonvolatile Memory Is Not Valid[1]	Firmware > 1.*xxx* and Internal Nonvolatile Memory Is Valid[1]
User Initiated	Loads Firmware Only[2]	Does Nothing	Does Nothing
On Power Up	Loads both Firmware and Application	• Loads Firmware if there is a revision mismatch • Loads Application	• Loads Firmware if there is a revision mismatch • Loads Application
On Uninitialized Memory	Loads both Firmware and Application[1]	• Loads Firmware if there is a revision mismatch • Loads Application	Does Nothing

[1] "Valid" includes the No Project condition.
[2] Indicates change in behavior from CompactLogix 5370 and older controllers.

User-initiated Action

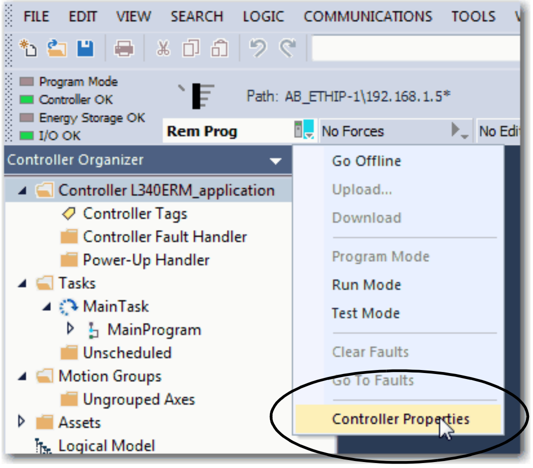
IMPORTANT For an out-of-box controller that uses firmware revision 1.xx, you must manually update the controller to the required firmware revision before you can load a project on the controller.

You must complete the following before you can load 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 SD card, complete these steps.

1. From the Controller Status pull-down menu, click Controller Properties.



2. On the Nonvolatile Memory tab, verify that the project that is listed is the correct one.

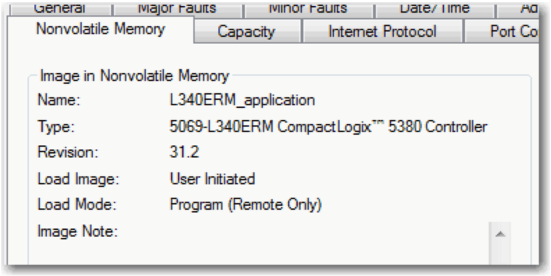
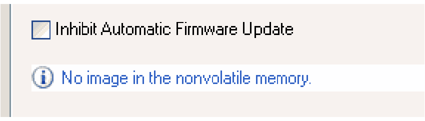


Image in Nonvolatile Memory
Name: L340ERM_application
Type: 5069-L340ERM CompactLogix™ 5380 Controller
Revision: 31.2
Load Image: User Initiated
Load Mode: Program (Remote Only)
Image Note:

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


□ Inhibit Automatic Firmware Update

No image in the nonvolatile memory.

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

3. Click Load/Store.

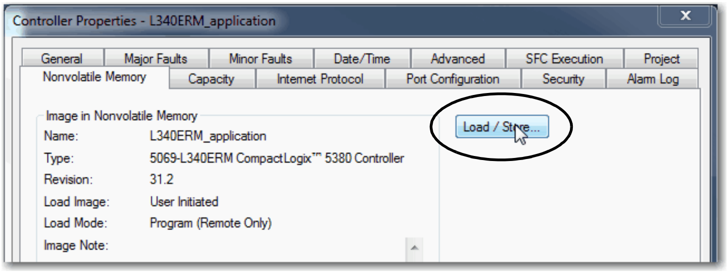


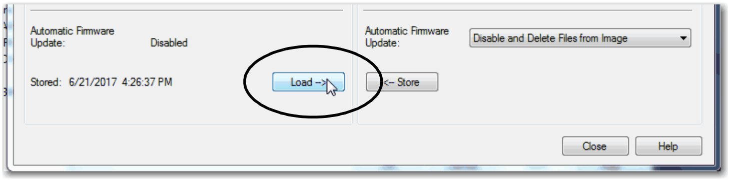
Image in Nonvolatile Memory
Name: L340ERM_application
Type: 5069-L340ERM CompactLogix™ 5380 Controller
Revision: 31.2
Load Image: User Initiated
Load Mode: Program (Remote Only)
Image Note:

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.

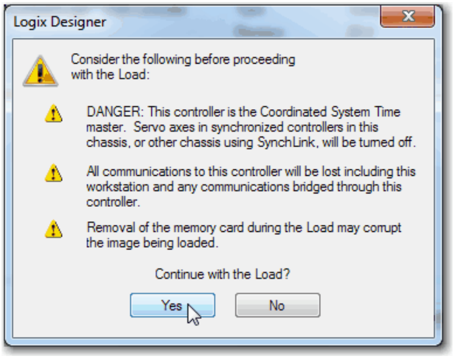
Verify that the controller is not in Run Mode.

4. Click Load.



Automatic Firmware Update: Disabled
Stored: 6/21/2017 4:26:37 PM
Automatic Firmware Update: Disable and Delete Files from Image

5. Click Yes in the confirmation dialog box that appears.



Consider the following before proceeding with the Load:

DANGER: This controller is the Coordinated System Time master. Servo axes in synchronized controllers in this chassis, or other chassis using SynchLink, will be turned off.

All communications to this controller will be lost including this workstation and any communications bridged through this controller.

Removal of the memory card during the Load may corrupt the image being loaded.

Continue with the Load?

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

Table 9 - Indications for Load Status

Controller	SD Indicator	OK LED on Controller	4-Character Display Message
CompactLogix 5380 controller when restoring firmware or project	Flashing Green	Solid Red	"LOAD", then followed by "UPDT"
Compact GuardLogix 5380 SIL 2 controller when restoring firmware or project	Flashing Green	Solid Red	"LOAD", then followed by "UPDT"
Compact GuardLogix 5380 SIL 3 controller during primary controller firmware update	Flashing Green	Solid Green	"Updating Firmware…Do Not Remove SD Card"
Compact GuardLogix 5380 SIL 3 controller during Safety Partner firmware update	Flashing Green	Blinking Red	"Updating Firmware…Do Not Remove SD Card"
Compact GuardLogix 5380 SIL 3 controller during when loading project	Flashing Green	Solid Green	"Loading…Do Not Remove SD Card"

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

When the load is complete, the controller reboots.

Other Secure Digital Card Tasks

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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—Compact GuardLogix 5380 controllers only.

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

Notes:

EtherNet/IP Network

Overview

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers operate on EtherNet/IP™ networks. Before your controller can operate on EtherNet/IP network, you must configure driver in RSLinx® Classic software. For information on how to configure EtherNet/IP or USB drivers, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.

IMPORTANT	Some example graphics in this chapter use CompactLogix 5380 controllers and some use Compact GuardLogix 5380 controllers. The controller used is for example purposes only. Each example can use either controller type. For example, the graphics shown in section Linear Network Topology beginning on page 107 use Compact GuardLogix 5380 controllers. You can use CompactLogix 5380 controllers in the same examples.

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

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

EtherNet/IP Network Functionality

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The CompactLogix 5380 and Compact GuardLogix 5380 controllers support the following:

- Dual built-in EtherNet/IP network ports - Port A1 and port A2
- Support for these EtherNet/IP modes:
  - Dual-IP mode - Available with the Logix Designer® application, version 29 or later
  - Linear/DLR mode
- Support for these EtherNet/IP network topologies:
  - Device Level Ring (DLR)
  - Linear
  - Star
- Support for these EtherNet/IP network communication rates:
  - 10 Mbps
  - 100 Mbps
  - 1 Gbps
- Support for only full-duplex operation

IMPORTANT	If a device supports only half-duplex, you must connect it to a switch to communicate with a CompactLogix 5380 or Compact GuardLogix 5380 controller.

- Support for CIP Sync™ technology that is based on Time Synchronization using the IEEE-1588 Precision Time Protocol
- Duplicate IP address detection

For more information about network design, see the Ethernet Design Considerations Reference Manual, publication ENET-RM002.

Nodes on an EtherNet/IP Network

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

When you configure your CompactLogix 5380 or Compact GuardLogix 5380 control system, you must account for the number of EtherNet/IP nodes that you include in the I/O configuration section of your project.

Table 10 - CompactLogix 5380 and Compact GuardLogix 5380 Controller EtherNet/IP Nodes

CompactLogix 5380 Controllers	Compact GuardLogix 5380 Controllers	Nodes Supported, Max[1]
5069-L306ER, 5069-L306ERM	5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3	16
5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L310ERMK	5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	24
5069-L320ER, 5069-L320ERM, 5069-L320ERP	L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	40
5069-L330ER, 5069-L330ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	60
5069-L340ER, 5069-L340ERM, 5069-L340ERP	5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3	90
5069-L350ERM	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K 5069-L350ERMS3, 5069-L350ERMS3K	120
5069-L380ERM	5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3	150
5069-L3100ERM	5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	180

[1] With controller firmware revision 31 or later. Earlier firmware revisions can have lower node counts.

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 limit. The following are examples of devices that must be counted:

- Remote communication adapters
- Switches that are included in the I/O configuration section
- Devices with an embedded Ethernet port, such as drives, I/O modules, and linking devices
- Remote controllers when a produce/consume connection is established between the two controllers
- HMI devices that are included in the I/O configuration section
- Third-party devices that are directly connected to the EtherNet/IP network

Devices Excluded from the Node Count

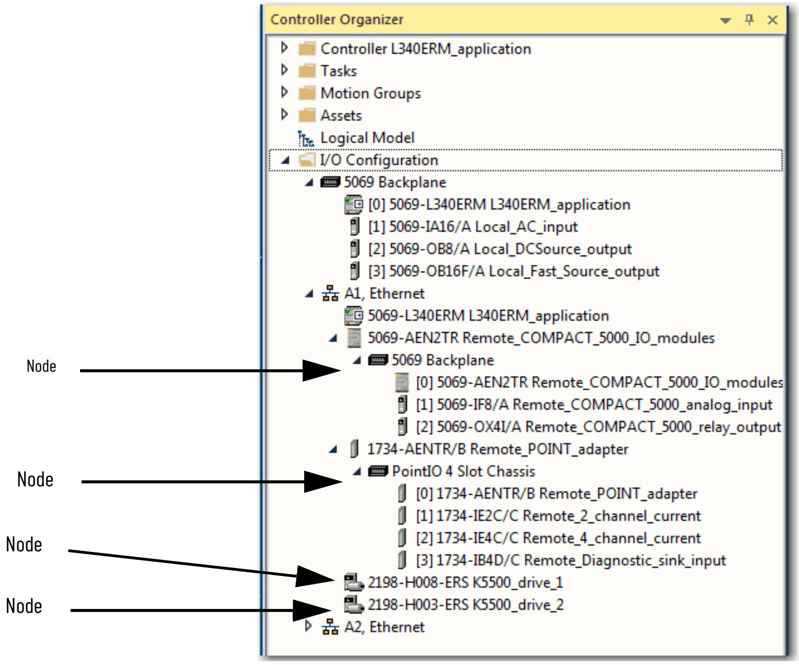
When you calculate the EtherNet/IP node limitation of a controller, do not count devices that exist on the EtherNet/IP network but are not added to the I/O configuration section.

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

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

Figure 24 shows nodes in the I/O tree.

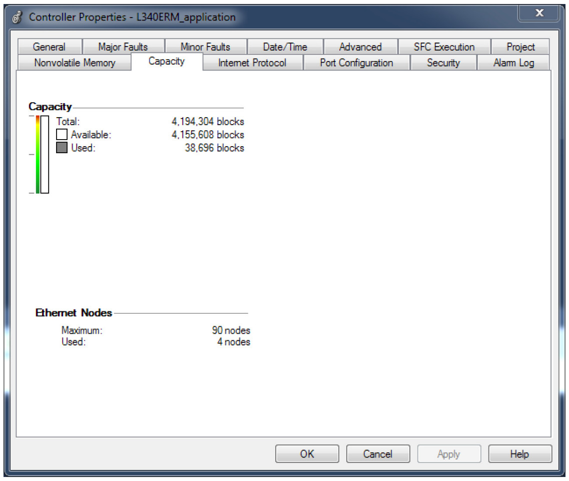
Figure 24 - Example EtherNet/IP Nodes



```
Controller Organizer
▷ Controller L340ERM_application
▷ Tasks
▷ Motion Groups
▷ Assets
  Logical Model
◢ I/O Configuration
  ◢ 5069 Backplane
      [0] 5069-L340ERM L340ERM_application
      [1] 5069-IA16/A Local_AC_input
      [2] 5069-OB8/A Local_DCSource_output
      [3] 5069-OB16F/A Local_Fast_Source_output
  ◢ A1, Ethernet
      5069-L340ERM L340ERM_application
    ◢ 5069-AEN2TR Remote_COMPACT_5000_IO_modules
      ◢ 5069 Backplane
          [0] 5069-AEN2TR Remote_COMPACT_5000_IO_modules
          [1] 5069-IF8/A Remote_COMPACT_5000_analog_input
          [2] 5069-OX4I/A Remote_COMPACT_5000_relay_output
    ◢ 1734-AENTR/B Remote_POINT_adapter
      ◢ PointIO 4 Slot Chassis
          [0] 1734-AENTR/B Remote_POINT_adapter
          [1] 1734-IE2C/C Remote_2_channel_current
          [2] 1734-IE4C/C Remote_4_channel_current
          [3] 1734-IB4D/C Remote_Diagnostic_sink_input
      2198-H008-ERS K5500_drive_1
      2198-H003-ERS K5500_drive_2
  ▷ A2, Ethernet
```

The Capacity tab in the Controller Properties dialog box displays the number of Ethernet nodes that are used in a project. The following graphic represents the project in Figure 24.

Figure 25 - Capacity Tab



Capacity

Total:	4,194,304 blocks
□ Available:	4,155,608 blocks
■ Used:	38,696 blocks

Ethernet Nodes

Maximum:	90 nodes
Used:	4 nodes

EtherNet/IP Network Topologies

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

CompactLogix 5380 and Compact GuardLogix 5380 controllers support these EtherNet/IP network types:

- Device Level Ring Network Topology
- Linear Network Topology
- Star Network Topology

Some examples in this section use a CompactLogix 5380 controller and other examples use Compact GuardLogix 5380 controllers. This is for example purposes only. Either controller type can be used in each example.

Device Level Ring Network Topology

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

A DLR network includes the following types of ring nodes.

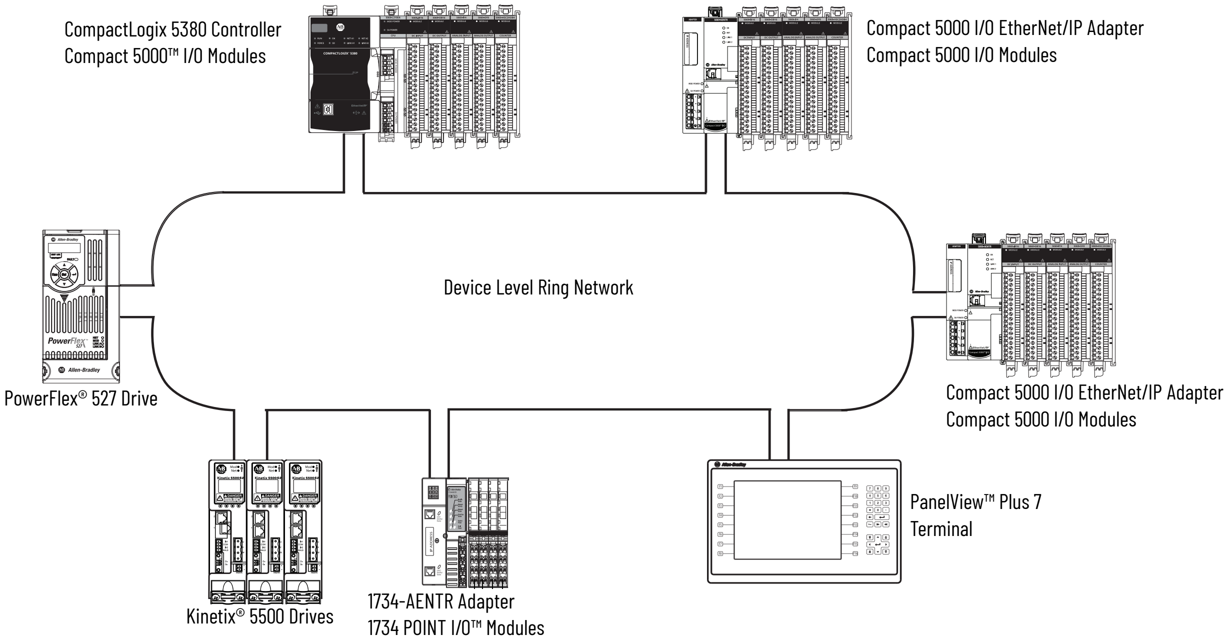
Node	Description
Ring supervisor	A ring supervisor provides these functions: • Manages traffic on the DLR network • Collects diagnostic information for the network A DLR network requires at least one node to be configured as ring supervisor. By default, the supervisor function is disabled on supervisor-capable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

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

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

IMPORTANT A CompactLogix 5380 or Compact GuardLogix 5380 controller is typically in Linear/DLR mode when it is used in a DLR topology. If the controller operates in Dual-IP mode, it must connect to a DLR topology via an ETAP that is connected to an Ethernet port on the controller.

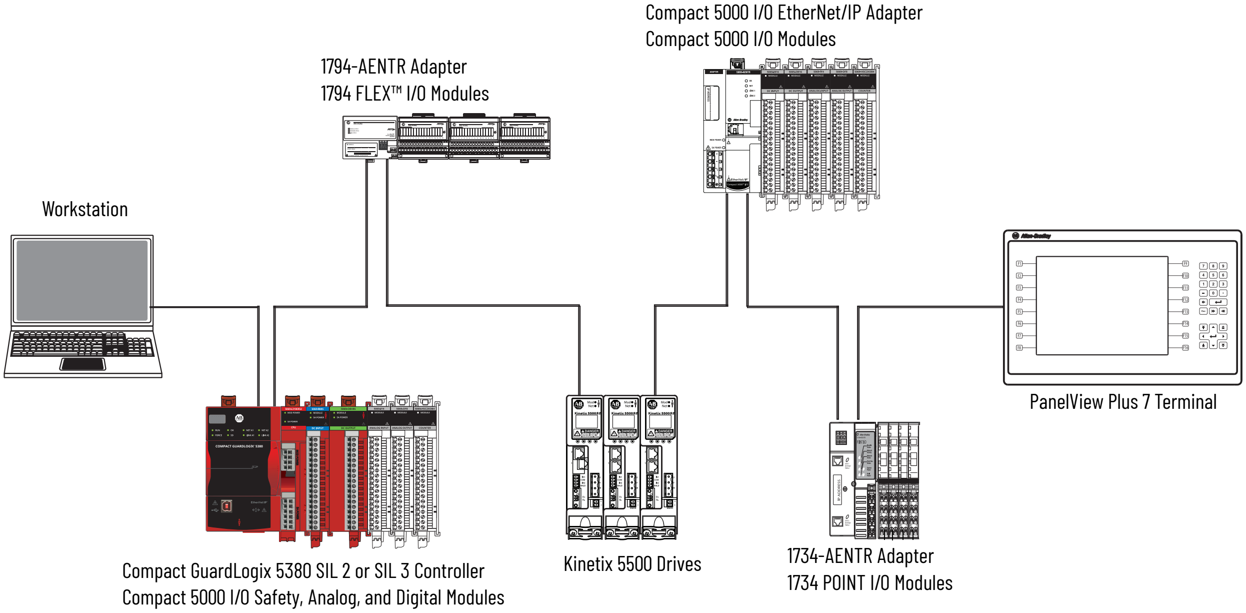
Figure 26 - CompactLogix 5380 Controller in a DLR Topology



Linear Network Topology

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

Figure 27 - Compact GuardLogix 5380 Controller in a Linear Network Topology


Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
1794-AENTR Adapter
1794 FLEX™ I/O Modules
Workstation
PanelView Plus 7 Terminal
Compact GuardLogix 5380 SIL 2 or SIL 3 Controller
Compact 5000 I/O Safety, Analog, and Digital Modules
Kinetix 5500 Drives
1734-AENTR Adapter
1734 POINT I/O Modules

For more information on how to design a DLR network, see the EtherNet/IP Embedded Switch Technology Application Guide, publication ENET-AP005

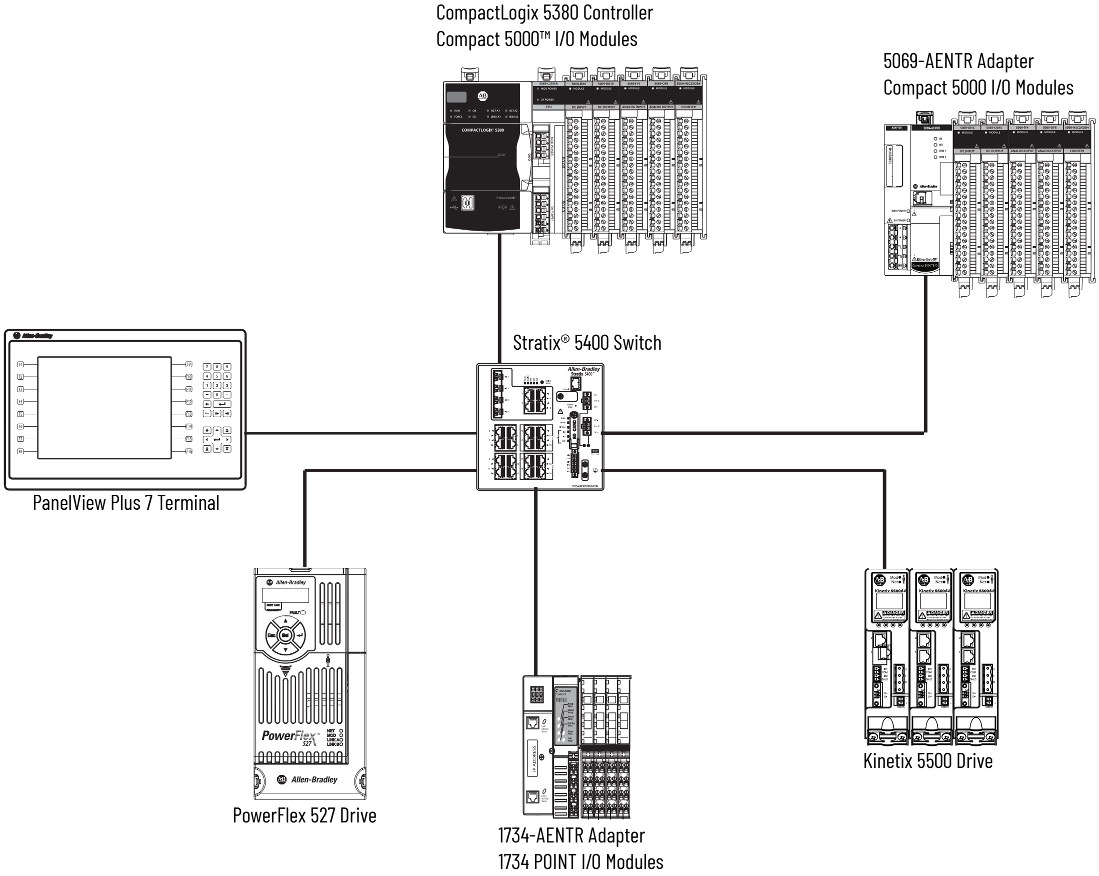
Star Network Topology

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

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

For more information on how to configure a controller that uses Dual-IP mode, see Use EtherNet/IP Modes on page 117.

Figure 28 - CompactLogix 5380 Controllers in a Star Network Topology



Integrated Architecture Tools

For more information when you design your CompactLogix 5380 system, see the Integrated Architecture® Tools and Resources web page. For example, you can access the Popular Configuration Drawings with different EtherNet/IP network topologies.

The tool and resources are available at: http://www.rockwellautomation.com/global/products-technologies/integrated-architecture/tools/overview.page

EtherNet/IP Network Communication Rates

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The CompactLogix 5380 and Compact GuardLogix 5380 controllers support these EtherNet/IP network communication rates:

- 10 Mbps
- 100 Mbps
- 1 Gbps

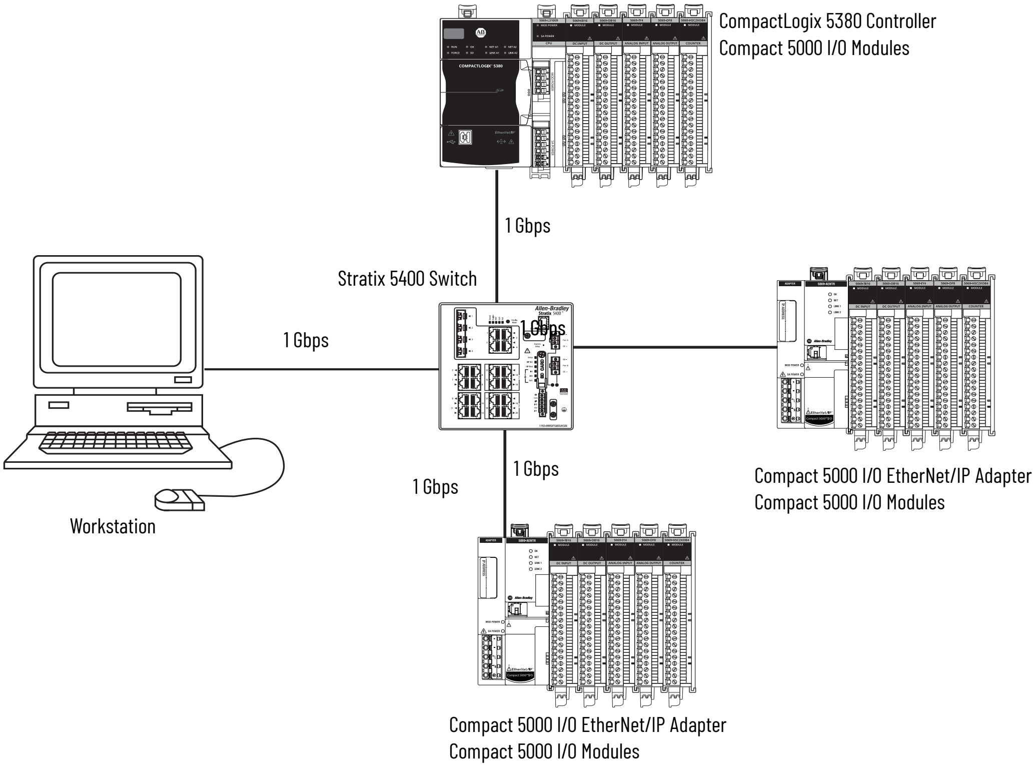
Network performance in a CompactLogix 5380 system is optimal if the 1 Gbps network communication rate is used. However, many Ethernet devices do not support the 1 Gbps network communication rate. Instead, they support a maximum rate of 100 Mbps.

The difference in maximum network communication rates impacts your CompactLogix 5380 system and, in some applications, restricts you from using the 1 Gbps network communication rate on a controller.

When you design a CompactLogix 5380 system and consider using the 1 Gbps rate on the controller, remember the following:

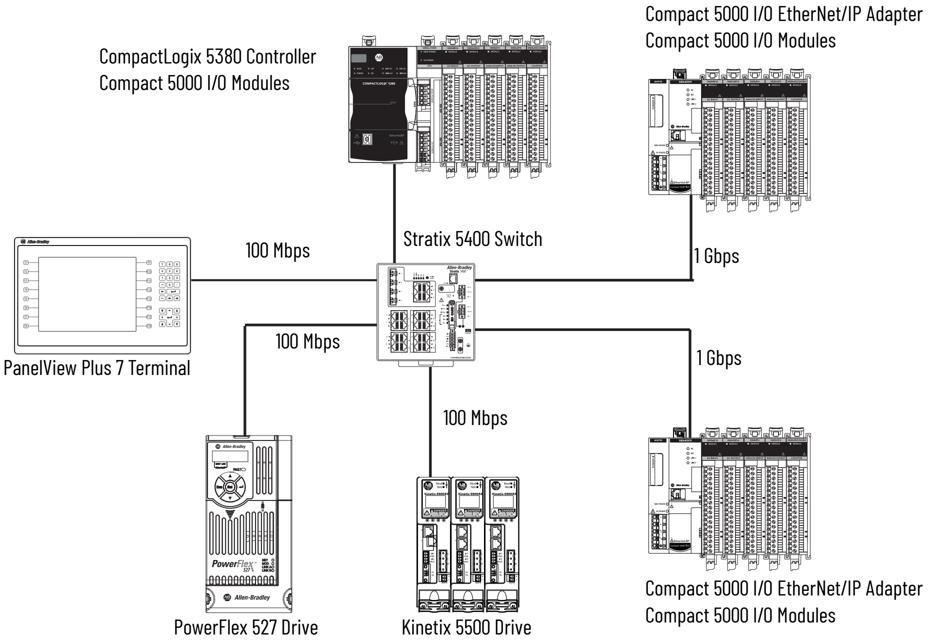
- You can use the 1 Gbps network communication rate on the controller ports when all network devices support the 1 Gbps, for example, 5069-AEN2TR adapters with Compact 5000 I/O modules and a gigabit-capable switch.

  When you use the 1 Gbps network communication rate, configure the controller ports to use Auto-Negotiate.



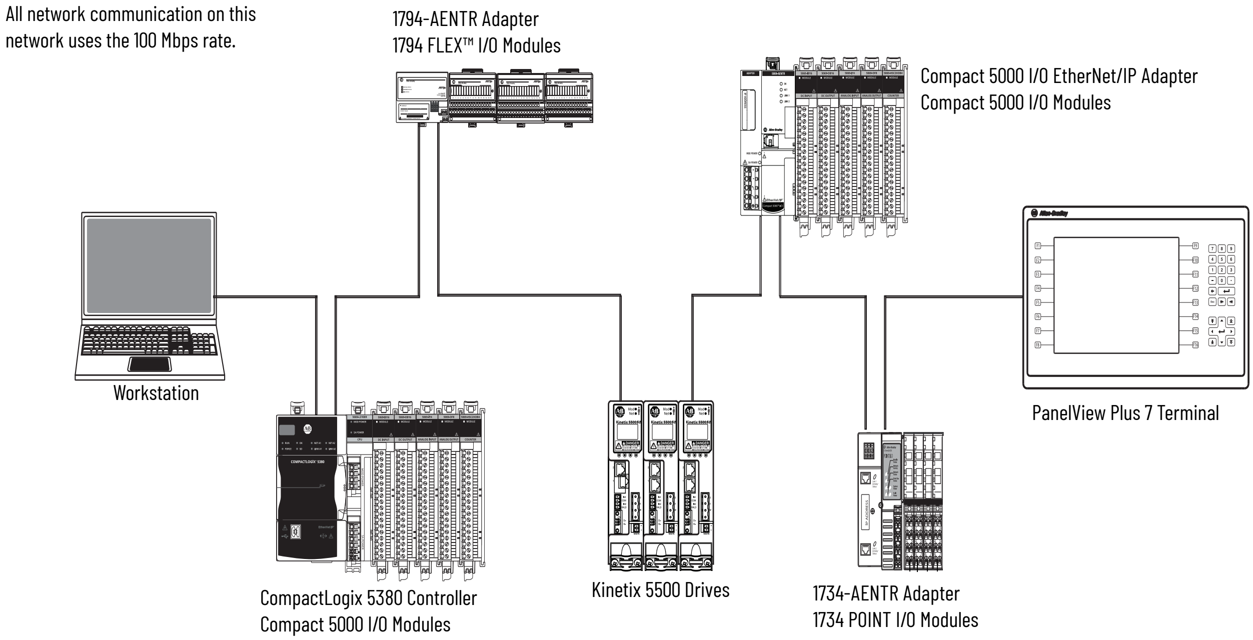
- You can use the 1 Gbps network communication rate on the controller ports when some network devices support a maximum network communication rate of 100 Mbps. However, in this case, the controller **must be connected** to those devices through a **managed switch**.

The port to which the controller is connected must be configured for Auto-Negotiate and the 1 Gbps network communication rate.



We recommend that you do not use the 1 Gbps network communication rate on the controller ports if it operates on a linear or DLR network topology and at least one device on the network supports the maximum network communication rate of 100 Mbps.

That is, do not use different network communication rates on device ports in the same EtherNet/IP network without a managed switch.



Simple Network Management Protocol (SNMP)

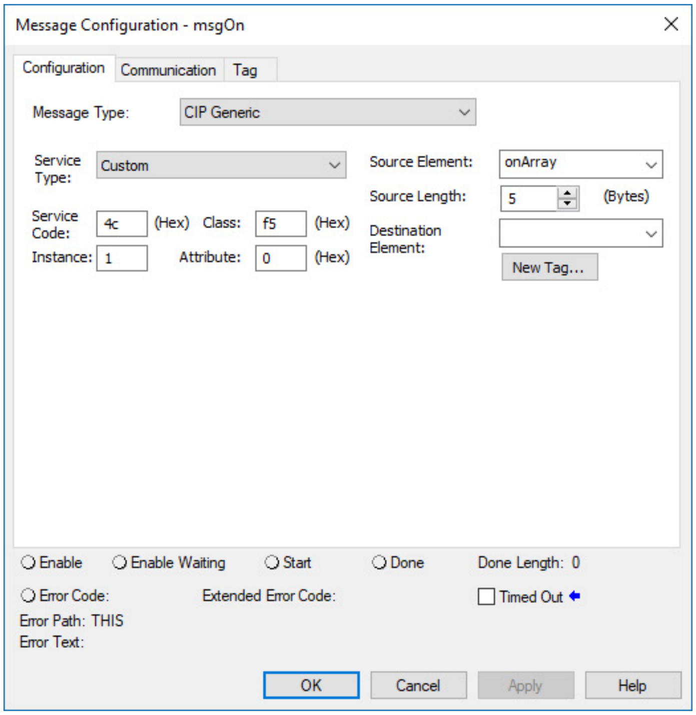
SNMP enables the controller to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. SNMP is disabled on the controller by default.

For more information about SNMP, see the Ethernet Reference Manual, publication ENET-RM002.

Use a CIP Generic MSG to Enable SNMP on the Controller

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

1. Add a MSG instruction to your program.
2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 11.



Message Configuration - msgOn

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex)

Instance: 1 Attribute: 0 (Hex)

Source Element: onArray

Source Length: 5 (Bytes)

Destination Element:

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

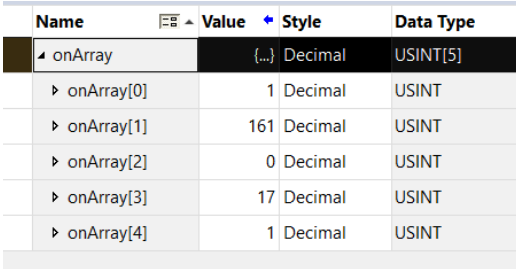
Error Path: THIS

Error Text:

Table 11 - Enable SNMP

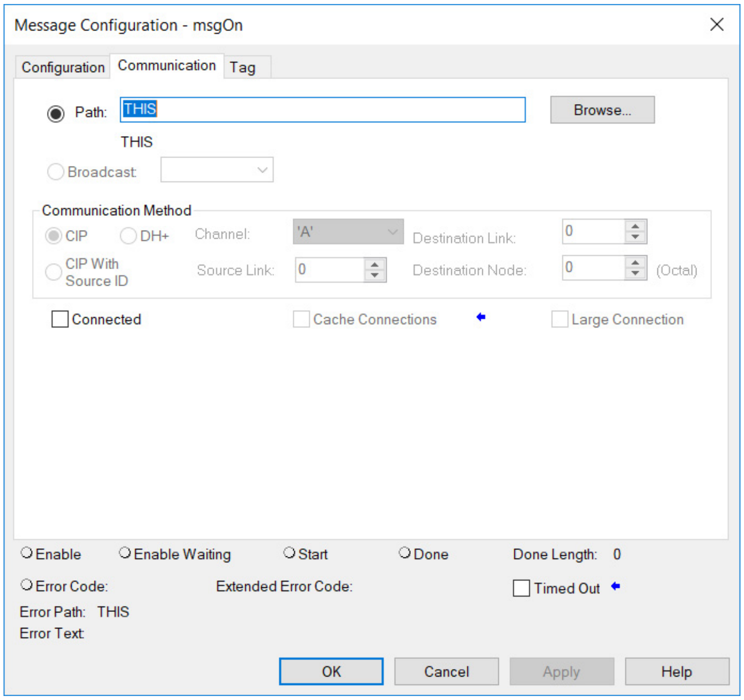
Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode
Class	f5

Table 11 - Enable SNMP (Continued)

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

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

IMPORTANT Messages to THIS must be unconnected messages.



Message Configuration - msgOn

● Path: THIS

THIS

○ Broadcast:

Communication Method

○ CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

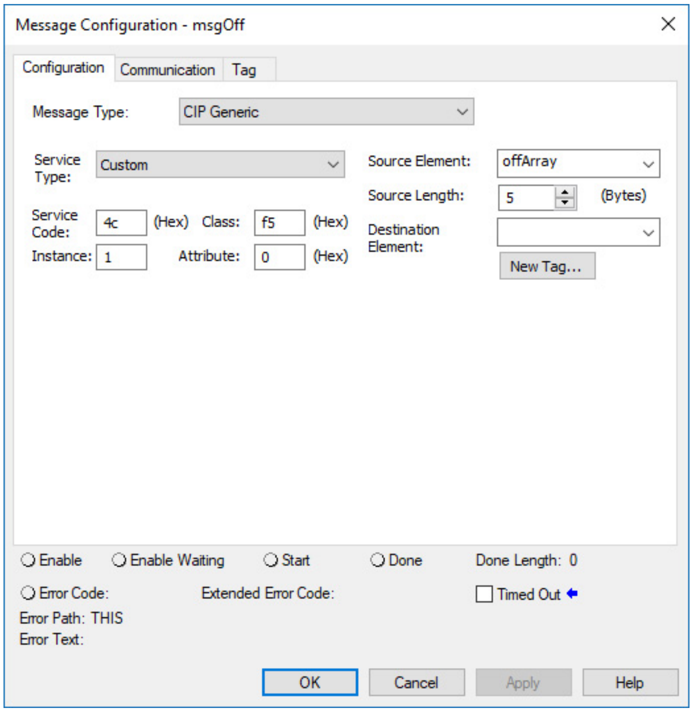
Error Text:

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 mode switch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 12.



Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex)

Class: f5 (Hex)

Instance: 1

Attribute: 0 (Hex)

Source Element: offArray

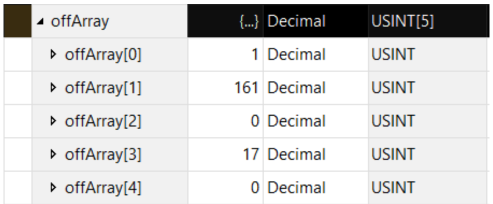
Source Length: 5 (Bytes)

Destination Element:

Error Path: THIS

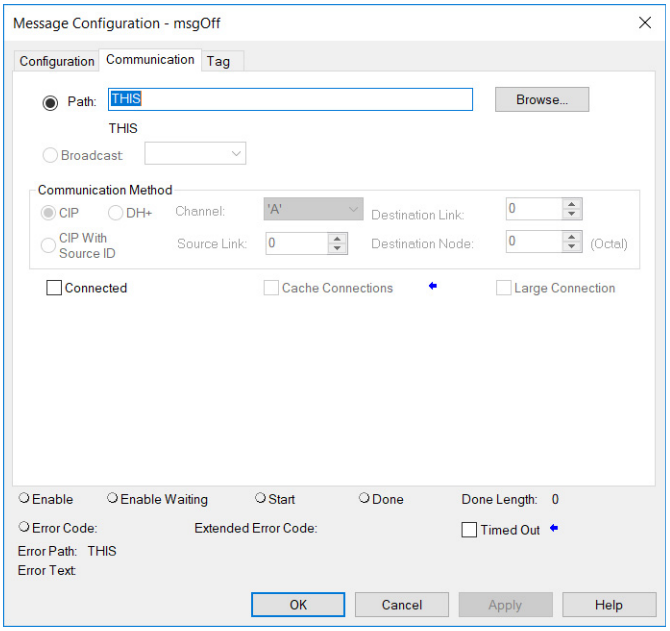
Error Text:

Table 12 - Disable SNMP

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode
Class	f5
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:  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 **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.
Source Length	5

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

IMPORTANT	Messages to THIS must be unconnected messages.



Message Configuration - msgOff

● Path: THIS

THIS

○ Broadcast:

Communication Method

○ CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

Socket Interface

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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.

The controllers support up to 32 socket instances.

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

- All CompactLogix 5380 and Compact GuardLogix 5380 controllers must use unconnected MSG instructions for socket servers. When you configure a message for a CompactLogix 5380 and Compact GuardLogix 5380 controller, make sure that the Connected checkbox on the Message Configuration dialog box is cleared.
- When the controller operates in Dual-IP mode and uses a socket object, you can use an IP address with a Socket_Create service type. For more information, see Use Socket Object on page 134.

These products support a secure socket object:

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

For more information on the socket interface, see the following:

- EtherNet/IP Socket Interface Application Technique, publication ENET-AT002
- Knowledgebase Article *Socket Communication in ControlLogix and CompactLogix*

TLS Support

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

HTTP(S) REST API Client Support

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

- raC_Impl_HTTPClient
- raC_Impl_HTTPCmdGET
- raC_Impl_HTTPCmdPOST
- raC_Impl_HTTPCmdPUT

Notes:

Use EtherNet/IP Modes

Overview

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

This chapter describes the EtherNet/IP™ modes that are available with the CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers.

- Dual-IP
- Linear/DLR

We expect you to have a working knowledge of both modes before using a CompactLogix 5380 or Compact GuardLogix 5380 controller. This chapter describes specific tasks in each application that are related to the EtherNet/IP modes.

Other chapters in this publication describe how to perform more general tasks in the Studio 5000 Logix Designer® application and RSLinx® Classic software. If necessary, read those chapters to understand better the tasks that are described in this chapter.

Available Network Levels

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controllers can connect to these EtherNet/IP network levels:

- Enterprise-level Network
- Device-level Network

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

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

Enterprise-level Network

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

- You can connect only port A1 to an enterprise-level network.

IMPORTANT	When you set the IP address and subnet mask, you establish an IP address range for the port. Make sure that the IP address ranges that are established for each port on the controller do not overlap. For more information on overlapping IP address ranges, see Overlapping IP Address Ranges on page 123.

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

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

Device-level Network

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

- You are not required to connect the controller to an enterprise-level network to connect to device-level networks.
- You can connect port A1, port A2, or ports A1 and A2 to device-level networks.

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

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

EtherNet/IP Modes

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

With the Logix Designer application, version 29 or later, the controllers support these EtherNet/IP modes:

- Dual-IP Mode
- Linear/DLR Mode

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

Dual-IP Mode

Dual-IP mode lets you connect ports A1 and A2 to separate networks. In this mode, port A1 can connect to an enterprise-level network or a device-level network. Port A2 can only connect to a device-level network.

IMPORTANT	Dual-IP mode is first available with CompactLogix 5380 controller firmware revision 29.011 or later.

In this mode, each port requires its own network configuration. For more information on how to configure the Ethernet ports when the controller uses Dual-IP mode, see Configure EtherNet/IP Modes on page 124.

You must avoid overlapping IP address ranges when you configure the Ethernet ports in Dual-IP mode. For more information, see Overlapping IP Address Ranges on page 123.

Figure 29 shows a CompactLogix 5380 controller using Dual-IP mode in with connections to an enterprise-level network and a device-level network.

Figure 29 - Controller in Dual-IP Mode with Enterprise-level and Device-level Network Connections

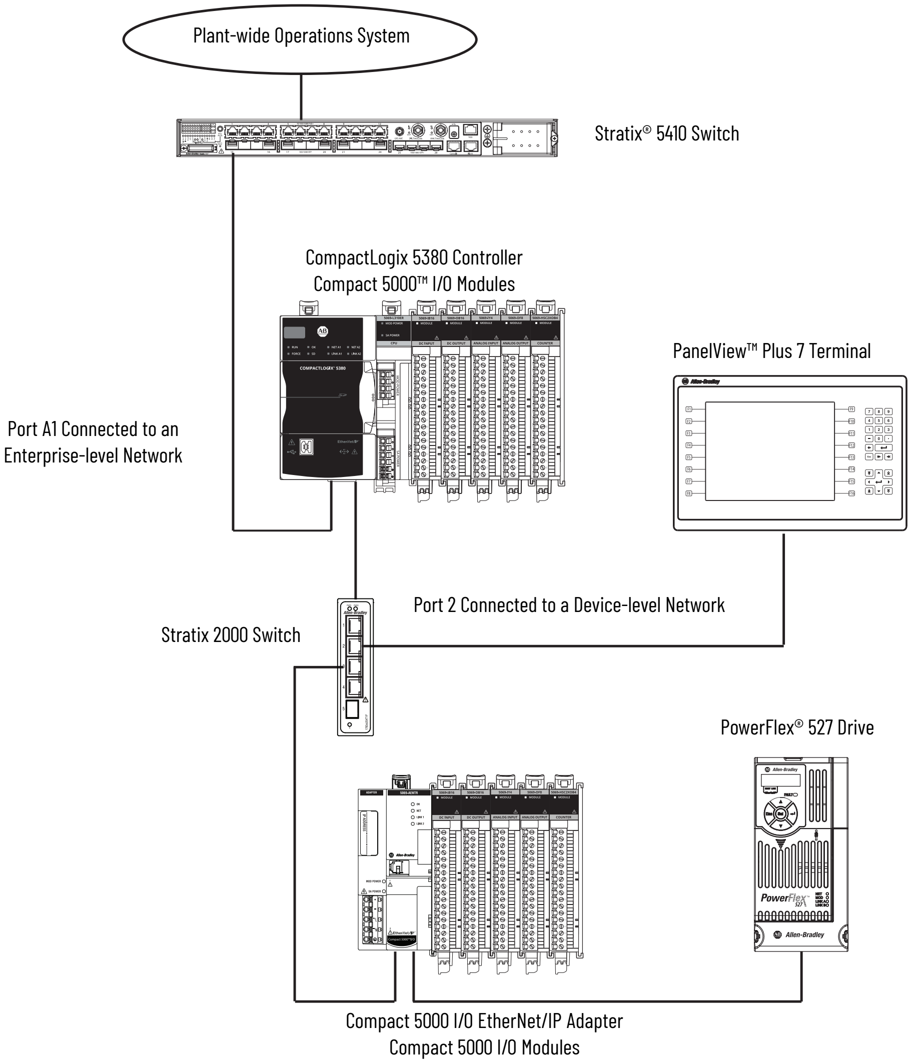
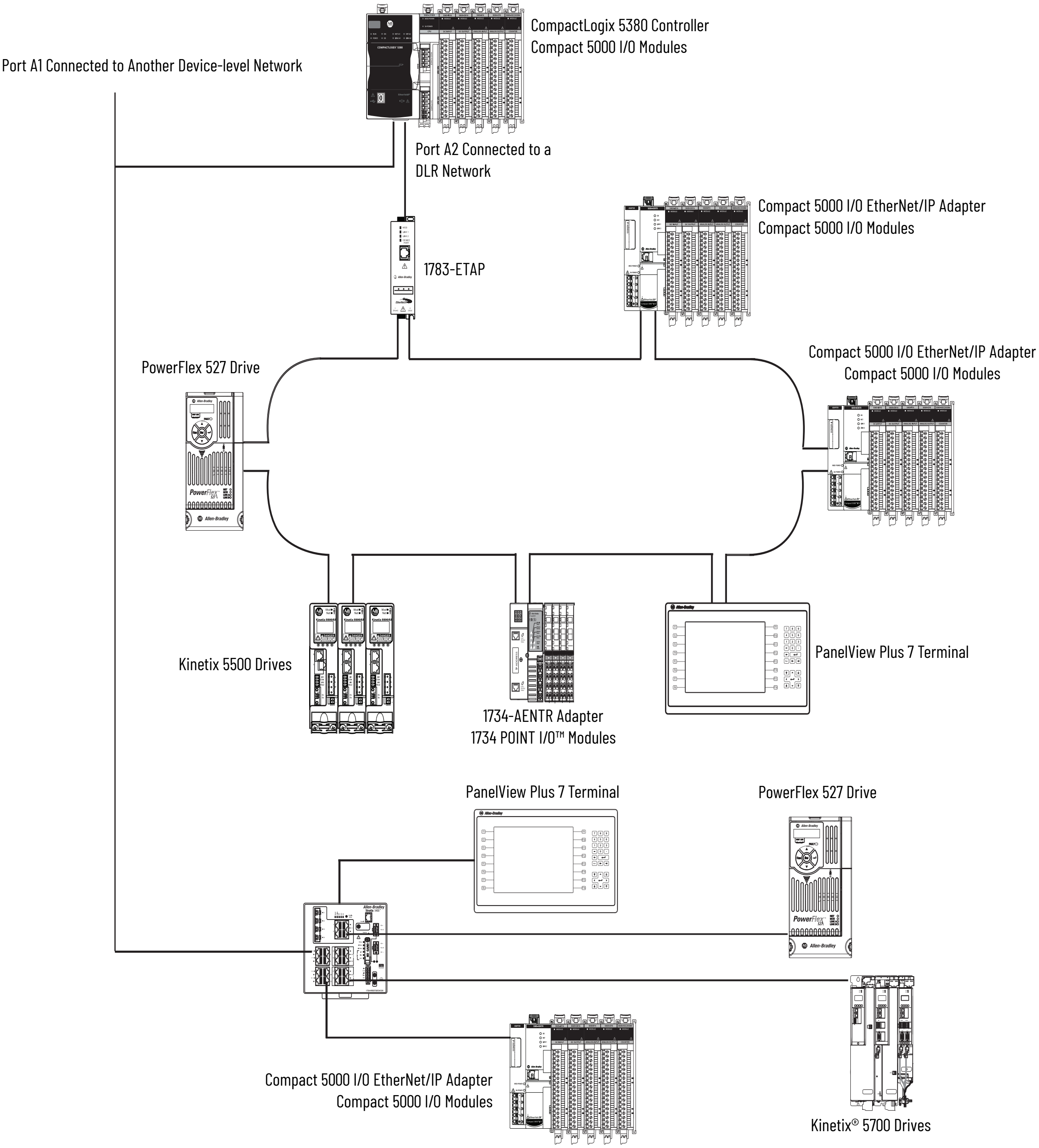

Plant-wide Operations System
Stratix® 5410 Switch
CompactLogix 5380 Controller
Compact 5000™ I/O Modules
PanelView™ Plus 7 Terminal
Port A1 Connected to an Enterprise-level Network
Port 2 Connected to a Device-level Network
Stratix 2000 Switch
PowerFlex® 527 Drive
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules

Figure 30 shows a CompactLogix 5380 controller using Dual-IP mode in with connections to separate device-level networks, including a DLR network.

IMPORTANT	If a controller is using Dual-IP mode, it can connect to a DLR network topology only through a 1783 Ethernet tap, in this case via port A2.

Figure 30 - Controller in Dual-IP Mode with Device-level Network Connections Only


CompactLogix 5380 Controller
Compact 5000 I/O Modules
Port A1 Connected to Another Device-level Network
Port A2 Connected to a DLR Network
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
1783-ETAP
PowerFlex 527 Drive
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
Kinetix 5500 Drives
1734-AENTR Adapter
1734 POINT I/O™ Modules
PanelView Plus 7 Terminal
PanelView Plus 7 Terminal
PowerFlex 527 Drive
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
Kinetix® 5700 Drives

Controller Functionality Considerations in Dual-IP Mode

Remember these controller functions when you use Dual-IP mode:

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

Linear/DLR Mode

When controllers operate in Linear/DLR mode, they can only connect to one network with one network configuration. The two physical ports allow the controller to connect to linear or DLR media topologies.

After firmware revision 29.011 or later is installed on a controller, the EtherNet/IP mode is automatically set to Dual-IP mode. You must change the EtherNet/IP Mode to use Linear/DLR mode.

For more information on how to change the controller to Linear/DLR mode, see Change the EtherNet/IP Mode on page 129.

Figure 31 - CompactLogix 5380 Controller in Linear/DLR Mode in a DLR Network

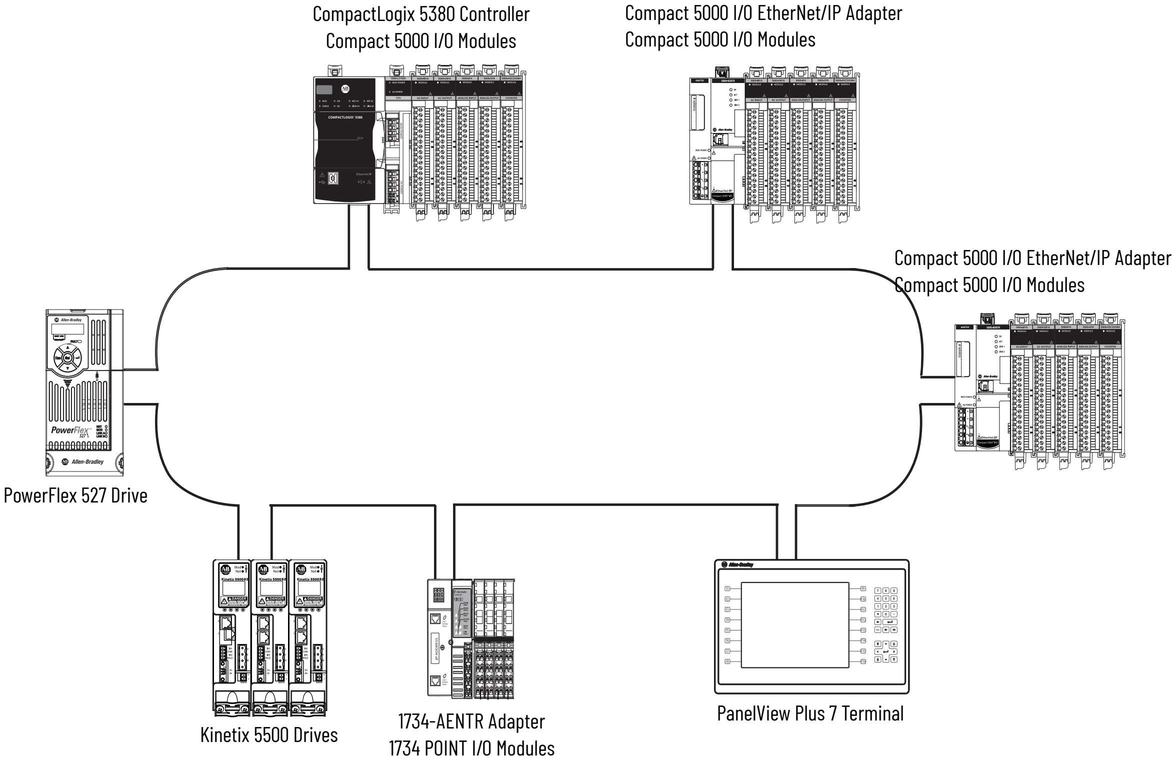


Figure 32 - Compact GuardLogix 5380 Controller in Linear/DLR Mode in a Linear Network

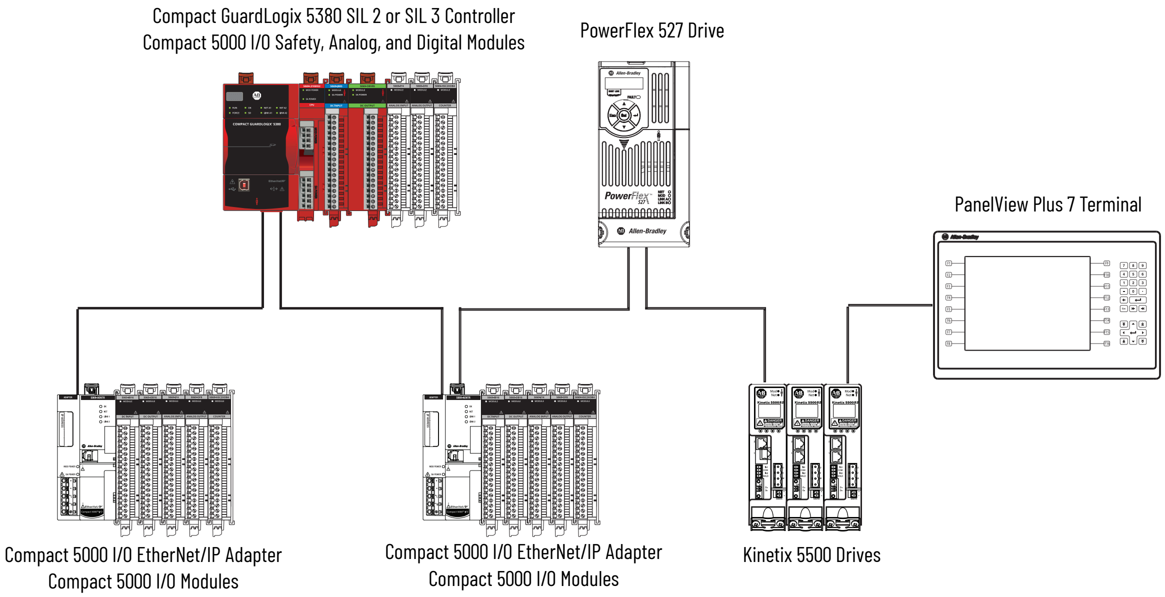
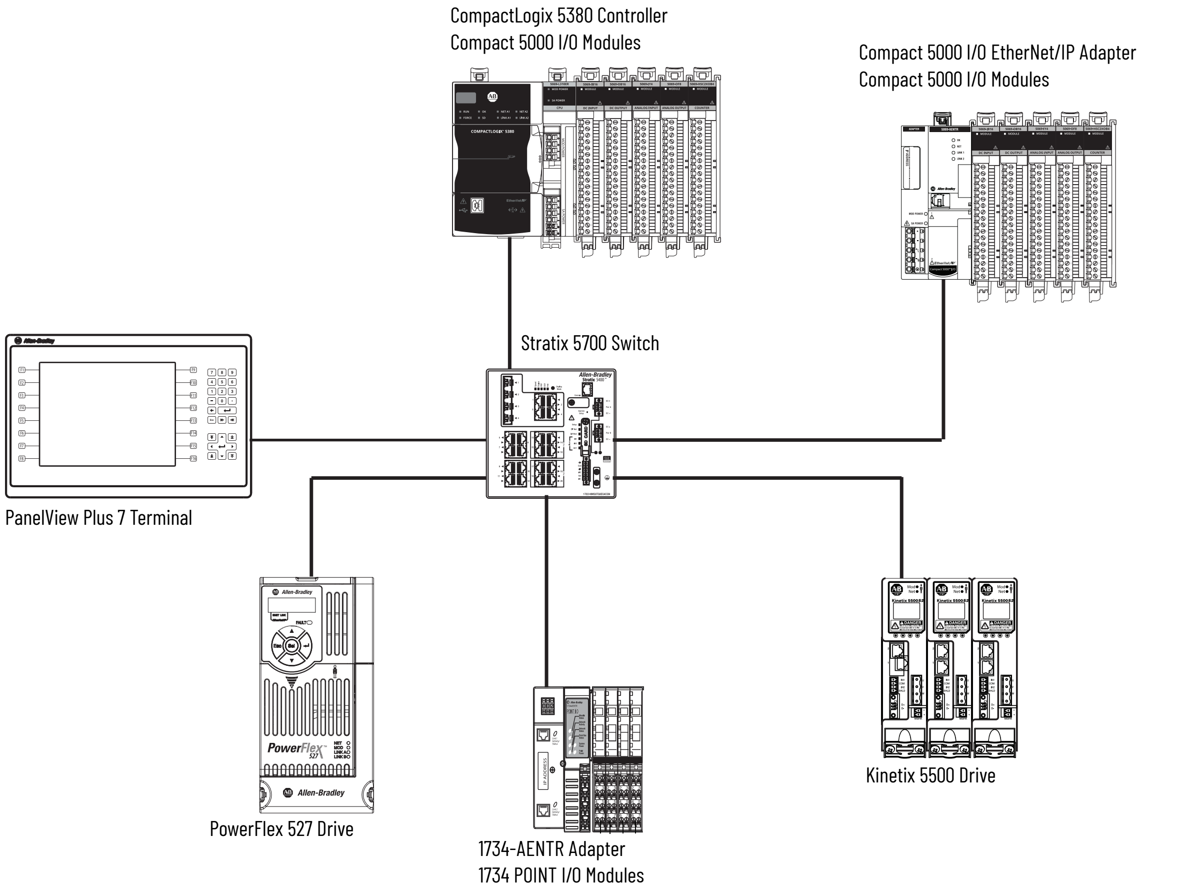

Compact GuardLogix 5380 SIL 2 or SIL 3 Controller
Compact 5000 I/O Safety, Analog, and Digital Modules
PowerFlex 527 Drive
PanelView Plus 7 Terminal
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
Compact 5000 I/O EtherNet/IP Adapter
Compact 5000 I/O Modules
Kinetix 5500 Drives

Figure 33 - CompactLogix 5380 Controller in Linear/DLR Mode in a Star Network



Overlapping IP Address Ranges

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

If you use the controller in Linear/DLR mode, you can skip this section and proceed to Linear/DLR Mode on page 121.

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

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

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

EXAMPLE **IP Address Ranges Do Not Overlap**

The table describes port A1 and port A2 configurations that use IP address ranges that do not overlap.

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

Port Number	IP Address	Subnet Mask/ Network Mask	IP Address Range (Low to High)
A1	192.168.1.5	255.255.255.0	192.168.1.1…192.168.1.254
A2	192.168.2.1	255.255.255.0	192.168.2.1…192.168.2.254

EXAMPLE **IP Address Ranges Do Overlap**

The table describes port A1 and port A2 configurations that use IP address ranges that do overlap.

All IP addresses in the port A2 IP address range are in the port A1 IP address range.

Port Number	IP Address	Subnet Mask/ Network Mask	IP Address Range (Low to High)
A1	192.168.1.5	255.255.252.0	192.168.0.1…192.168.3.254
A2	192.168.2.1	255.255.255.0	192.168.2.1…192.168.2.254

The difference between the port configurations in the examples is the Subnet Mask/Network Mask value for port A1.

In the first example, the value is 255.255.255.0. In the second example, the value 255.255.252.0.

Configure EtherNet/IP Modes

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can configure both Dual-IP and Linear/DLR EtherNet/IP modes with these software applications:

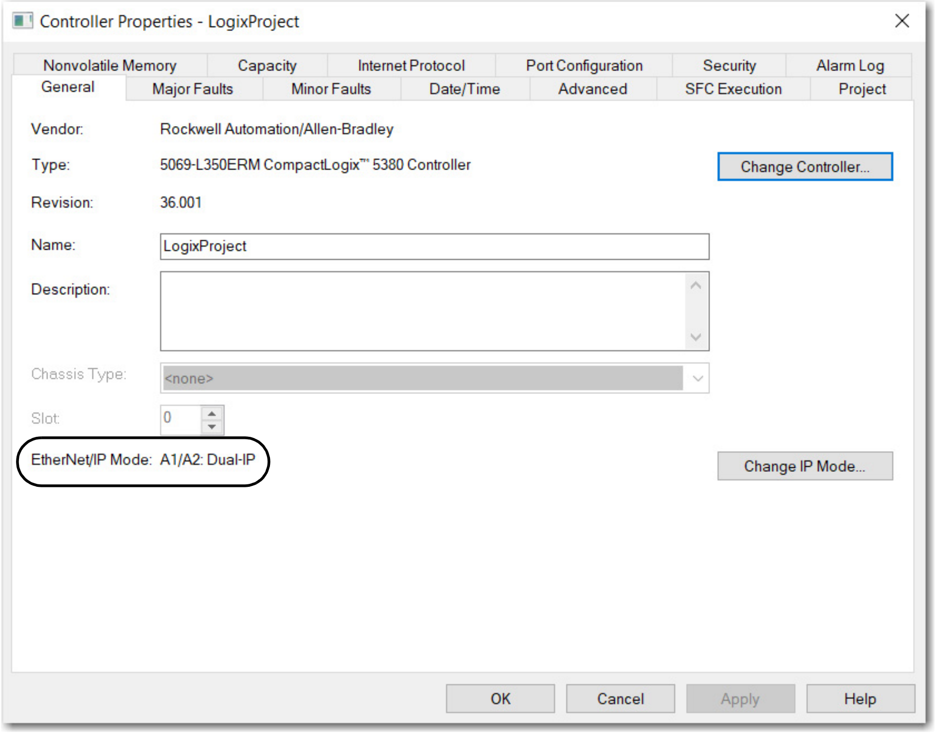
- Logix Designer application, version 29 or later
- RSLinx Classic software, version 3.81.00 or later
- With the Logix Designer application, version 28, the 5069-L320ER and 5069-L340ERM controllers only support Linear/DLR mode.

IMPORTANT	Keep in mind that the applicable minimum software versions vary by controller catalog number. That is, you can use some controllers in lower software minimum versions than others.

The screens can be slightly different on the Controller Properties dialog box for Compact GuardLogix 5380 controllers. For example, the Compact GuardLogix 5380 Controller Properties dialog box includes a Safety tab that does not exist in the CompactLogix 5380 Controller Properties dialog box.

Configure Dual-IP Mode in the Logix Designer Application

In the Logix Designer application version 29 or later, the EtherNet/IP mode is Dual-IP by default and is displayed on the General tab in the Controller Properties dialog box.



Vendor: Rockwell Automation/Allen-Bradley

Type: 5069-L350ERM CompactLogix™ 5380 Controller

Revision: 36.001

Name: LogixProject

Description:

Chassis Type: <none>

Slot: 0

EtherNet/IP Mode: A1/A2: Dual-IP

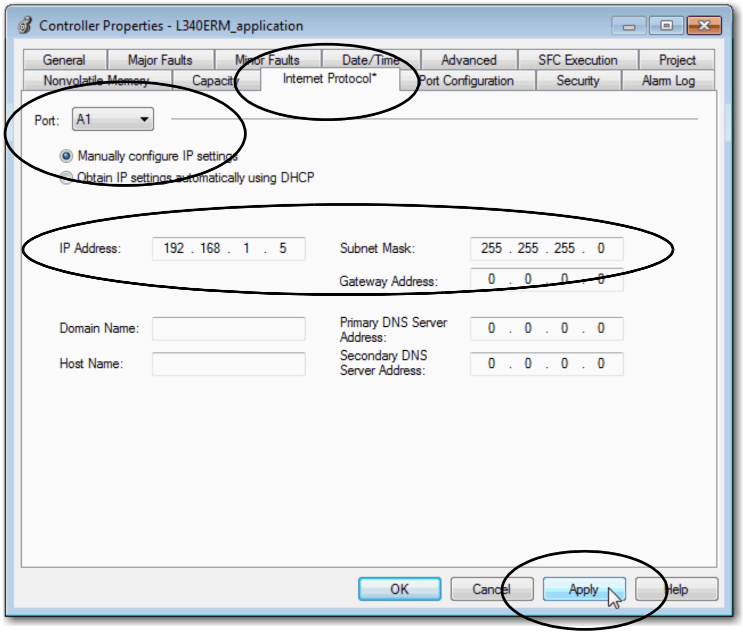
You set the IP address and subnet mask on the Internet Protocol tab.

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

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

   You cannot change the IP address or subnet mask if the controller is in Run mode.
3. Click the Internet Protocol tab.
4. From the Port pull-down menu, choose A1.

5. Click Manually configure IP settings.
6. Assign the IP address and network mask values.
7. Click Apply.



Port: A1

● Manually configure IP settings

○ Obtain IP settings automatically using DHCP

IP Address: 192 . 168 . 1 . 5

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

Domain Name:

Primary DNS Server Address: 0 . 0 . 0 . 0

Host Name:

Secondary DNS Server Address: 0 . 0 . 0 . 0

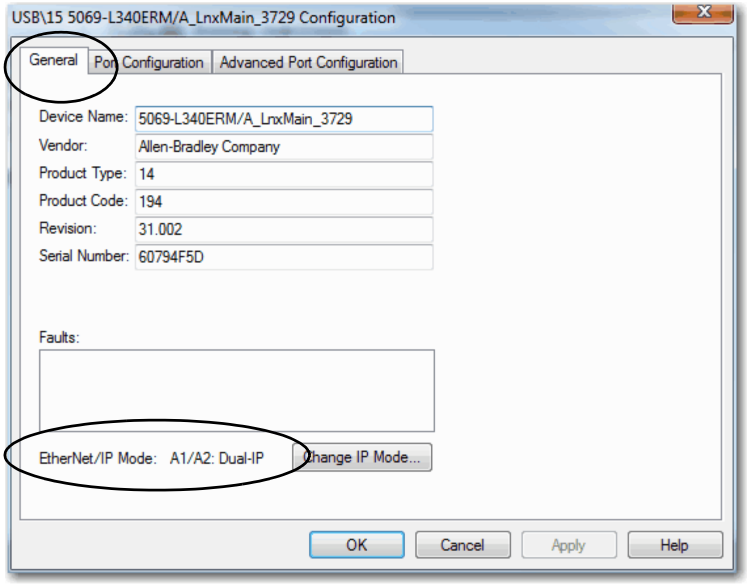
8. Repeat the previous steps, beginning at step 4.

   In step 4, make sure that you choose A2 in the Port field.

Configure Dual-IP Mode in RSLinx Classic Software

In RSLinx Classic software, the IP Mode for which the controller is configured is displayed on the General tab in the Configuration dialog box.

For example, this graphic displays that the controller is in Dual-IP mode.


USB\15 5069-L340ERM/A_LnxMain_3729 Configuration
General
Port Configuration
Advanced Port Configuration
Change IP Mode...
OK
Cancel
Apply
Help

Device Name: 5069-L340ERM/A_LnxMain_3729

Vendor: Allen-Bradley Company

Product Type: 14

Product Code: 194

Revision: 31.002

Serial Number: 60794F5D

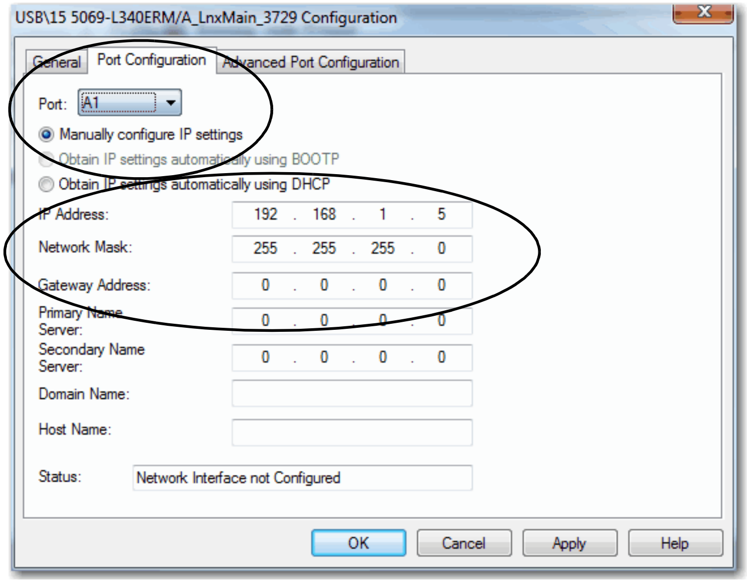
Faults:

EtherNet/IP Mode: A1/A2: Dual-IP

You set the IP Address and Network Mask on the Port Configuration tab.

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

1. From the Port pull-down menu, choose A1.
2. Click Manually configure IP settings.
3. Assign IP Address and Network Mask values.
4. Click Apply.


USB\15 5069-L340ERM/A_LnxMain_3729 Configuration
General
Port Configuration
Advanced Port Configuration
OK
Cancel
Apply
Help

Port: A1

● Manually configure IP settings

○ Obtain IP settings automatically using BOOTP

○ Obtain IP settings automatically using DHCP

IP Address: 192 . 168 . 1 . 5

Network Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

Primary Name Server: 0 . 0 . 0 . 0

Secondary Name Server: 0 . 0 . 0 . 0

Domain Name:

Host Name:

Status: Network Interface not Configured

5. Repeat the steps.

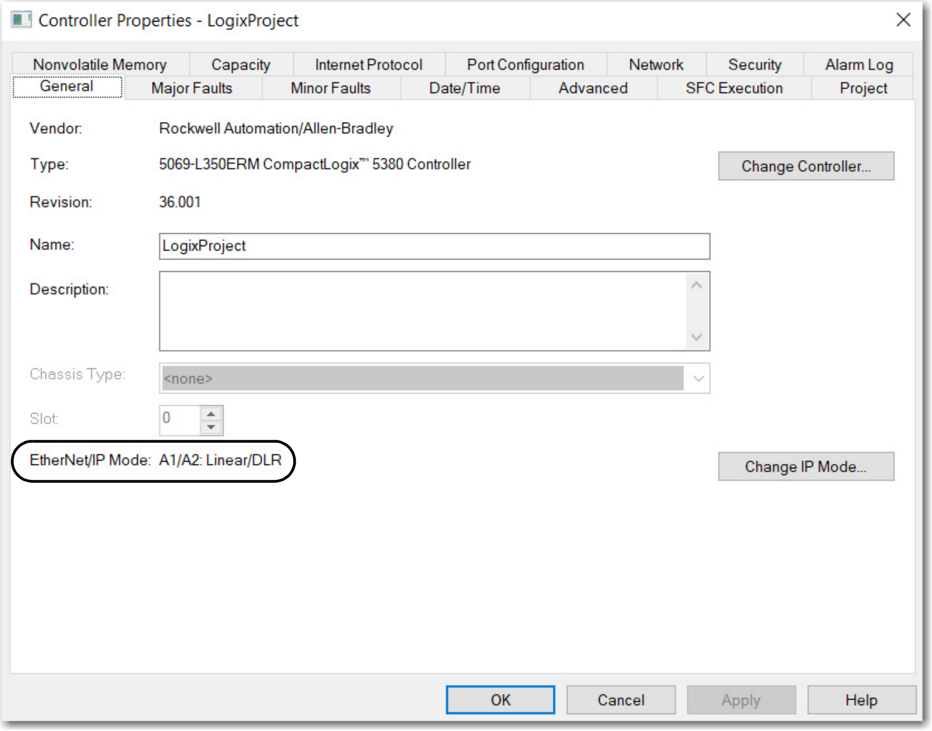
   In step 1, make sure that you choose A2 from the Port pull-down menu.

Configure Linear/DLR Mode in the Logix Designer Application

Remember, with firmware revision 29.011 or later, the EtherNet/IP Mode is Dual-IP by default. You must change the mode to use Linear/DLR mode.

IMPORTANT	For more information on how to change the controller EtherNet/IP mode, see Change the EtherNet/IP Mode on page 129.

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



Controller Properties - LogixProject

Vendor: Rockwell Automation/Allen-Bradley

Type: 5069-L350ERM CompactLogix™ 5380 Controller

Revision: 36.001

Name: LogixProject

Description:

Chassis Type: <none>

Slot: 0

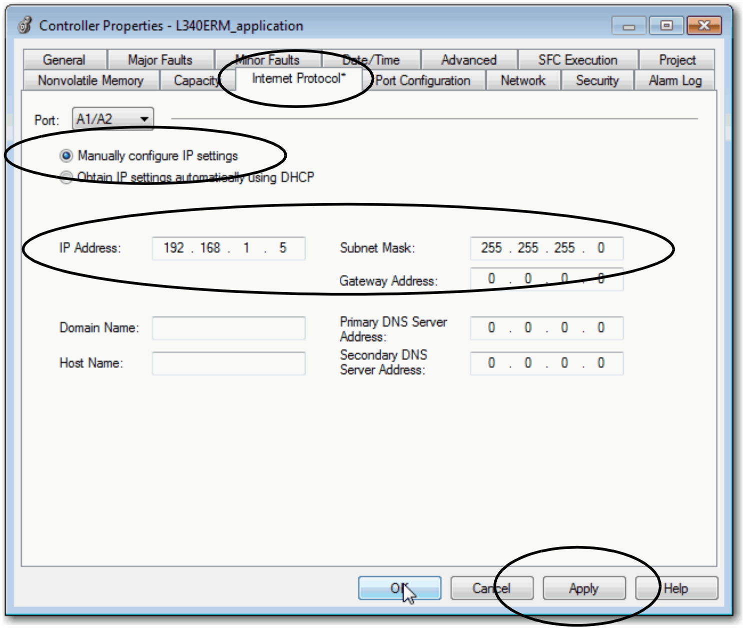
EtherNet/IP Mode: A1/A2: Linear/DLR

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

1. Confirm that the project is online and the controller is in Program mode, Remote Program mode, or Remote Run mode.

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

2. Click the Internet Protocol tab.
3. Click Manually configure IP settings.
4. Assign the IP address and network mask values and click Apply.



Controller Properties - L340ERM_application

Port: A1/A2

● Manually configure IP settings

○ Obtain IP settings automatically using DHCP

IP Address: 192 . 168 . 1 . 5

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

Domain Name:

Host Name:

Primary DNS Server Address: 0 . 0 . 0 . 0

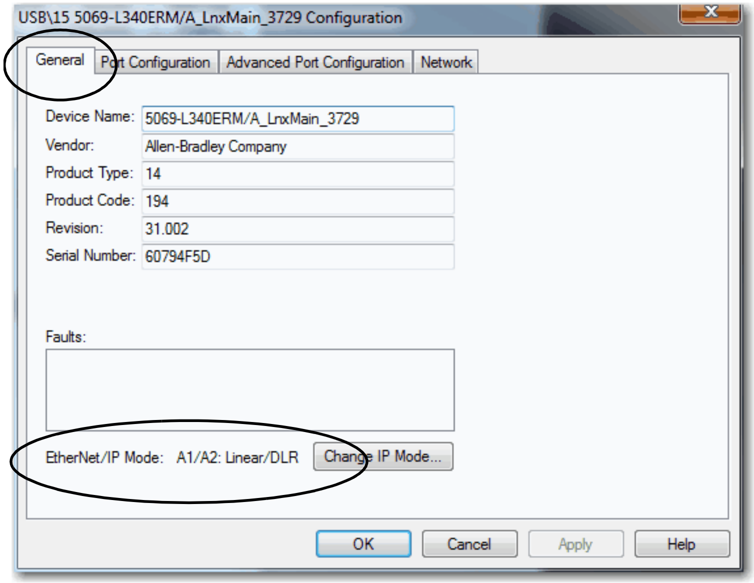
Secondary DNS Server Address: 0 . 0 . 0 . 0

Configure Linear/DLR Mode in RSLinx Classic Software

Remember, with firmware revision 29.011 or later, the EtherNet/IP Mode is Dual-IP by default. You must change the mode to use Linear/DLR mode.

IMPORTANT For more information on how to change the controller EtherNet/IP mode, see Change the EtherNet/IP Mode on page 129.

The new mode choice is displayed on the General tab in the Controller Properties dialog box.



USB\15 5069-L340ERM/A_LnxMain_3729 Configuration

Device Name: 5069-L340ERM/A_LnxMain_3729

Vendor: Allen-Bradley Company

Product Type: 14

Product Code: 194

Revision: 31.002

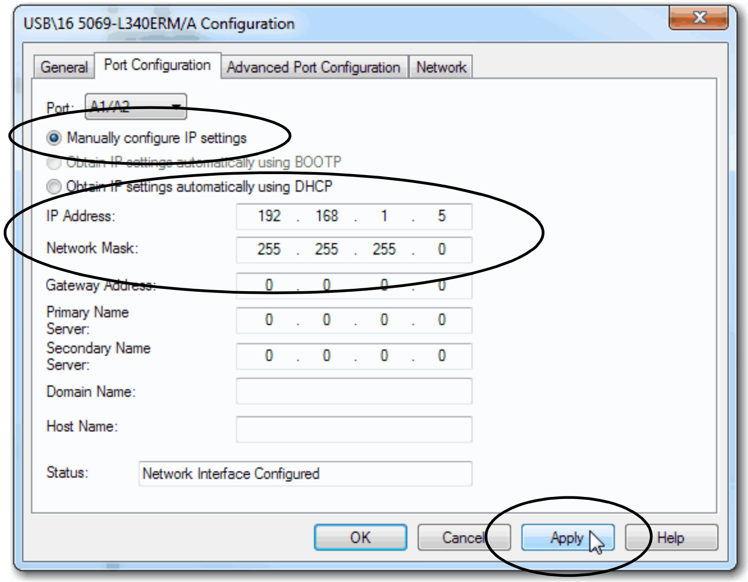
Serial Number: 60794F5D

Faults:

EtherNet/IP Mode: A1/A2: Linear/DLR

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

1. Confirm that the project is online.
2. Click the Port Configuration tab.
3. Click Manually configure IP settings.
4. Assign IP Address and Network Mask values.
5. Click Apply.



USB\16 5069-L340ERM/A Configuration

Port: A1/A2

● Manually configure IP settings

○ Obtain IP settings automatically using BOOTP

○ Obtain IP settings automatically using DHCP

IP Address: 192 . 168 . 1 . 5

Network Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

Primary Name Server: 0 . 0 . 0 . 0

Secondary Name Server: 0 . 0 . 0 . 0

Domain Name:

Host Name:

Status: Network Interface Configured

Change the EtherNet/IP Mode

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can change the EtherNet/IP mode in the Logix Designer application or RSLinx Classic software.

IMPORTANT Remember the following:

- Exercise caution when you change the EtherNet/IP mode on your controller, and consider the possible effects of the change.
- You cannot change the controller EtherNet/IP mode from Dual-IP to Linear/DLR when you are connected through port A1 port. You must be connected to the controller via port A2 to change from Dual-IP mode to Linear/DLR mode.

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

Table 13 - Effect of Changing the EtherNet/IP Mode

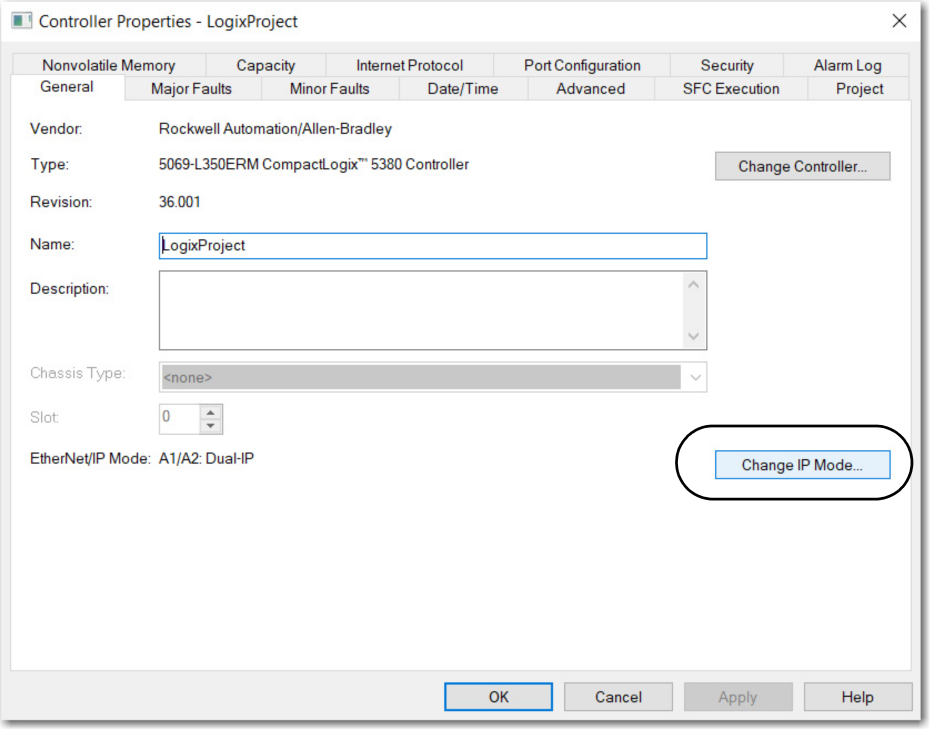
EtherNet/IP Mode Change	Effects
Dual-IP Mode to Linear/DLR Mode	• The port A2 IP address, network mask, default gateway settings are applied to the A1/A2 port. • The MAC address of port A1 is applied to port A1/A2. • This scenario exists if the controller firmware is upgraded to revision 29.011 or greater before an IP address is set. • Attempts to change from Dual-IP mode to Linear/DLR mode are only successful if the I/O configuration section in at least one port does not contain modules. • If the I/O configuration sections for both ports include modules, you cannot change the EtherNet/IP mode from Dual-IP mode to Linear/DLR mode.
Linear/DLR Mode to Dual-IP Mode	• The port A1/A2 IP address, network mask, default gateway settings are applied to port A2. • Other port A1/A2 settings, for example, DNS servers and Domain Name, are lost. • The port A1/A2 MAC address is applied to port A1. A separate MAC address is applied to Port A2. • Port A1 is DHCP-enabled. • The I/O Configuration section in the Logix Designer application project is automatically assigned to port A1. • You can change the I/O configuration in the Logix Designer application project to assign it to port A2.

Change the EtherNet/IP Mode in the Logix Designer Application

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

To change the EtherNet/IP mode in the Logix Designer application, complete these steps.

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



Controller Properties - LogixProject

Vendor: Rockwell Automation/Allen-Bradley

Type: 5069-L350ERM CompactLogix™ 5380 Controller

Revision: 36.001

Name: LogixProject

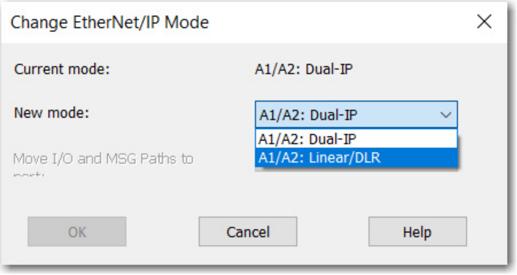
Description:

Chassis Type: <none>

Slot: 0

EtherNet/IP Mode: A1/A2: Dual-IP

3. From the New mode pull-down menu, choose the new mode and click OK.



Change EtherNet/IP Mode

Current mode: A1/A2: Dual-IP

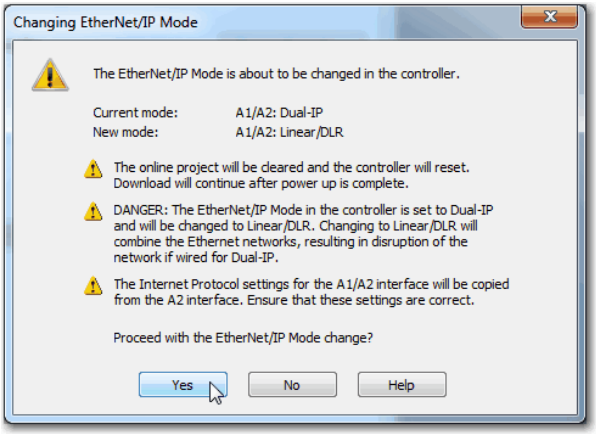
New mode: A1/A2: Dual-IP

Move I/O and MSG Paths to port:

4. Click OK on the Controller Properties dialog box.
5. Save the project.
6. Download the updated project to the controller.
7. When the following warning appears, read it carefully.

IMPORTANT Before you change the EtherNet/IP mode, make sure that you understand the impact on your controller when you change the mode.

For more information on the impact of changing the EtherNet/IP mode, see Table 13 on page 129.



Changing EtherNet/IP Mode

The EtherNet/IP Mode is about to be changed in the controller.

Current mode: A1/A2: Dual-IP
New mode: A1/A2: Linear/DLR

The online project will be cleared and the controller will reset. Download will continue after power up is complete.

DANGER: The EtherNet/IP Mode in the controller is set to Dual-IP and will be changed to Linear/DLR. Changing to Linear/DLR will combine the Ethernet networks, resulting in disruption of the network if wired for Dual-IP.

The Internet Protocol settings for the A1/A2 interface will be copied from the A2 interface. Ensure that these settings are correct.

Proceed with the EtherNet/IP Mode change?

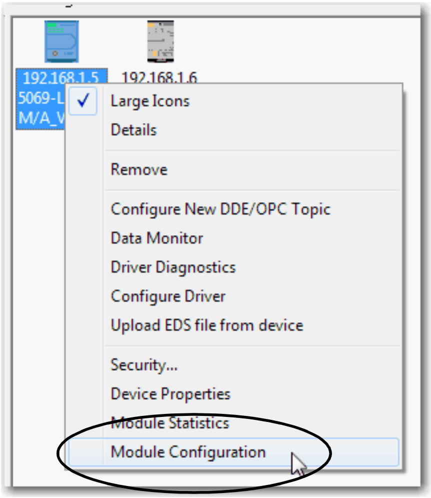
8. Click Yes to continue.

Change the EtherNet/IP Mode in RSLinx Classic Software

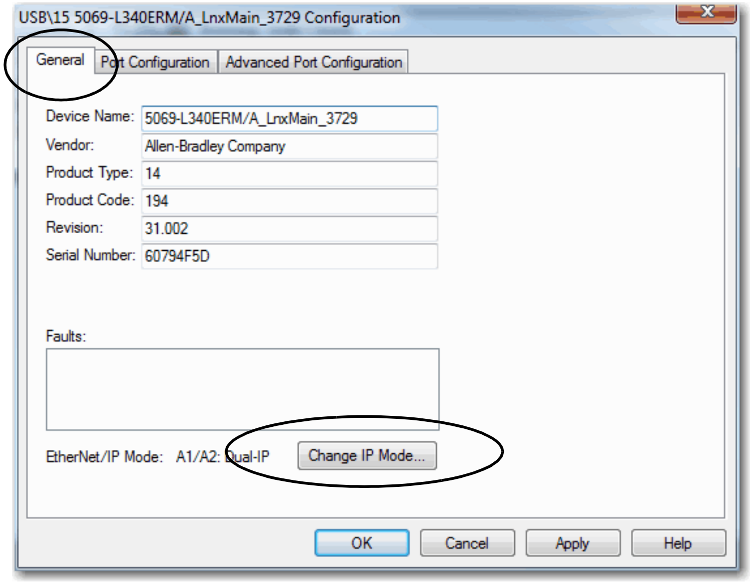
To change the EtherNet/IP mode in RSLinx Classic software, complete these steps.

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

   You cannot change the IP Address or Subnet Mask if the controller is in Run mode.
3. Right-click the controller and choose Module Configuration.



4. On the General tab of the Configuration dialog box, click Change IP Mode.



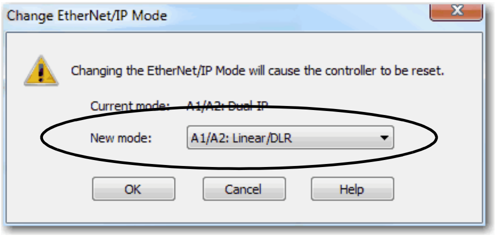
USB\15 5069-L340ERM/A_LnxMain_3729 Configuration

Device Name: 5069-L340ERM/A_LnxMain_3729
Vendor: Allen-Bradley Company
Product Type: 14
Product Code: 194
Revision: 31.002
Serial Number: 60794F5D

Faults:

EtherNet/IP Mode: A1/A2: Dual-IP

5. From the New mode pull-down menu, choose the new mode and click OK.



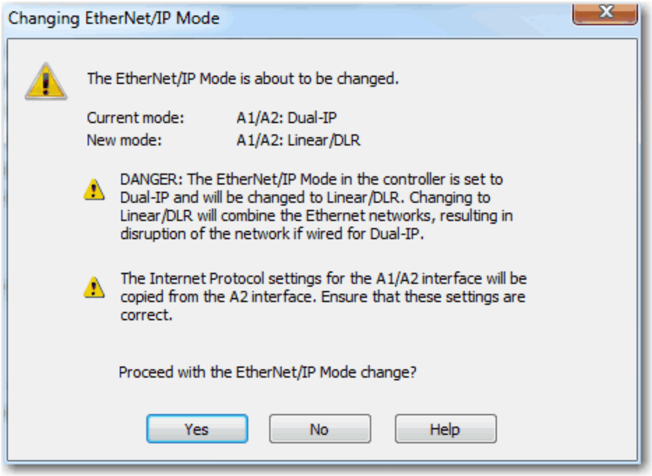
Change EtherNet/IP Mode

Changing the EtherNet/IP Mode will cause the controller to be reset.

Current mode: A1/A2: Dual-IP
New mode: A1/A2: Linear/DLR

6. When the following warning appears, read it carefully.

IMPORTANT	Before you change the EtherNet/IP mode, make sure that you understand the impact on your controller when you change the mode. For more information on the impact of changing the EtherNet/IP mode, see Table 13 on page 129.



Changing EtherNet/IP Mode

The EtherNet/IP Mode is about to be changed.

Current mode: A1/A2: Dual-IP
New mode: A1/A2: Linear/DLR

DANGER: The EtherNet/IP Mode in the controller is set to Dual-IP and will be changed to Linear/DLR. Changing to Linear/DLR will combine the Ethernet networks, resulting in disruption of the network if wired for Dual-IP.

The Internet Protocol settings for the A1/A2 interface will be copied from the A2 interface. Ensure that these settings are correct.

Proceed with the EtherNet/IP Mode change?

7. Click Yes to continue.

DNS Requests

To qualify the address of a module, use DNS addressing to specify a host name for a module, which also includes specifying a domain name and DNS servers. DNS addressing makes it possible to configure similar network structures and IP address sequences under different domains.

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

IMPORTANT	Safety Consideration For information on DNS Addressing for Compact GuardLogix 5380 controllers, see DNS Addressing on page 53.

For more information on DNS addressing, see the EtherNet/IP Network Configuration User Manual, publication ENET-UM001.

DNS Request Routing

DNS requests can be generated from port A1 or port A2.

DNS Request Generated From Port A1

- If the DNS server address is in the local subnet of port A1, DNS requests leave through A1 port.
- If port A2 is enabled and the DNS server address is in local subnet of port A2, DNS requests leave through A2 port.
- If the DNS server address is outside of all local subnets, DNS requests leave through A1 port towards port A1 default gateway.

DNS Request Generated From Port A2

- If port A1 is enabled and the DNS server address is in local subnet of port A1, DNS requests leave through A1 port.
- If the DNS server address is in local subnet of port A2, DNS requests leave through A2 port.
- If port A1 is enabled and the DNS server address is outside of all local subnets, DNS requests leave through A1 port towards port A1 default gateway.
- If port A1 is disabled and the DNS server address is outside of all local subnets, DNS requests leave through A2 port towards port A2 default gateway.

SMTP Server

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

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

Use Socket Object

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

Remember the following:

- If you use INADDR_ANY, IP communication that the Socket Object instance initiates follows the same routing rules as DNS request routing rules described in DNS Request Routing on page 133.
- If you use the IP address of port A1 instead of INADDR_ANY, IP packets can only go to the port A1 subnet or via its default gateway.
- If you use the IP address of port A2 instead of INADDR_ANY, IP packets can go only to port A2 subnet or via its default gateway.
- If you use an IP address other than the port A1 or A2 IP addresses or INADDR_ANY, the Create_Socket_Service request is rejected.

Send Message Instructions

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

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

- Enterprise port (Port A1) - 3
- Device-level port (Port A2) - 4

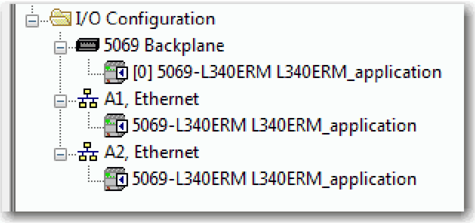
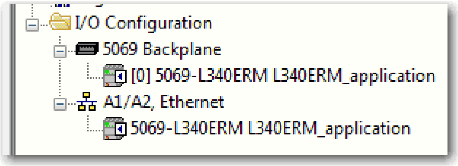
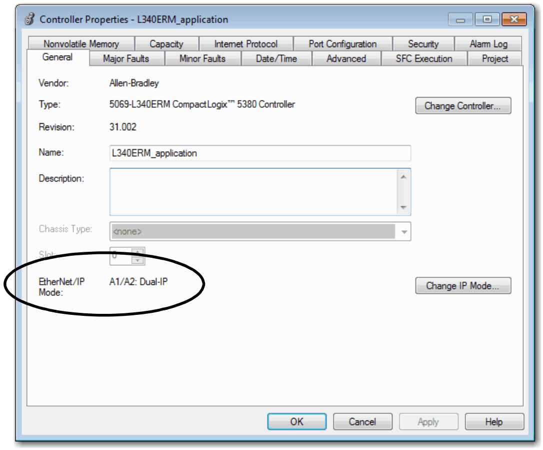
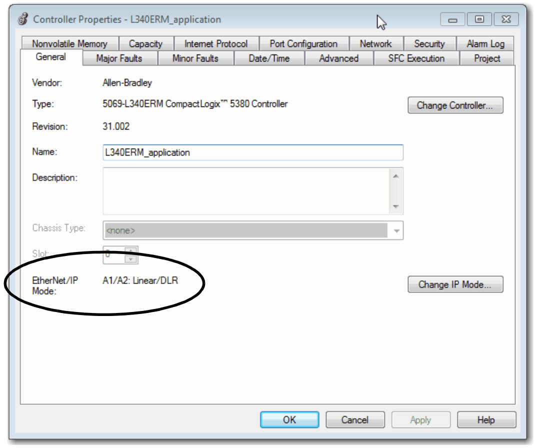
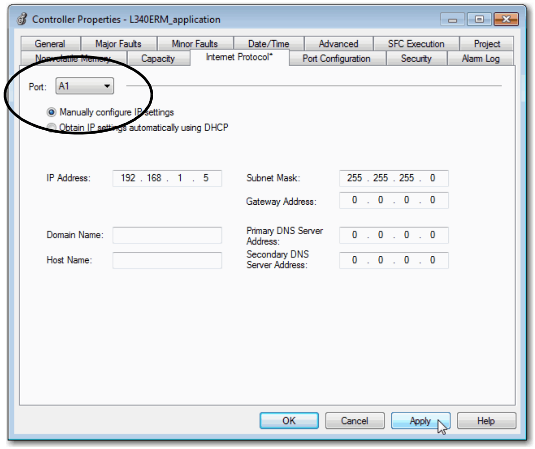
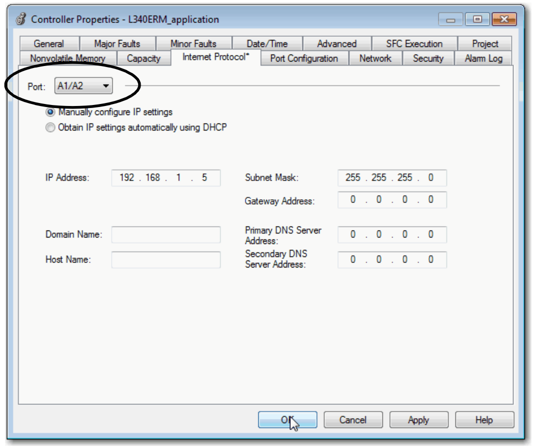
If the controller operates in Linear/DLR mode, the path is 2.

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

Software Display Differences for EtherNet/IP Modes

Table 14 shows differences in the Logix Designer application when the controller uses Dual-IP mode or Linear/DLR mode.

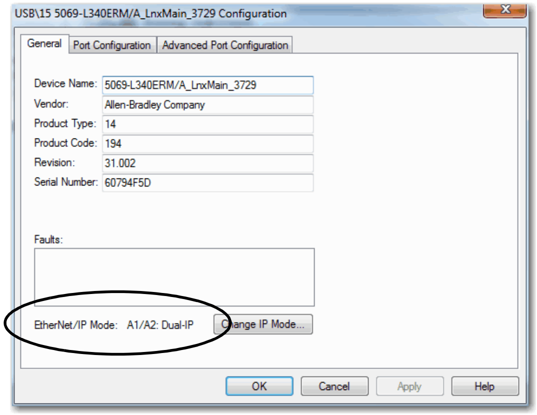
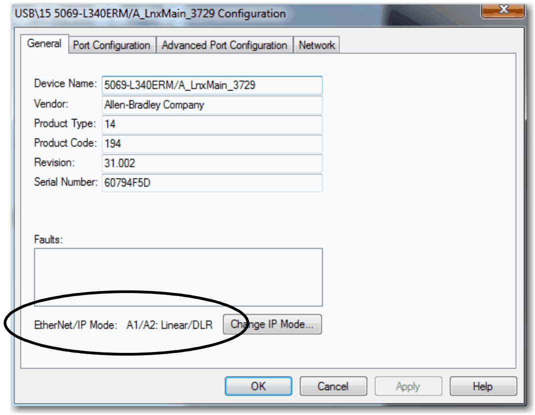
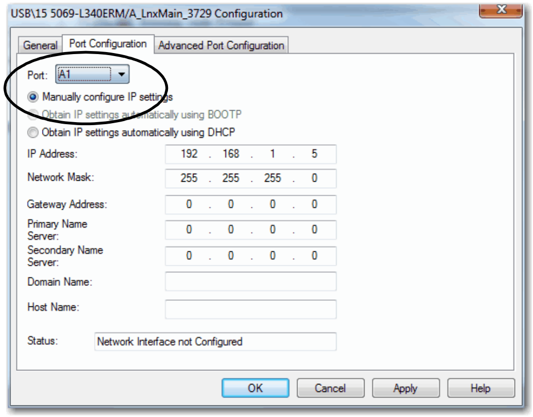
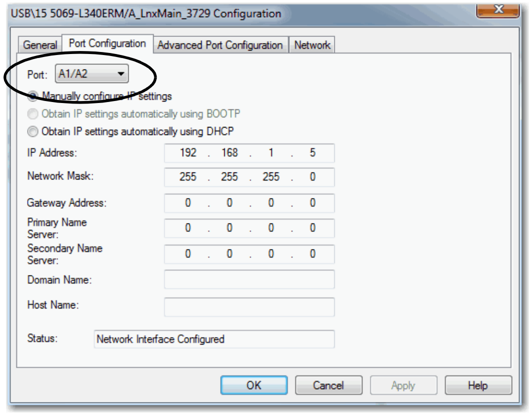
Table 14 - EtherNet/IP Mode Display Differences in the Logix Designer Application

	EtherNet/IP Mode	
Section in Application	**Dual-IP Mode**	**Linear/DLR Mode**
I/O Configuration Tree in Controller Organizer	 I/O Configuration 5069 Backplane [0] 5069-L340ERM L340ERM_application A1, Ethernet 5069-L340ERM L340ERM_application A2, Ethernet 5069-L340ERM L340ERM_application	 I/O Configuration 5069 Backplane [0] 5069-L340ERM L340ERM_application A1/A2, Ethernet 5069-L340ERM L340ERM_application
General Tab on Controller Properties Dialog Box	 Controller Properties - L340ERM_application Vendor: Allen-Bradley Type: 5069-L340ERM CompactLogix™ 5380 Controller Revision: 31.002 Name: L340ERM_application Description: Chassis Type: <none> Slot: 0 EtherNet/IP Mode: A1/A2: Dual-IP	 Controller Properties - L340ERM_application Vendor: Allen-Bradley Type: 5069-L340ERM CompactLogix™ 5380 Controller Revision: 31.002 Name: L340ERM_application Description: Chassis Type: <none> Slot: 0 EtherNet/IP Mode: A1/A2: Linear/DLR
Internet Protocol on Controller Properties Dialog Box	 Controller Properties - L340ERM_application Port: A1 ● Manually configure IP settings ○ Obtain IP settings automatically using DHCP IP Address: 192 . 168 . 1 . 5 Subnet Mask: 255 . 255 . 255 . 0 Gateway Address: 0 . 0 . 0 . 0 Domain Name: Host Name: Primary DNS Server Address: 0 . 0 . 0 . 0 Secondary DNS Server Address: 0 . 0 . 0 . 0 If you connect port A1 to a device-level network, some parameters appear as configurable but are not used. For more information on what parameters you configure to connect a port to a device-level network, see Device-level Network on page 118.	 Controller Properties - L340ERM_application Port: A1/A2 ● Manually configure IP settings ○ Obtain IP settings automatically using DHCP IP Address: 192 . 168 . 1 . 5 Subnet Mask: 255 . 255 . 255 . 0 Gateway Address: 0 . 0 . 0 . 0 Domain Name: Host Name: Primary DNS Server Address: 0 . 0 . 0 . 0 Secondary DNS Server Address: 0 . 0 . 0 . 0

The Controller Properties dialog box also provides a Network tab in the Logix Designer application when the controller uses Linear/DLR mode. The Network tab is not available when the controller uses Dual-IP mode.

Table 15 shows differences in RSLinx Classic software when the controller uses Dual-IP mode or Linear/DLR mode.

Table 15 - EtherNet/IP Mode Display Differences in the RSLinx Classic Software

	EtherNet/IP Mode	
Section in Software	**Dual-IP Mode**	**Linear/DLR Mode**
General Tab	 USB\15 5069-L340ERM/A_LnxMain_3729 Configuration General, Port Configuration, Advanced Port Configuration Device Name: 5069-L340ERM/A_LnxMain_3729 Vendor: Allen-Bradley Company Product Type: 14 Product Code: 194 Revision: 31.002 Serial Number: 60794F5D Faults: EtherNet/IP Mode: A1/A2: Dual-IP Change IP Mode... OK Cancel Apply Help	 USB\15 5069-L340ERM/A_LnxMain_3729 Configuration General, Port Configuration, Advanced Port Configuration, Network Device Name: 5069-L340ERM/A_LnxMain_3729 Vendor: Allen-Bradley Company Product Type: 14 Product Code: 194 Revision: 31.002 Serial Number: 60794F5D Faults: EtherNet/IP Mode: A1/A2: Linear/DLR Change IP Mode... OK Cancel Apply Help
Port Configuration Tab	 USB\15 5069-L340ERM/A_LnxMain_3729 Configuration General, Port Configuration, Advanced Port Configuration Port: A1 ● Manually configure IP settings ○ Obtain IP settings automatically using BOOTP ○ Obtain IP settings automatically using DHCP IP Address: 192 . 168 . 1 . 5 Network Mask: 255 . 255 . 255 . 0 Gateway Address: 0 . 0 . 0 . 0 Primary Name Server: 0 . 0 . 0 . 0 Secondary Name Server: 0 . 0 . 0 . 0 Domain Name: Host Name: Status: Network Interface not Configured OK Cancel Apply Help If you connect port A1 to a device-level network, some parameters appear as configurable but are not used. For more information on what parameters you configure to connect a port to a device-level network, see Device-level Network on page 118.	 USB\15 5069-L340ERM/A_LnxMain_3729 Configuration General, Port Configuration, Advanced Port Configuration, Network Port: A1/A2 ● Manually configure IP settings ○ Obtain IP settings automatically using BOOTP ○ Obtain IP settings automatically using DHCP IP Address: 192 . 168 . 1 . 5 Network Mask: 255 . 255 . 255 . 0 Gateway Address: 0 . 0 . 0 . 0 Primary Name Server: 0 . 0 . 0 . 0 Secondary Name Server: 0 . 0 . 0 . 0 Domain Name: Host Name: Status: Network Interface Configured OK Cancel Apply Help

The Configuration dialog box also provides a Network tab in RSLinx Classic software when the controller uses Linear/DLR mode. The Network tab is not available when the controller uses Dual-IP mode.

Manage Controller Communication

Connections

Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Connections are used when the system contains these conditions:

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

Controller Communication Interaction with Control Data

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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
- 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 controller behavior.

Table 16 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Behavior

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

Blocks - HelOps to prevents 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 verify 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 that are added to a structure for data integrity checking. That is, Start Data and End Data are added. 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

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:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controllers let you produce (transmit) and consume (receive) controller-scoped tags. CompactLogix 5380 and Compact GuardLogix 5380 controllers produce the same standard tag through the Ethernet ports and the backplane, and consumer counts apply to the total consumers from all ports.

Figure 34 - Example Produced and Consumed Tags

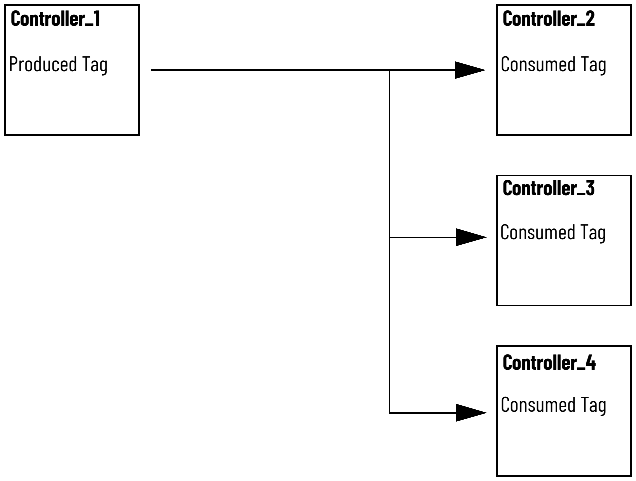


Table 18 describes the system-shared tags.

Table 18 - Produced and Consumed Tag Descriptions

Tag	Description
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.

The Compact GuardLogix 5380 controllers can also use produced and consumed safety tags. For more information on how to use them, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

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 that use the same port must request the same RPI value as the first consumer, otherwise they fail to connect. Controllers with backplane and Ethernet ports can produce data at an independent RPI value on each port.

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

Send and Receive Messages

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Messages transfer data to other devices, such as other controllers or operator interfaces. The MSG instruction is a Ladder Diagram 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 unconnected or connected. Unconnected messages depend on the availability of unconnected buffers in all devices through which the message passes. Connected messages begin with a request to allocate connection buffers in all of those devices, before sending the actual message. If you choose to cache a connected message, the controller keeps the connection open after the message is complete. Cached message improves efficiency if you intend to send the message repeatedly.

Connected messages use connection resources, and are less efficient than connected cached messages or unconnected messages. 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. Cached messages can get pushed from the cache if the application exceeds the cache capacity of the controller.

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

Table 19 - Message Types

Message Type	Communication Method	Connected Message	Message Can Be Cached
CIP™ data table read or write	—	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	—	Optional [1]	Yes[2]
Block-transfer read or write	—	Yes	Yes[2]

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

[2] We recommend that you cache connected messages that occur more frequently than once every 60 seconds, if possible.

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

Determine Whether to Cache Message Connections

When you configure a message instruction, you can cache the connection. Use Table 20 to decide to cache a connection.

Table 20 - Options for Caching Connections

If the Message Executes	Then
Repeatedly	Cache the connection. When you cache the connection, the connection remains open and execution time is optimized. If a connection is opened each time that the message executes, execution time is increased.
Infrequently	Do not cache the connection. When you do not cache the connection, the connection closes upon completion of the message. As a result, the connection is available for other uses. Unconnected messages are best used for infrequent cached message connections.

Cached connections transfer data faster than uncached connections. The controller can cache as many as 256 connections.

Standard I/O Modules

CompactLogix™ 5380 and Compact GuardLogix® 5380 systems support these I/O module options:

- Local I/O modules
- Remote I/O modules

Local I/O Modules

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The CompactLogix 5380 system uses Compact 5000™ I/O modules as local I/O modules. The modules are installed to the right of the controller.

The number of local Compact 5000 I/O modules that you can install in a CompactLogix 5380 system varies based on the controller that is used, up to a maximum of 31 modules.

Table 21 lists the number of local I/O modules that controllers support.

Table 21 - Local I/O Modules in CompactLogix 5380 System

CompactLogix 5380 Controllers	Compact GuardLogix 5380 Controllers	Local I/O Modules Supported, Max.
5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ERM, 5069-L310ERMK, 5069-L310ER-NSE	5069-L306ERS2, 5069-L306ERMS2, 5069-L306ERMS3, 5069-L310ERS2, 5069-L310ERS2K, 5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	8
5069-L320ER, 5069-L320ERM, 5069-L320ERP	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	16
5069-L330ER[1], 5069-L330ERM[1], 5069-L340ER, 5069-L340ERM, 5069-L340ERP, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2,5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K, 5069-L340ERS2, 5069-L340ERMS2, 5069-L340ERMS3, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K, 5069-L380ERS2, 5069-L380ERMS2, 5069-L380ERMS3, 5069-L3100ERS2, 5069-L3100ERMS2, 5069-L3100ERMS3	31

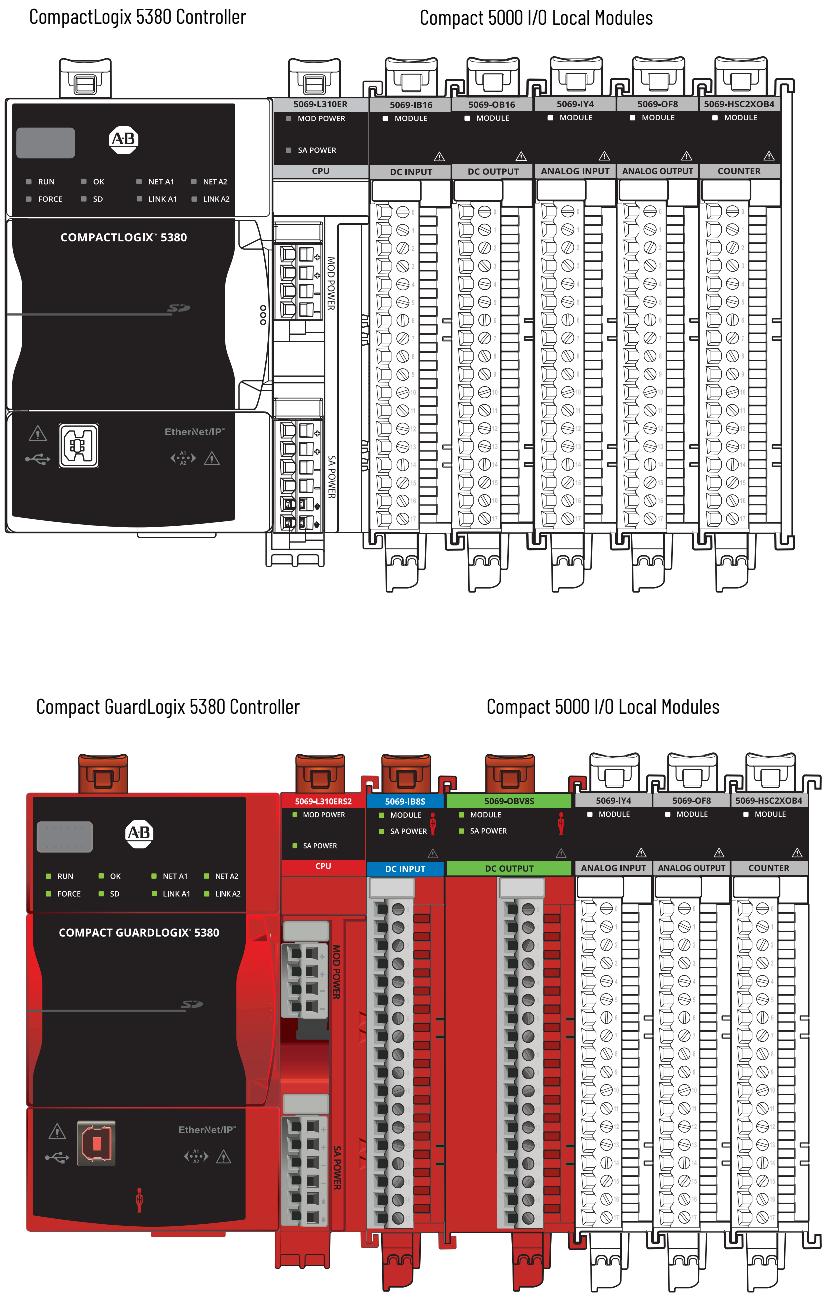
[1] When you use this controller with the Studio 5000 Logix Designer® application, version 29.00.00, the application limits the number of local I/O modules in the project to 16. For more information, see the Knowledgebase Article*5380 CompactLogix controllers limited to 16 local Compact 5000 I/O modules in V29 of Studio 5000.®* With the Logix Designer application, version 30.00.00 or later, the controller supports as many as 31 local I/O modules.

The following are some of the factors to consider when you decide how to use local I/O modules in a CompactLogix 5380 system:

- Number of local I/O modules that the controller supports
- Features available on different modules, for example, sequence of events per point timestamping on only some Compact 5000 I/O digital input modules
- I/O module power usage, including MOD power and SA power

For more information on Compact 5000 I/O modules, see Additional Resources on page 11.

Figure 35 - CompactLogix 5380 and Compact GuardLogix 5380 Systems



Add Local I/O Modules to a Project

Before you can add local I/O modules to a Logix Designer application project, you must open an existing project or create a project. For information on how to create a project, see Create a Logix Designer Application Project on page 65.

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

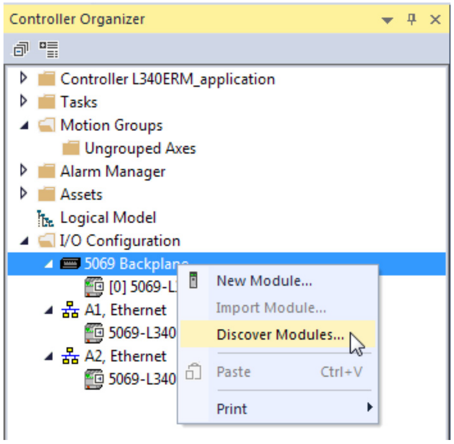
- Discover Modules
- New Module

Discover Modules

The Discover Modules feature is useful when I/O modules are already installed and you can connect the Logix Designer application to the controller.

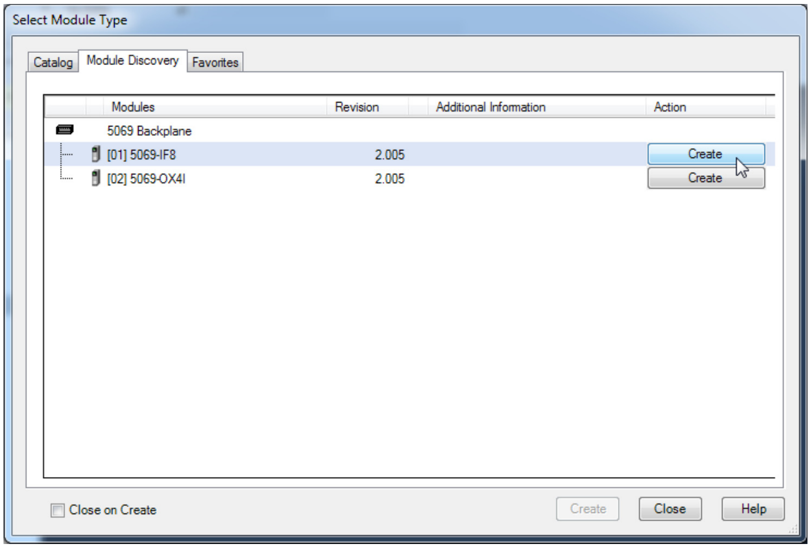
To discover a local I/O module, complete these steps.

1. Go online with your Logix Designer application.
2. Right-click 5069 Backplane and choose Discover Modules.



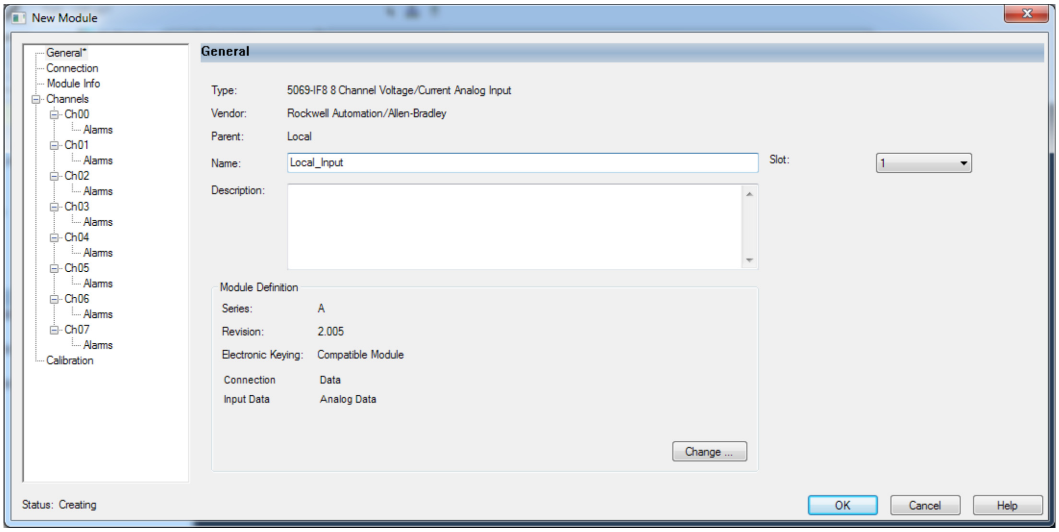
The Logix Designer application automatically detects available modules that are installed in the system.

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



Modules	Revision	Additional Information	Action
5069 Backplane			
[01] 5069-IF8	2.005		Create
[02] 5069-OX4I	2.005		Create

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



General

Type: 5069-IF8 8 Channel Voltage/Current Analog Input

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name: Local_Input

Slot: 1

Description:

Module Definition

Series: A

Revision: 2.005

Electronic Keying: Compatible Module

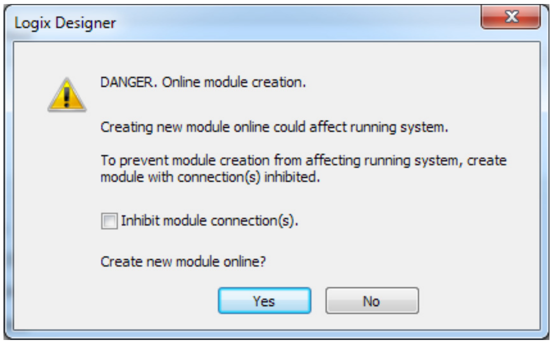
Connection: Data

Input Data: Analog Data

Status: Creating

5. When the following warning message appears, choose whether to inhibit the module connection, and then click Yes.

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



DANGER. Online module creation.

Creating new module online could affect running system.

To prevent module creation from affecting running system, create module with connection(s) inhibited.

□ Inhibit module connection(s).

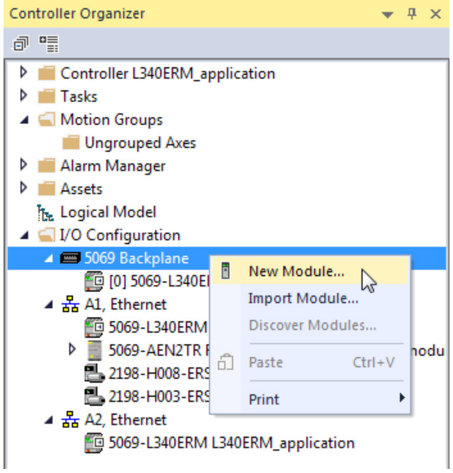
Create new module online?

New Module

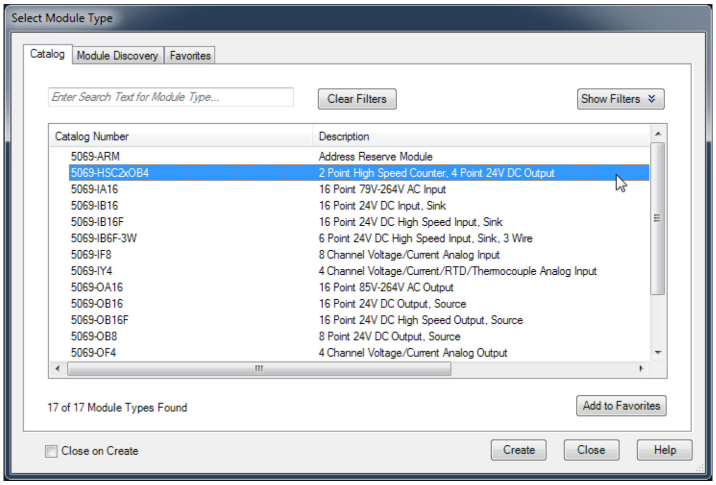
You can add a standard I/O module offline or online. If you do not have physical I/O installed, or you cannot connect to the controller, this is the easiest method to add I/O.

To add a local I/O module, complete these steps.

1. Right-click 5069 Backplane and select New Module.



2. Select the module to add and click Create to open the New Module dialog box.

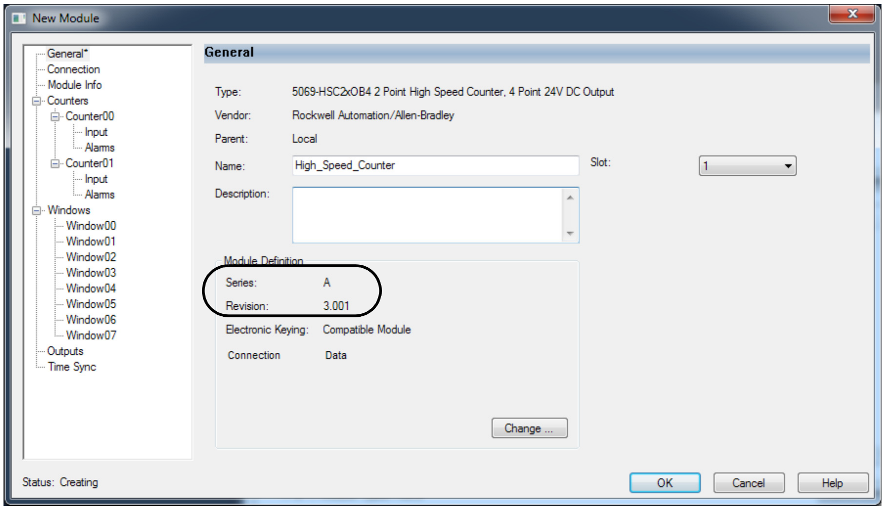


Catalog Number	Description
5069-ARM	Address Reserve Module
5069-HSC2xOB4	2 Point High Speed Counter, 4 Point 24V DC Output
5069-IA16	16 Point 79V-264V AC Input
5069-IB16	16 Point 24V DC Input, Sink
5069-IB16F	16 Point 24V DC High Speed Input, Sink
5069-IB6F-3W	6 Point 24V DC High Speed Input, Sink, 3 Wire
5069-IF8	8 Channel Voltage/Current Analog Input
5069-IY4	4 Channel Voltage/Current/RTD/Thermocouple Analog Input
5069-OA16	16 Point 85V-264V AC Output
5069-OB16	16 Point 24V DC Output, Source
5069-OB16F	16 Point 24V DC High Speed Output, Source
5069-OB8	8 Point 24V DC Output, Source
5069-OF4	4 Channel Voltage/Current Analog Output

17 of 17 Module Types Found

3. On the General tab, set the Series and Revision parameters.

IMPORTANT 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.



General

Type: 5069-HSC2xOB4 2 Point High Speed Counter, 4 Point 24V DC Output

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name: High_Speed_Counter

Slot: 1

Description:

Module Definition

Series: A

Revision: 3.001

Electronic Keying: Compatible Module

Connection Data

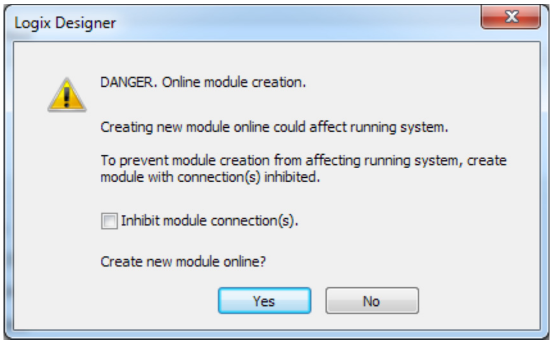
Status: Creating

4. Configure the rest of the module as needed and click OK.

   For information on electronic keying, see Electronic Keying on page 147.

5. If you are online and the following warning appears, choose whether to inhibit the module coonection and then click Yes.

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



DANGER. Online module creation.

Creating new module online could affect running system.

To prevent module creation from affecting running system, create module with connection(s) inhibited.

☐ Inhibit module connection(s).

Create new module online?

6. To add additional local I/O modules:
   - 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.

Electronic Keying

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

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

The following Electronic Keying options are available.

Keying Option	Description
Compatible Module	Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has these characteristics: • Same catalog number • Same or higher Major Revision • Minor Revision as follows: – If the Major Revision is the same, the Minor Revision must be the same or higher. – If the Major Revision is higher, the Minor Revision can be any number.
Disable Keying	Indicates that the keying attributes are not considered when attempting to communicate with a device. With Disable Keying, communication can occur with a device other than the type specified in the project. **ATTENTION**: Be cautious when using Disable Keying; if used incorrectly, this option can lead to personal injury or death, property damage, or economic loss. We **strongly recommend** that you **do not use** Disable Keying. If you use Disable Keying, you must take full responsibility for understanding whether the device being used can fulfill the functional requirements of the application.
Exact Match	Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.

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

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

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

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

Remote I/O Modules

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Remote I/O modules do not reside in the same chassis as the CompactLogix 5380 or Compact GuardLogix 5380 controller. The controller connects to the I/O modules via an EtherNet/IP™ network. The controllers support the use of a wide range of remote I/O modules. For maximum performance, we recommend that you use Compact 5000 I/O modules when you use remote I/O modules.

For example, CompactLogix 5380 and Compact GuardLogix 5380 controllers can connect to following:

- Chassis-based I/O module families, such as Compact 5000 I/O, 1756 ControlLogix® I/O, 1769 Compact I/O™, or 1746 SLC™ I/O modules
- In-cabinet I/O module families, such as 1734 POINT I/O™ or 1794 FLEX™ I/O modules
- On-Machine™ I/O module families, such as 1732E ArmorBlock® I/O modules

IMPORTANT The following network examples are solely intended to show remote I/O modules in various network topologies. The examples do not address network communication rates between the controller and the I/O modules.

We recommend, however, that you consider network communication rates when you determine the best way to incorporate remote I/O modules in your CompactLogix 5380 system.

For more information, see EtherNet/IP Network Communication Rates on page 109.

Figure 36 - Remote I/O Modules in a CompactLogix 5380 System on a DLR Network Topology

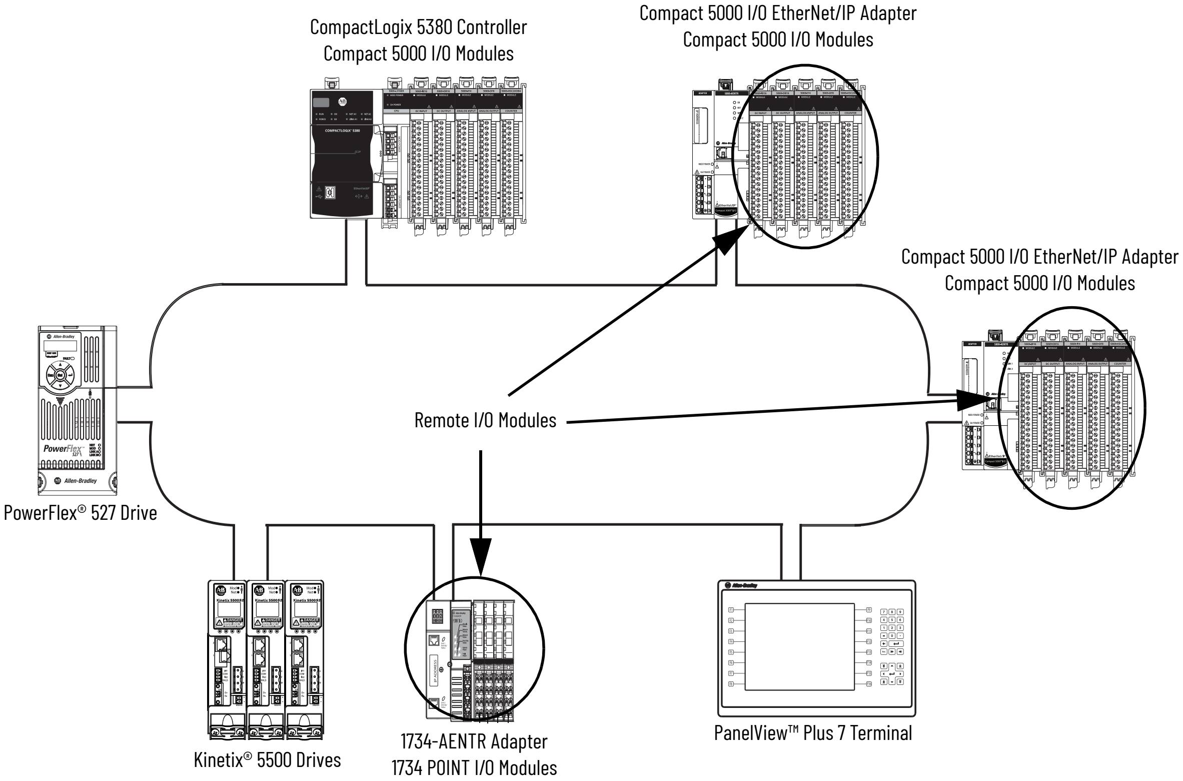


Figure 37 - Remote I/O Modules in a CompactLogix 5380 System on a Linear Network Topology

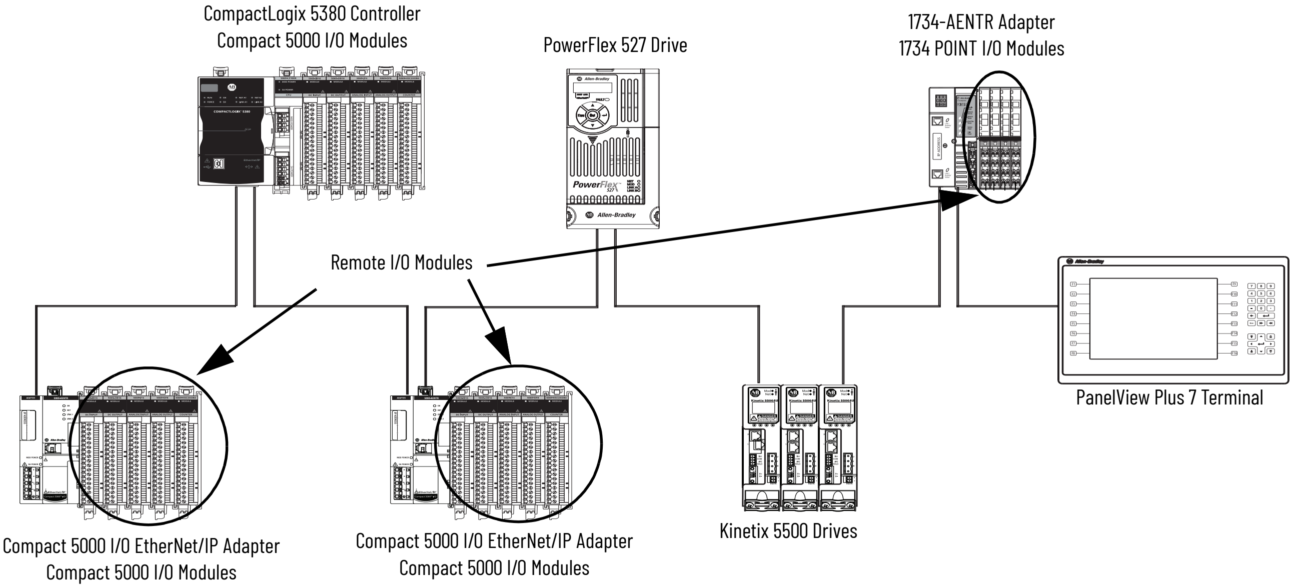
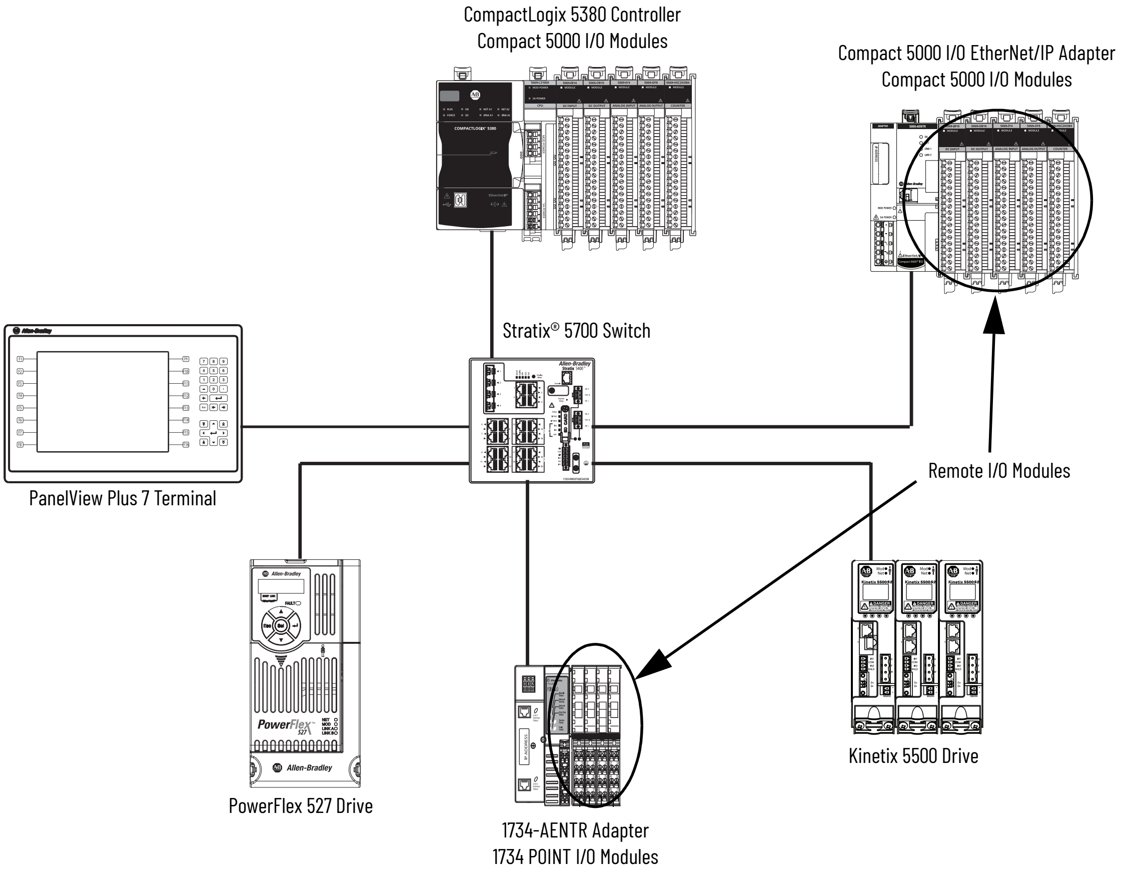


Figure 38 - Remote I/O Modules in a CompactLogix 5380 System on a Star Network Topology



Add Remote I/O Modules to a Project

Before you can add remote I/O modules to a project, you must add the EtherNet/IP communication module that facilitates communication between the controller and the remote I/O modules.

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

- Discover Modules
- New Module

Discover Modules

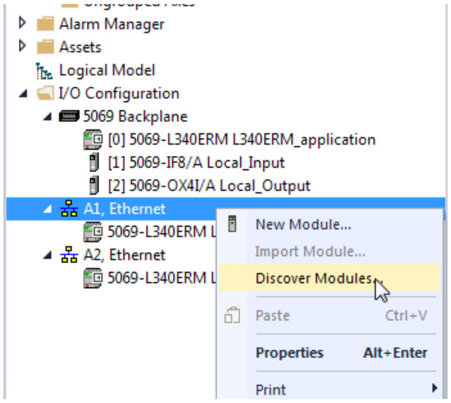
The Discover Modules feature is useful when I/O modules are already installed and connected to the network. When you use Discover Modules to find Ethernet devices, the Logix Designer application browses based on how Ethernet browsing is configured in RSLinx® Classic software.

- If the EtherNet/IP driver is used in RSLinx Classic software, the Logix Designer application automatically detects remote I/O modules.
- If the Ethernet devices driver is used in RSLinx Classic software, you must configure the IP address for each Ethernet device that you want to display in the Select Module Type dialog box that is shown on page 150.
- If the Ethernet bus is browsed via a CIP™ router, you must configure the IP address for each Ethernet device that you want to display in the Select Module Type dialog box that is shown on page 150.

The tasks in this section apply when you use the EtherNet/IP driver in RSWho to browse the network.

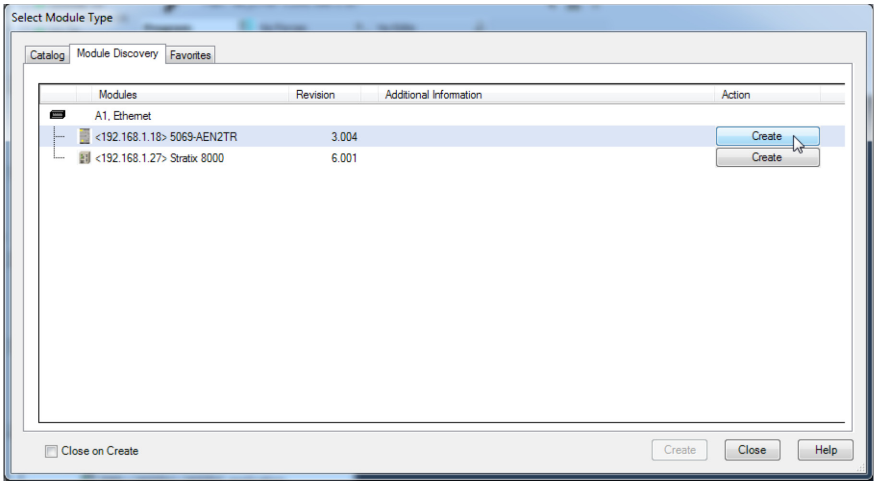
To use Discover Modules to add a remote I/O module, complete these steps.

1. Go online with your Logix Designer application.
2. Right-click Ethernet 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 adapter to your project.

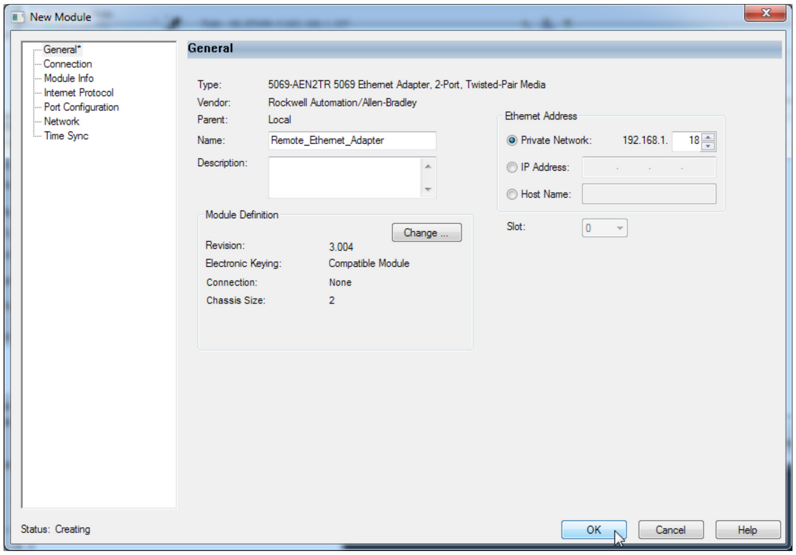


Select Module Type

Modules	Revision	Additional Information	Action
A1, Ethernet			
<192.168.1.18> 5069-AEN2TR	3.004		Create
<192.168.1.27> Stratix 8000	6.001		Create

□ Close on Create

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



New Module

General

Type: 5069-AEN2TR 5069 Ethernet Adapter, 2-Port, Twisted-Pair Media
Vendor: Rockwell Automation/Allen-Bradley
Parent: Local
Name: Remote_Ethernet_Adapter
Description:

Module Definition
Revision: 3.004
Electronic Keying: Compatible Module
Connection: None
Chassis Size: 2

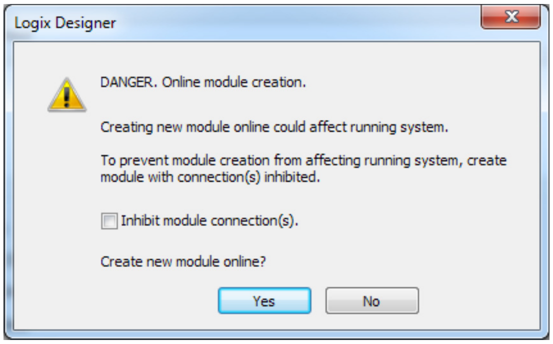
Ethernet Address
● Private Network: 192.168.1. 18
○ IP Address:
○ Host Name:

Slot: 0

Status: Creating

5. At the warning dialog box, click Yes.

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



Logix Designer

DANGER. Online module creation.

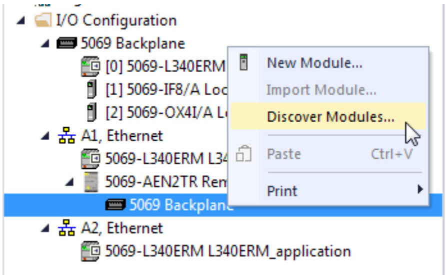
Creating new module online could affect running system.

To prevent module creation from affecting running system, create module with connection(s) inhibited.

□ Inhibit module connection(s).

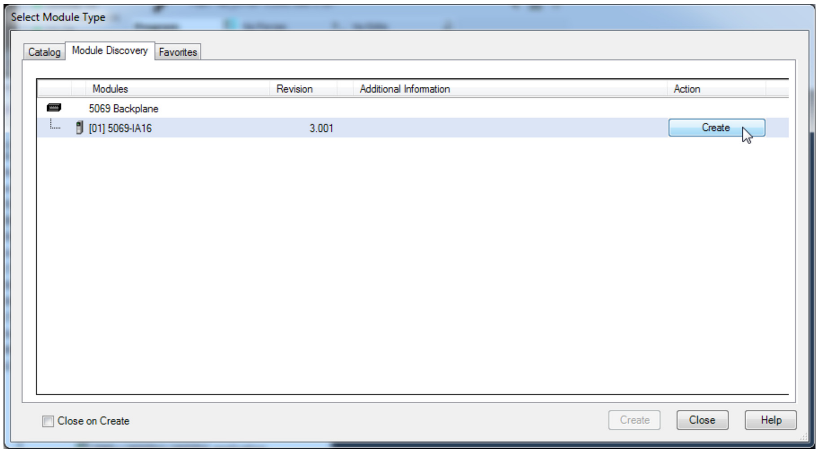
Create new module online?

6. Close the Select Module Type dialog box.
7. Right-click 5069 Backplane and choose Discover Modules.



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

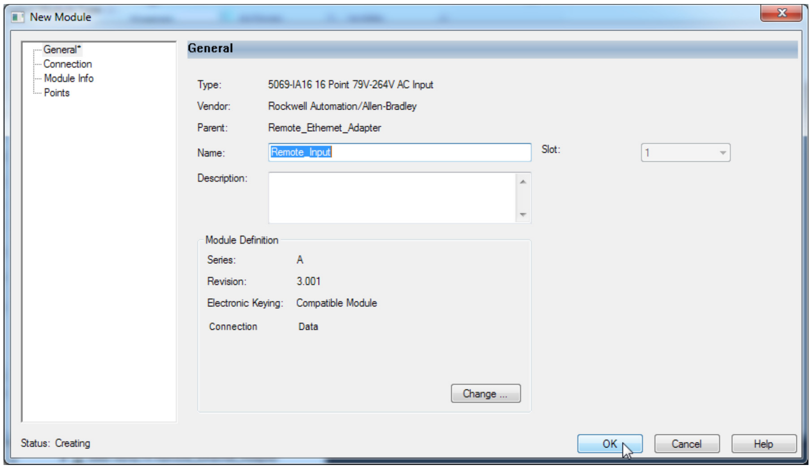
8. At the Select Module Type window, click Create to add a discovered module to your project.



Select Module Type

Modules	Revision	Additional Information	Action
5069 Backplane			
[01] 5069-IA16	3.001		Create

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



New Module

General

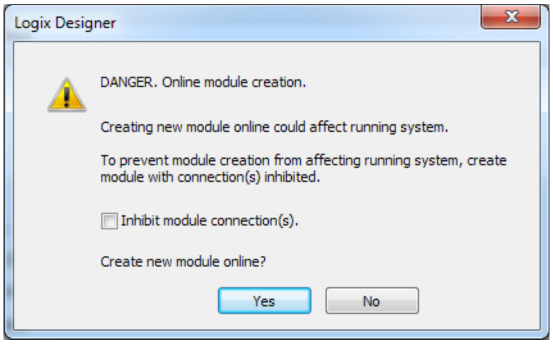
Type: 5069-IA16 16 Point 79V-264V AC Input
Vendor: Rockwell Automation/Allen-Bradley
Parent: Remote_Ethernet_Adapter
Name: Remote_Input
Slot: 1
Description:

Module Definition
Series: A
Revision: 3.001
Electronic Keying: Compatible Module
Connection Data

Status: Creating

10. At the warning dialog box, click Yes.

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



Logix Designer

DANGER. Online module creation.

Creating new module online could affect running system.

To prevent module creation from affecting running system, create module with connection(s) inhibited.

□ Inhibit module connection(s).

Create new module online?

11. Close the Select Module Type dialog box.

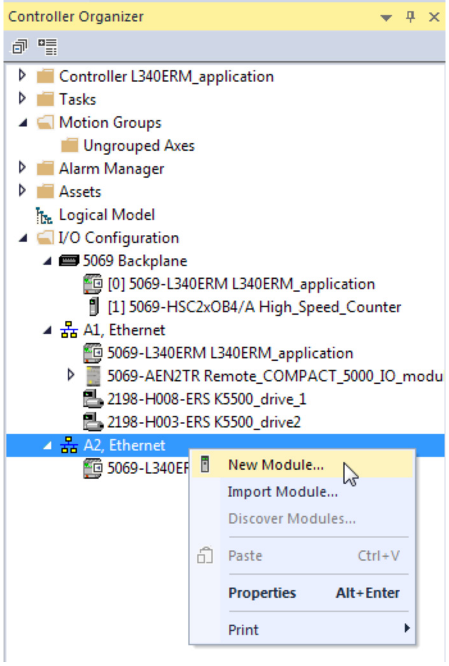
After you add the remote I/O module, consider the following:

- To add remote I/O modules in the same remote location:
  - If you cleared the Close on Create checkbox when you created the first I/O module, repeat steps 8...11.
  - If you did not clear the Close on Create checkbox when you created the first I/O module, repeat steps 7...11.
- To add remote I/O modules in another new remote location, repeat steps 2...11.

New Module

You can add a standard I/O module offline or online. If you do not have physical I/O installed, or you cannot connect to the controller, this is the easiest method to add I/O. To use New Module to add a remote I/O module, complete these steps.

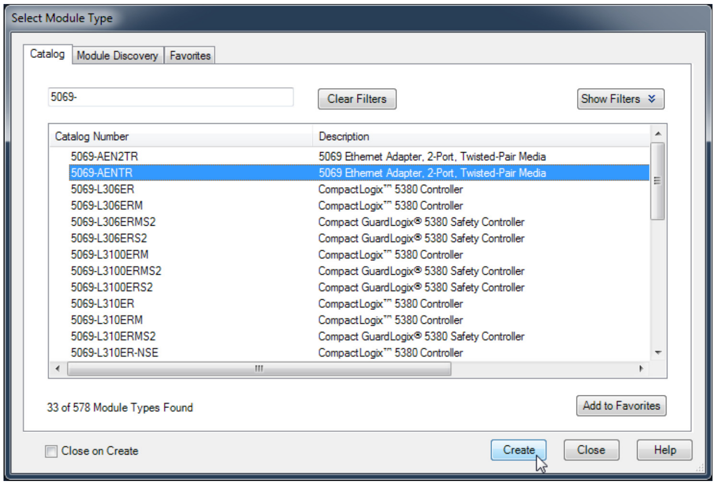
1. Right-click Ethernet and choose New Module.



2. Select the EtherNet/IP adapter and click Create.

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.

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.

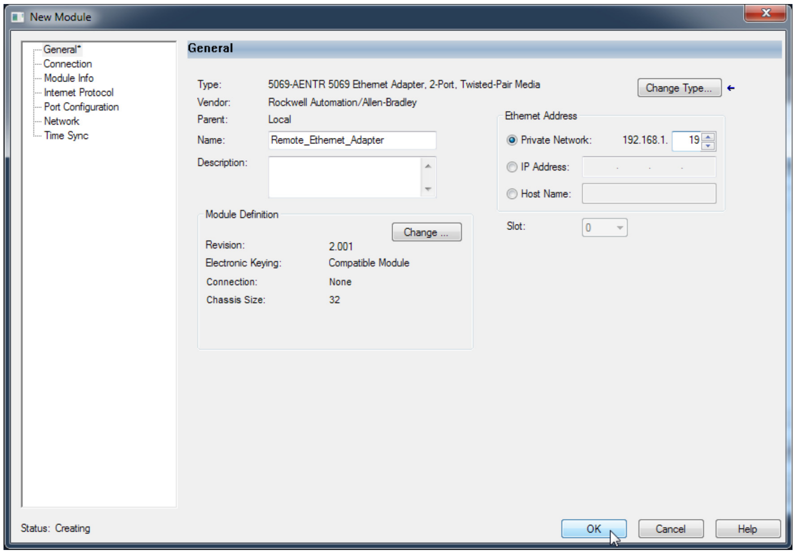


Catalog Number	Description
5069-AEN2TR	5069 Ethernet Adapter, 2-Port, Twisted-Pair Media
5069-AENTR	5069 Ethernet Adapter, 2-Port, Twisted-Pair Media
5069-L306ER	CompactLogix™ 5380 Controller
5069-L306ERM	CompactLogix™ 5380 Controller
5069-L306ERMS2	Compact GuardLogix® 5380 Safety Controller
5069-L306ERS2	Compact GuardLogix® 5380 Safety Controller
5069-L3100ERM	CompactLogix™ 5380 Controller
5069-L3100ERMS2	Compact GuardLogix® 5380 Safety Controller
5069-L3100ERS2	Compact GuardLogix® 5380 Safety Controller
5069-L310ER	CompactLogix™ 5380 Controller
5069-L310ERM	CompactLogix™ 5380 Controller
5069-L310ERMS2	Compact GuardLogix® 5380 Safety Controller
5069-L310ER-NSE	CompactLogix™ 5380 Controller

33 of 578 Module Types Found

□ Close on Create

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



General

Type: 5069-AENTR 5069 Ethernet Adapter, 2-Port, Twisted-Pair Media

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name: Remote_Ethernet_Adapter

Description:

Module Definition

Revision: 2.001

Electronic Keying: Compatible Module

Connection: None

Chassis Size: 32

Ethernet Address

● Private Network: 192.168.1. 19

○ IP Address:

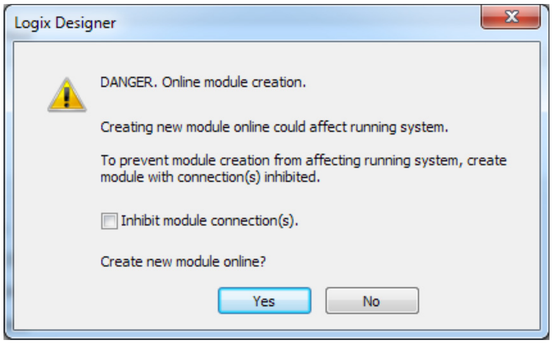
○ Host Name:

Slot: 0

Status: Creating

4. If you add a module while online, then at the warning dialog box, click Yes.

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



DANGER. Online module creation.

Creating new module online could affect running system.

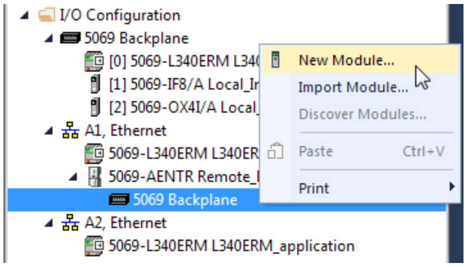
To prevent module creation from affecting running system, create module with connection(s) inhibited.

□ Inhibit module connection(s).

Create new module online?

5. Close the Select Module Type dialog box.

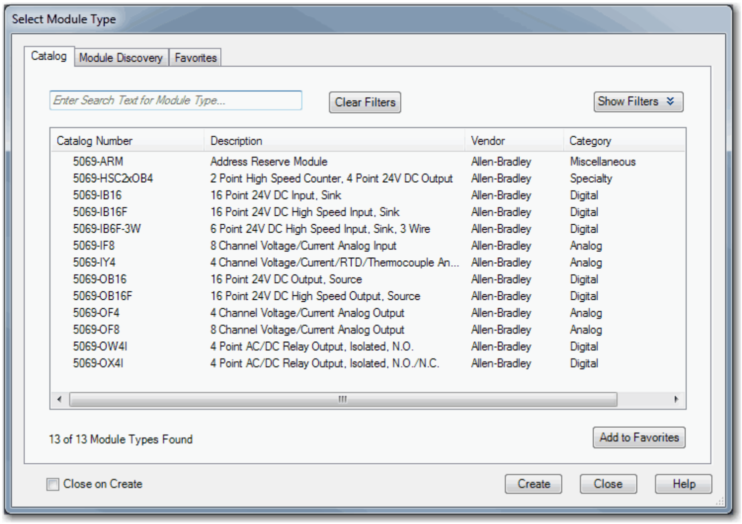
6. Right-click the newly added EtherNet/IP communication module or the backplane and choose New Module.



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

   If you must add multiple I/O modules to the same remote location, you can clear the Close on Create checkbox before you click Create to skip step 6.

   When the Close on Create checkbox is cleared, the select Module Type dialog box appears automatically after you complete configuration for an I/O module.

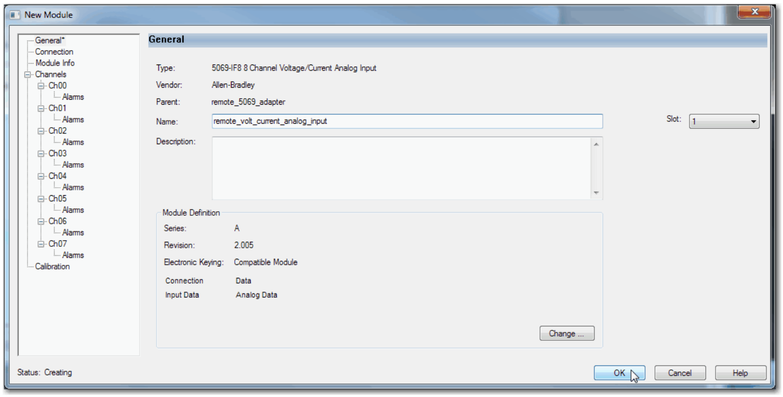


Catalog Number	Description	Vendor	Category
5069-ARM	Address Reserve Module	Allen-Bradley	Miscellaneous
5069-HSC2xOB4	2 Point High Speed Counter, 4 Point 24V DC Output	Allen-Bradley	Specialty
5069-IB16	16 Point 24V DC Input, Sink	Allen-Bradley	Digital
5069-IB16F	16 Point 24V DC High Speed Input, Sink	Allen-Bradley	Digital
5069-IB6F-3W	6 Point 24V DC High Speed Input, Sink, 3 Wire	Allen-Bradley	Digital
5069-IF8	8 Channel Voltage/Current Analog Input	Allen-Bradley	Analog
5069-IY4	4 Channel Voltage/Current/RTD/Thermocouple An...	Allen-Bradley	Analog
5069-OB16	16 Point 24V DC Output, Source	Allen-Bradley	Digital
5069-OB16F	16 Point 24V DC High Speed Output, Source	Allen-Bradley	Digital
5069-OF4	4 Channel Voltage/Current Analog Output	Allen-Bradley	Analog
5069-OF8	8 Channel Voltage/Current Analog Output	Allen-Bradley	Analog
5069-OW4I	4 Point AC/DC Relay Output, Isolated, N.O.	Allen-Bradley	Digital
5069-OX4I	4 Point AC/DC Relay Output, Isolated, N.O./N.C.	Allen-Bradley	Digital

13 of 13 Module Types Found

□ Close on Create

8. On the New Module dialog box, configure the I/O module and then click OK.



Type: 5069-IF8 8 Channel Voltage/Current Analog Input

Vendor: Allen-Bradley

Parent: remote_5069_adapter

Name: remote_volt_current_analog_input

Slot: 1

Description:

Module Definition

Series: A

Revision: 2.005

Electronic Keying: Compatible Module

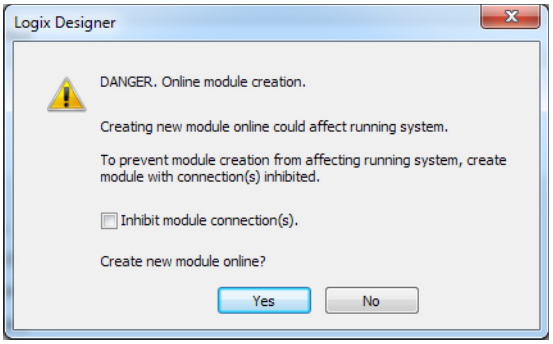
Connection Data

Input Data Analog Data

Status: Creating

9. If you add a module while online, choose whether to inhibit the module connection, and then click Yes.

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



DANGER. Online module creation.

Creating new module online could affect running system.

To prevent module creation from affecting running system, create module with connection(s) inhibited.

□ Inhibit module connection(s).

Create new module online?

After you add the remote I/O module, consider the following:

- To add remote I/O modules in the same remote location:
  - If you cleared the Close on Create checkbox when you created the first I/O module, repeat steps 7...8.
  - If you did not clear the Close on Create checkbox when you created the first I/O module, repeat steps 6...8.
- To add remote I/O modules in another new remote location, repeat steps 1....

Add to the I/O Configuration While Online

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can add local and remote I/O modules and other devices to the controller configuration while the project is online.

IMPORTANT	To add I/O modules when the controller is online, the controller mode switch must be in the REM or PROG position. The Compact 5000 I/O modules must already be installed in the system. You cannot install Compact 5000 I/O modules when the system is powered.

The modules and devices you can add while online depends on the software version that you use. 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

For more information about how to add 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 CompactLogix 5380 or Compact GuardLogix 5380 controller I/O configuration while online with Logix Designer, version 28 or later.

- Compact 5000 I/O modules - As local or remote I/O modules
- Compact 5000 I/O EtherNet/IP adapters
- 1756 ControlLogix EtherNet/IP modules
- 1756 ControlLogix I/O modules

IMPORTANT	These modules **cannot** be added while online: • 1756 ControlLogix Motion modules (1756-M02AE, 1756-HYD02, 1756-M02AS, 1756-M03SE, 1756-M08SE, 1756-M08SEG, 1756-M16SE) • ControlLogix 1756-RIO • ControlLogix 1756-SYNCH • Safety I/O

Determine When Data Is Updated

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

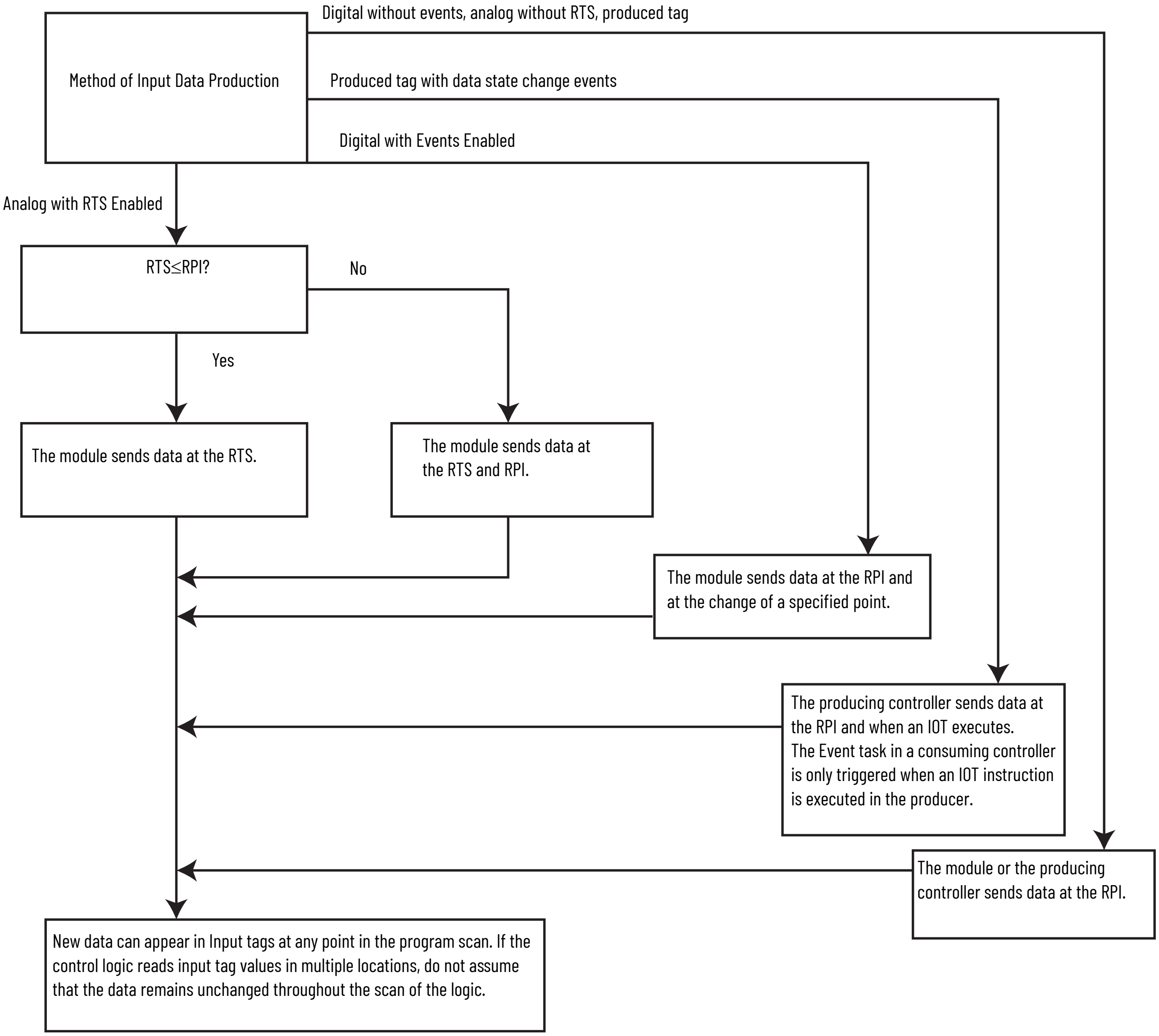
CompactLogix 5380 and Compact GuardLogix 5380 controllers update data asynchronously with the execution of logic. See these flowcharts to determine when a controller, input module, or bridge sends data:

- Input Data Update Flowchart
- Output Data Update Flowchart

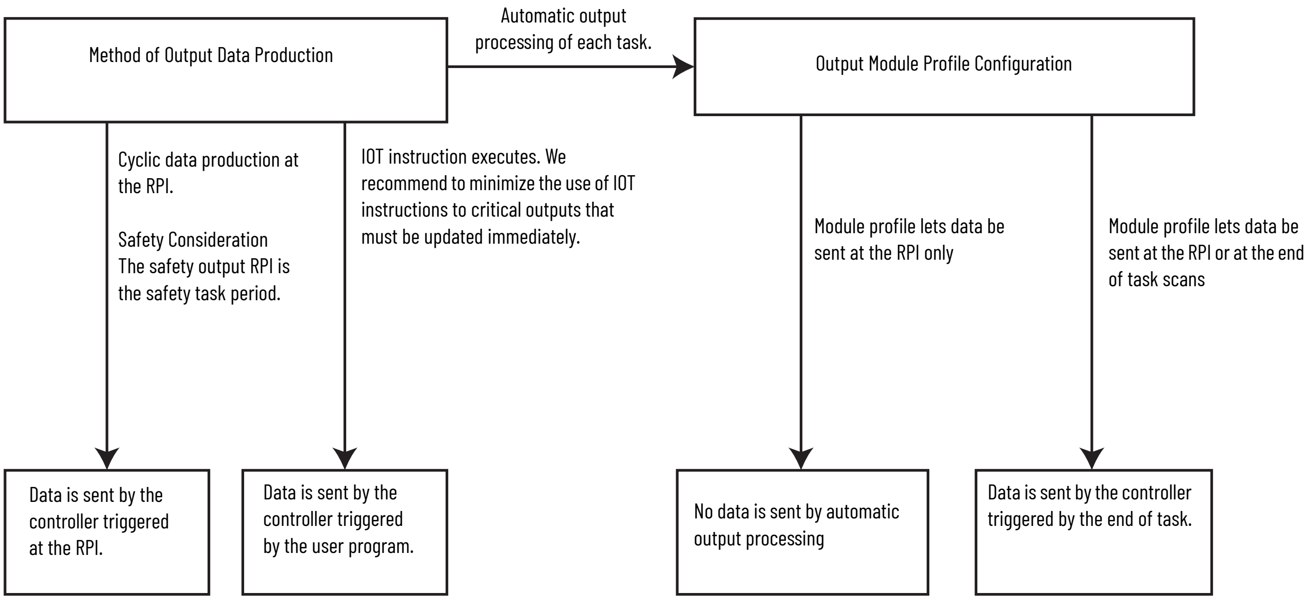
Input Data Update Flowchart

IMPORTANT Safety Consideration

Compact GuardLogix standard inputs are updated just like CompactLogix standard inputs, but Compact GuardLogix safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution. For more information, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.


Method of Input Data Production
Digital without events, analog without RTS, produced tag
Produced tag with data state change events
Digital with Events Enabled
Analog with RTS Enabled
RTS≤RPI?
No
Yes
The module sends data at the RTS.
The module sends data at the RTS and RPI.
The module sends data at the RPI and at the change of a specified point.
The producing controller sends data at the RPI and when an IOT executes.
The Event task in a consuming controller is only triggered when an IOT instruction is executed in the producer.
The module or the producing controller sends data at the RPI.
New data can appear in Input tags at any point in the program scan. If the control logic reads input tag values in multiple locations, do not assume that the data remains unchanged throughout the scan of the logic.

Output Data Update Flowchart


Method of Output Data Production
Automatic output processing of each task.
Output Module Profile Configuration
Cyclic data production at the RPI.
Safety Consideration
The safety output RPI is the safety task period.
IOT instruction executes. We recommend to minimize the use of IOT instructions to critical outputs that must be updated immediately.
Module profile lets data be sent at the RPI only
Module profile lets data be sent at the RPI or at the end of task scans
Data is sent by the controller triggered at the RPI.
Data is sent by the controller triggered by the user program.
No data is sent by automatic output processing
Data is sent by the controller triggered by the end of task.

Chapter 12

Safety I/O Devices

Add Safety I/O Devices

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

- Node address for DeviceNet® networks.

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

- IP address for EtherNet/IP networks.
- Safety network number (SNN). To set the SNN, see page 164.
- Configuration signature. For information on when the configuration signature is set automatically and when you must set it, see page 168.
- Reaction time limit. For information on setting the reaction time limit, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.
- Safety input, output, and test parameters complete the device configuration.

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

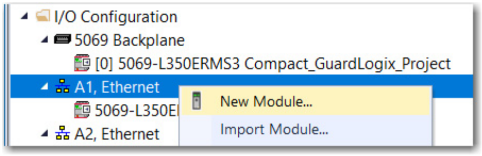
Configure Safety I/O Devices

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

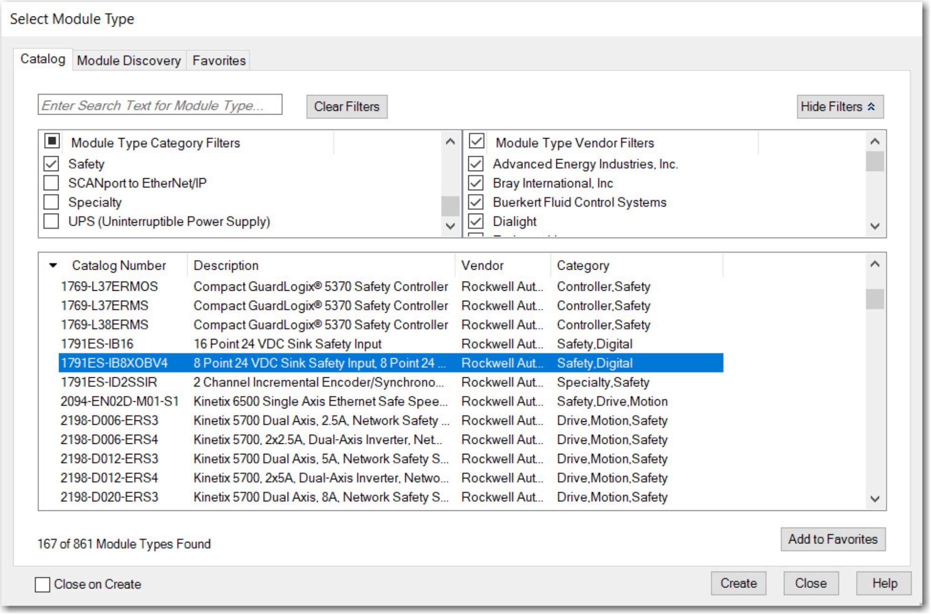
Some safety I/O devices support both standard and safety data. The device definition settings define what data is available.

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



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

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



Select Module Type

■ Module Type Category Filters
☑ Safety
☐ SCANport to EtherNet/IP
☐ Specialty
☐ UPS (Uninterruptible Power Supply)

☑ Module Type Vendor Filters
☑ Advanced Energy Industries, Inc.
☑ Bray International, Inc
☑ Buerkert Fluid Control Systems
☑ Dialight

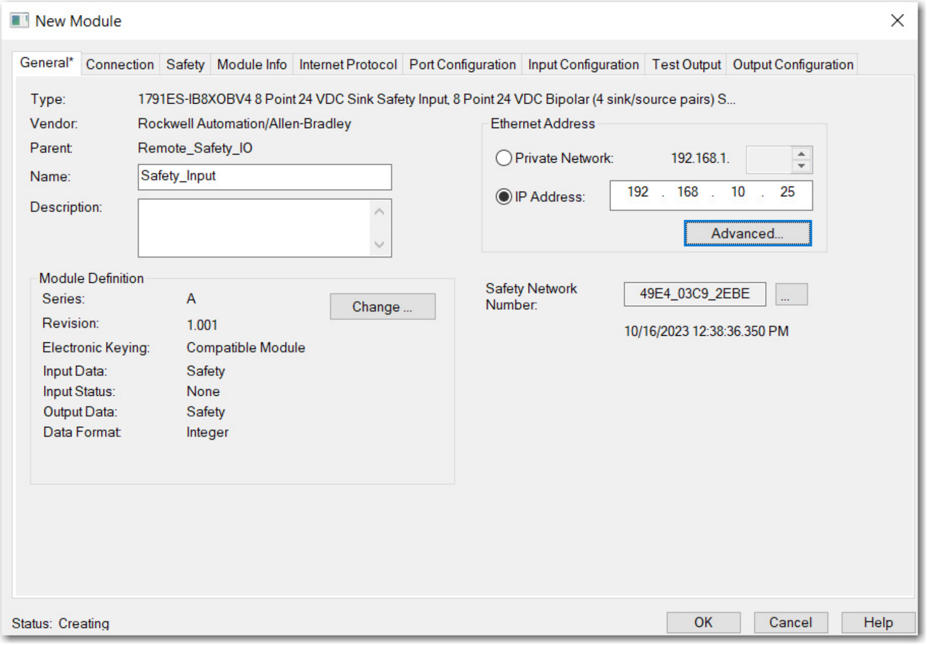
Catalog Number	Description	Vendor	Category
1769-L37ERMOS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety
1769-L37ERMS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety
1769-L38ERMS	Compact GuardLogix® 5370 Safety Controller	Rockwell Aut...	Controller,Safety
1791ES-IB16	16 Point 24 VDC Sink Safety Input	Rockwell Aut...	Safety,Digital
1791ES-IB8XOBV4	8 Point 24 VDC Sink Safety Input, 8 Point 24 ...	Rockwell Aut...	Safety,Digital
1791ES-ID2SSIR	2 Channel Incremental Encoder/Synchrono...	Rockwell Aut...	Specialty,Safety
2094-EN02D-M01-S1	Kinetix 6500 Single Axis Ethernet Safe Spee...	Rockwell Aut...	Safety,Drive,Motion
2198-D006-ERS3	Kinetix 5700 Dual Axis, 2.5A, Network Safety ...	Rockwell Aut...	Drive,Motion,Safety
2198-D006-ERS4	Kinetix 5700, 2x2.5A, Dual-Axis Inverter, Net...	Rockwell Aut...	Drive,Motion,Safety
2198-D012-ERS3	Kinetix 5700 Dual Axis, 5A, Network Safety S...	Rockwell Aut...	Drive,Motion,Safety
2198-D012-ERS4	Kinetix 5700, 2x5A, Dual-Axis Inverter, Netwo...	Rockwell Aut...	Drive,Motion,Safety
2198-D020-ERS3	Kinetix 5700 Dual Axis, 8A, Network Safety S...	Rockwell Aut...	Drive,Motion,Safety

167 of 861 Module Types Found

☐ Close on Create

3. Enter a name and IP address for the new device.

   If your network uses network address translation (NAT), see Using Network Address Translation (NAT) with CIP Safety Devices on page 163.



New Module

Type: 1791ES-IB8XOBV4 8 Point 24 VDC Sink Safety Input, 8 Point 24 VDC Bipolar (4 sink/source pairs) S...

Vendor: Rockwell Automation/Allen-Bradley

Parent: Remote_Safety_IO

Name: Safety_Input

Description:

Ethernet Address

○ Private Network: 192.168.1.

● IP Address: 192 . 168 . 10 . 25

Module Definition

Series: A

Revision: 1.001

Electronic Keying: Compatible Module

Input Data: Safety

Input Status: None

Output Data: Safety

Data Format: Integer

Safety Network Number: 49E4_03C9_2EBE

10/16/2023 12:38:36.350 PM

Status: Creating

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

IMPORTANT	For safety I/O devices, do not use Disable Keying. See Electronic Keying on page 147.

5. To modify the safety network number, click the ... button.

   See Set the SNN of a Safety I/O Device on page 164.

6. Set the connection reaction time limit on the Safety tab.

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

7. To complete the configuration of the safety I/O device, refer to the user documentation and the Logix Designer online help.

Using Network Address Translation (NAT) with CIP Safety Devices

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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

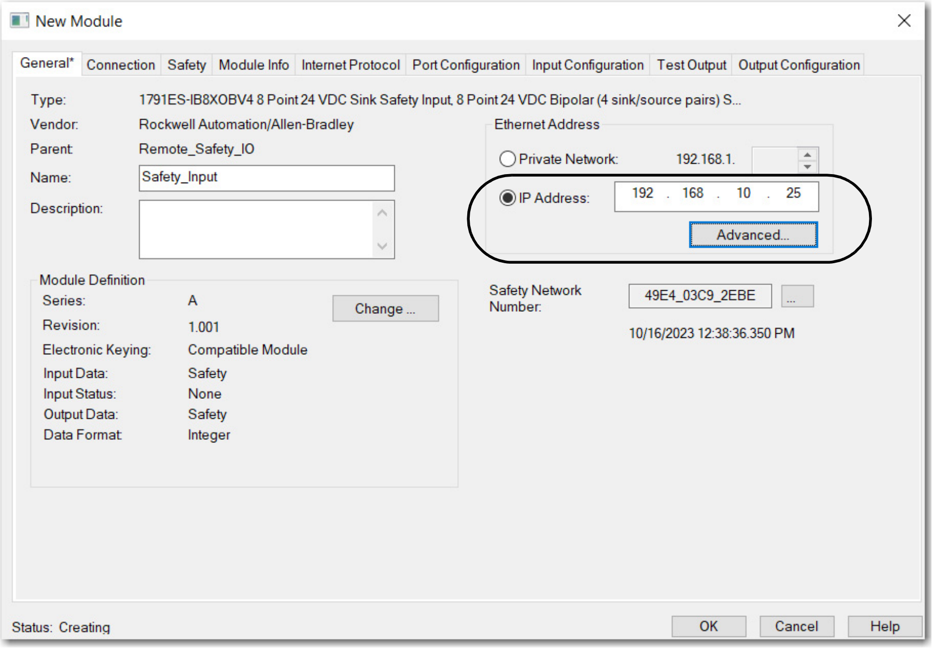
This section only applies to safety users where the controller and the devices it talks to are on separate sides of the NAT-configured router or switch.

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

If you 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.



Type: 1791ES-IB8XOBV4 8 Point 24 VDC Sink Safety Input, 8 Point 24 VDC Bipolar (4 sink/source pairs) S...
Vendor: Rockwell Automation/Allen-Bradley
Parent: Remote_Safety_IO
Name: Safety_Input
Description:

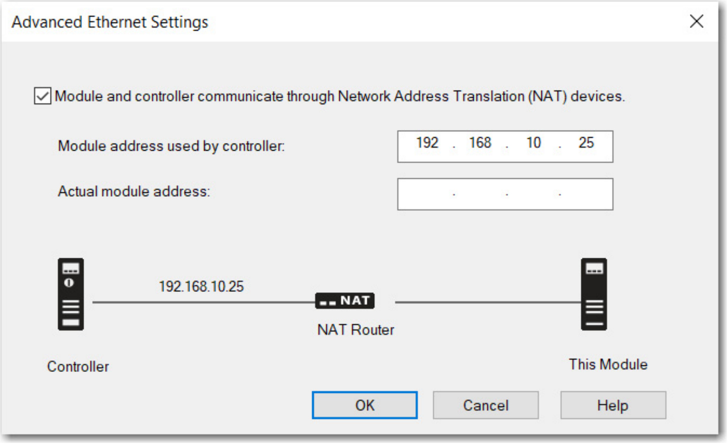
○ Private Network: 192.168.1.
● IP Address: 192 . 168 . 10 . 25

Series: A
Revision: 1.001
Electronic Keying: Compatible Module
Input Data: Safety
Input Status: None
Output Data: Safety
Data Format: Integer

Safety Network Number: 49E4_03C9_2EBE
10/16/2023 12:38:36.350 PM

Status: Creating

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



Advanced Ethernet Settings

☑ Module and controller communicate through Network Address Translation (NAT) devices.

Module address used by controller: 192 . 168 . 10 . 25

Actual module address: . . .

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

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

5. Click OK.

Set the SNN of a Safety I/O Device

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

A time-based SNN is automatically assigned when you add the first safety I/O device on the network. This does not apply to the controller backplane or Ethernet ports 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.

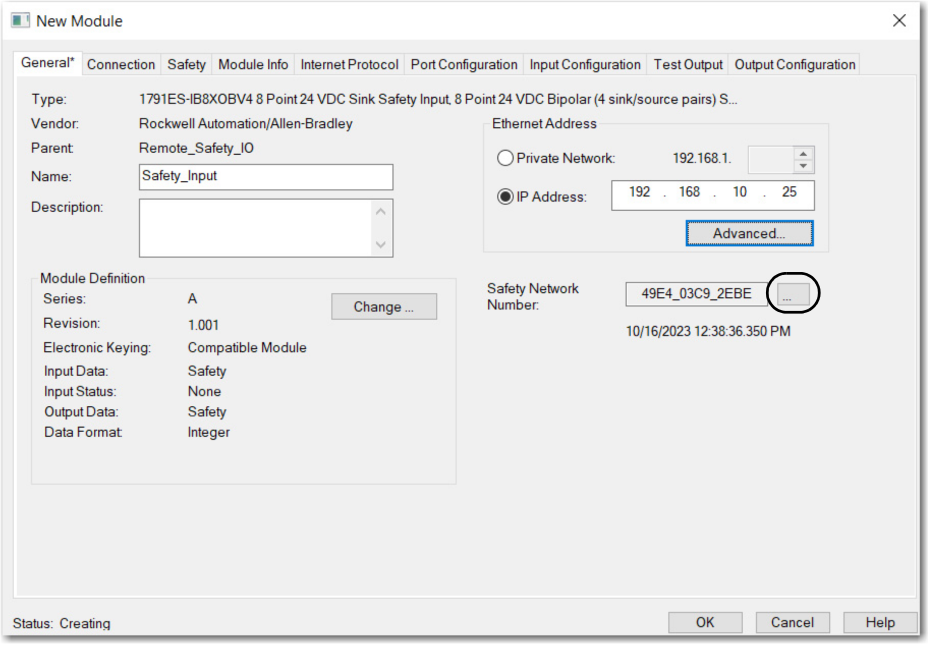
If your application requires you to manually assign the SNN of safety I/O devices, you only have to assign the SNN of the first safety I/O device you add in a remote network or backplane. Logix Designer then assigns the SNN of the first device to any additional devices that you add to that same remote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

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

Change a Safety I/O device SNN

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

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



Type: 1791ES-IB8XOBV4 8 Point 24 VDC Sink Safety Input, 8 Point 24 VDC Bipolar (4 sink/source pairs) S...
Vendor: Rockwell Automation/Allen-Bradley
Parent: Remote_Safety_IO
Name: Safety_Input
Description:

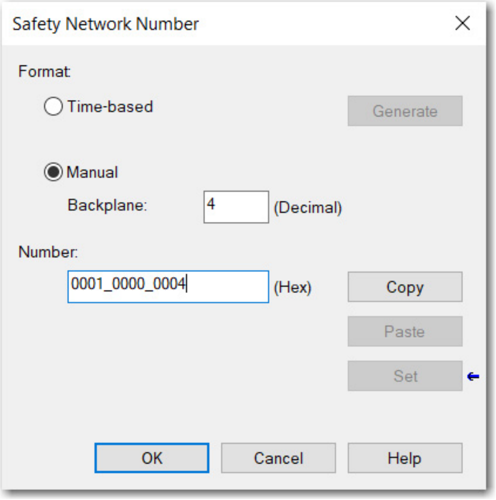
Module Definition
Series: A
Revision: 1.001
Electronic Keying: Compatible Module
Input Data: Safety
Input Status: None
Output Data: Safety
Data Format: Integer

Ethernet Address
○ Private Network: 192.168.1.
● IP Address: 192 . 168 . 10 . 25

Safety Network Number: 49E4_03C9_2EBE
10/16/2023 12:38:36.350 PM

Status: Creating

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



Format:
○ Time-based
● Manual
Backplane: 4 (Decimal)
Number: 0001_0000_0004 (Hex)

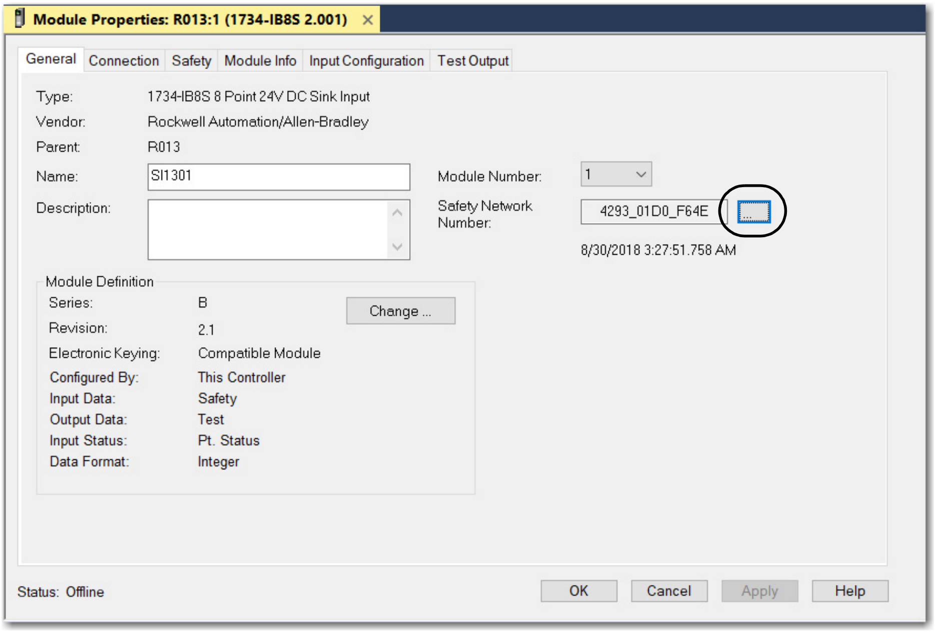
6. On the New Module dialog box, click OK.

Copy and Paste a Safety I/O Device SNN

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

Copy an SNN

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



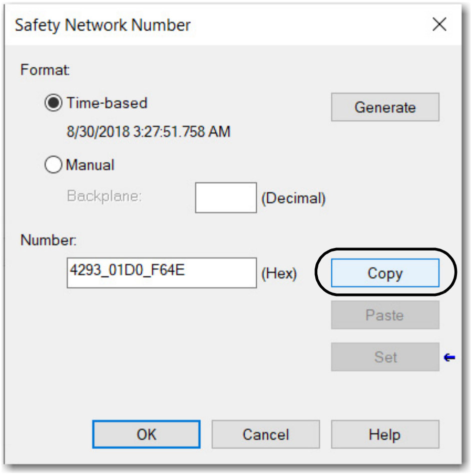
Module Properties: R013:1 (1734-IB8S 2.001)

Type: 1734-IB8S 8 Point 24V DC Sink Input
Vendor: Rockwell Automation/Allen-Bradley
Parent: R013
Name: SI1301
Description:
Module Number: 1
Safety Network Number: 4293_01D0_F64E
8/30/2018 3:27:51.758 AM

Module Definition
Series: B
Revision: 2.1
Electronic Keying: Compatible Module
Configured By: This Controller
Input Data: Safety
Output Data: Test
Input Status: Pt. Status
Data Format: Integer

Status: Offline

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

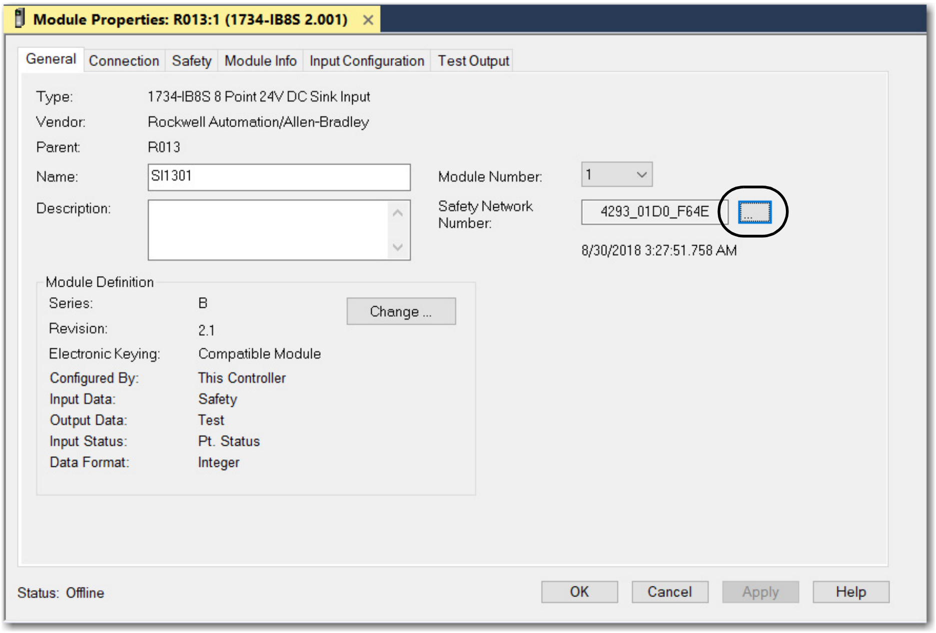


Safety Network Number

Format:
● Time-based
8/30/2018 3:27:51.758 AM
○ Manual
Backplane: (Decimal)
Number:
4293_01D0_F64E (Hex)

Paste an SNN

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



Module Properties: R013:1 (1734-IB8S 2.001)

Type: 1734-IB8S 8 Point 24V DC Sink Input

Vendor: Rockwell Automation/Allen-Bradley

Parent: R013

Name: SI1301

Description:

Module Number: 1

Safety Network Number: 4293_01D0_F64E

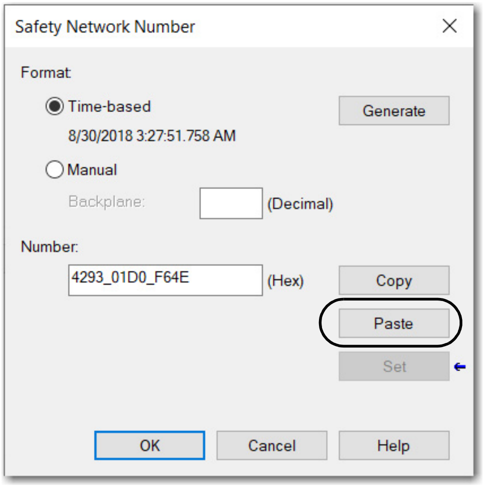
8/30/2018 3:27:51.758 AM

Module Definition

Series:	B
Revision:	2.1
Electronic Keying:	Compatible Module
Configured By:	This Controller
Input Data:	Safety
Output Data:	Test
Input Status:	Pt. Status
Data Format:	Integer

Status: Offline

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



Safety Network Number

Format:

● Time-based

8/30/2018 3:27:51.758 AM

○ Manual

Backplane: (Decimal)

Number:

4293_01D0_F64E (Hex)

Safety I/O Device Signature

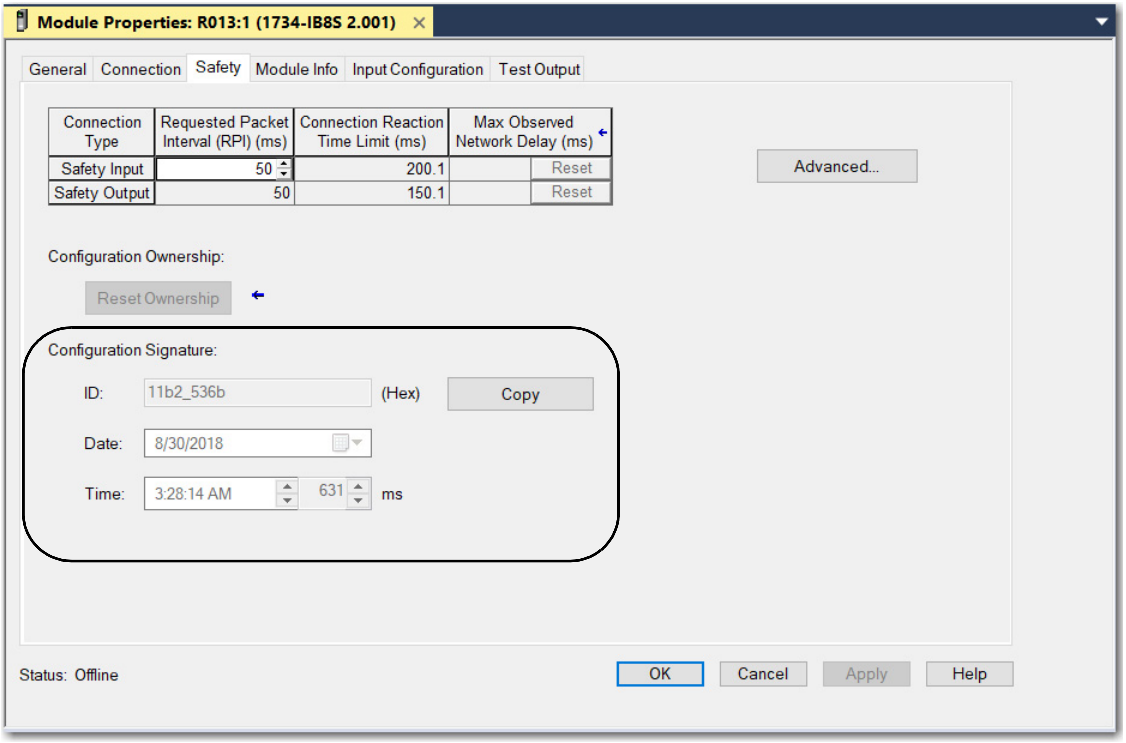
Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

Configuration via the Logix Designer Application

When the I/O device is configured via the Logix Designer application, the configuration signature is generated automatically. You can view and copy the configuration signature via the Safety tab of the device properties.

Figure 39 - View and Copy the Configuration Signature



Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)
Safety Input	50	200.1	Reset
Safety Output	50	150.1	Reset

Configuration Ownership:

Configuration Signature:

ID: 11b2_536b (Hex)

Date: 8/30/2018

Time: 3:28:14 AM 631 ms

Status: Offline

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

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

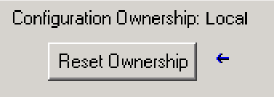
When the controller project is online, the Safety tab of the device properties displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the SNN and node address or slot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

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

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

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

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



Configuration Ownership: Local

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

I/O Device Address Format

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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

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

Table 22 - Safety I/O Device Address Format

Where	Is	
devicename	The name of the safety I/O device	
Type	Type of data	Input: I Output: O
Member	Specific data from the I/O device	
	Input-only device	devicename:I.RunMode[1] devicename:I.ConnectionFaulted[1] devicename:I.Input Members
	Output-only device	devicename:I.RunMode[1] devicename:I.ConnectionFaulted[1] devicename:O.Output Members
	Combination I/O	devicename:I.RunMode[1] devicename:I.ConnectionFaulted[1] devicename:I.Input Members devicename:O.Output Members

[1] This member is required.

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

Monitor Safety I/O Device Status

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

Replace a Safety I/O Device

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

Configuration Ownership

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

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

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

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

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™ device on a DeviceNet network, your choice depends on the type of device.

Table 23 - 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 device via a 1788-EN2DN linking device	Logix Designer application	Below
1734 POINT Guard I/O™ device via a 1788-EN2DN linking device and a 1734-PDN adapter	RSNetWorx™ for DeviceNet software	See the POINT Guard I/O Safety devices User Manual, publication 1734-UM013.

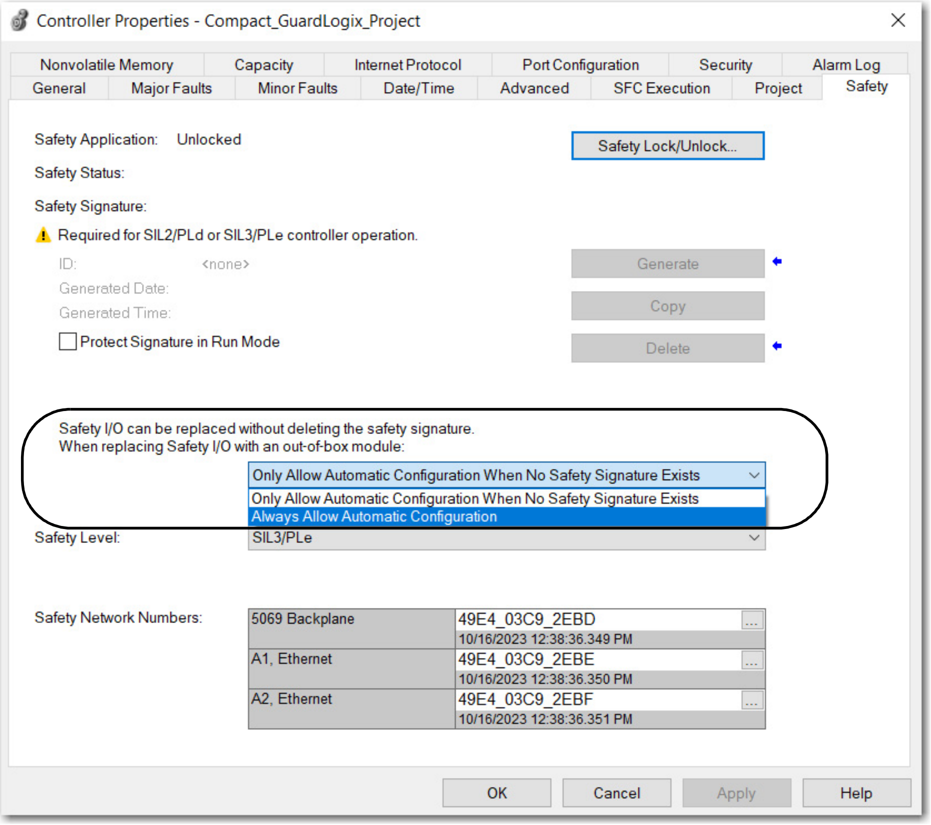
- If you are relying on a portion of the CIP Safety system to maintain SIL or PL-rated behavior during device replacement and functional testing, the Always Allow Automatic Configuration option cannot be used.

  For more information, see Only Allow Automatic Configuration When No Safety Signature Exists on page 172.
- If the entire routable CIP Safety control system is not being relied on to maintain SIL or PL-rated behavior during the replacement and functional testing of a device, the Always Allow Automatic Configuration option can be used.

  For more information, see Always Allow Automatic Configuration on page 175.

Safety I/O device replacement is configured on the Safety tab of the Controller Properties dialog box.

Figure 40 - Safety I/O Device Replacement



Controller Properties - Compact_GuardLogix_Project

Safety Application: Unlocked

Safety Status:

Safety Signature:

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

ID: <none>

Generated Date:

Generated Time:

□ Protect Signature in Run Mode

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

Only Allow Automatic Configuration When No Safety Signature Exists
- Only Allow Automatic Configuration When No Safety Signature Exists
- Always Allow Automatic Configuration

Safety Level: SIL3/PLe

Safety Network Numbers:

5069 Backplane	49E4_03C9_2EBD 10/16/2023 12:38:36.349 PM
A1, Ethernet	49E4_03C9_2EBE 10/16/2023 12:38:36.350 PM
A2, Ethernet	49E4_03C9_2EBF 10/16/2023 12:38:36.351 PM

Only Allow Automatic Configuration When No Safety Signature Exists

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

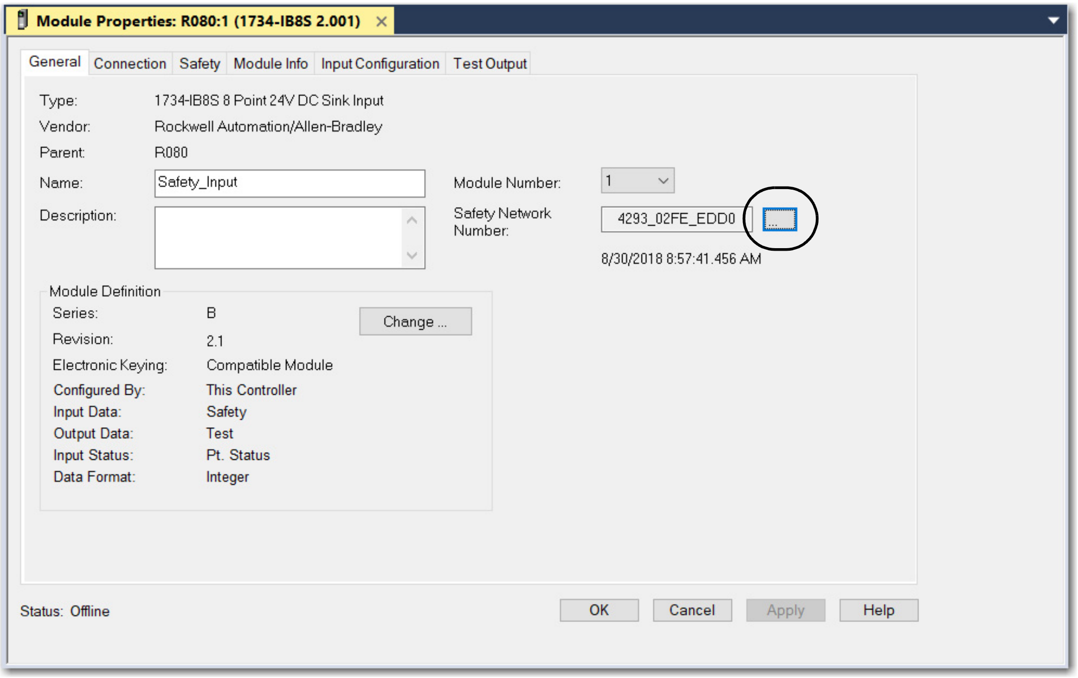
If you select the Only Allow Automatic Configuration When No Safety Signature Exists option, follow the guidance in Table 24 to replace a safety I/O device based on your scenario. After you complete the steps, the DeviceID matches the original and enables the safety controller to download the proper device configuration and re-establish the safety connection.

Table 24 - Replace a Device

Safety Signature Exists	Replacement Device Condition	Action Required
No	No SNN (out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (out-of-box)	See Scenario 1—Replacement Device Is Out-of-box and Safety Signature Exists on page 172.
Yes	Different SNN from original safety task configuration	See Scenario 2—Replacement Device SNN Is Different from Original and Safety Signature Exists on page 173.
No		See Scenario 3—Replacement Device SNN Is Different from Original and No Safety Signature Exists on page 175.

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



Module Properties: R080:1 (1734-IB8S 2.001)

Type: 1734-IB8S 8 Point 24V DC Sink Input

Vendor: Rockwell Automation/Allen-Bradley

Parent: R080

Name: Safety_Input

Description:

Module Number: 1

Safety Network Number: 4293_02FE_EDD0

8/30/2018 8:57:41.456 AM

Module Definition

Series: B

Revision: 2.1

Electronic Keying: Compatible Module

Configured By: This Controller

Input Data: Safety

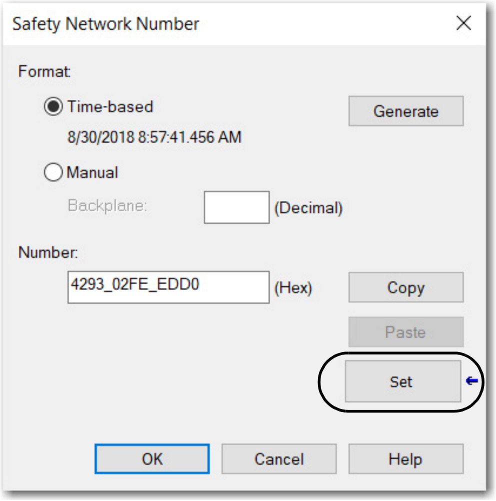
Output Data: Test

Input Status: Pt. Status

Data Format: Integer

Status: Offline

4. Click Set.



Safety Network Number

Format:

● Time-based

8/30/2018 8:57:41.456 AM

○ Manual

Backplane: (Decimal)

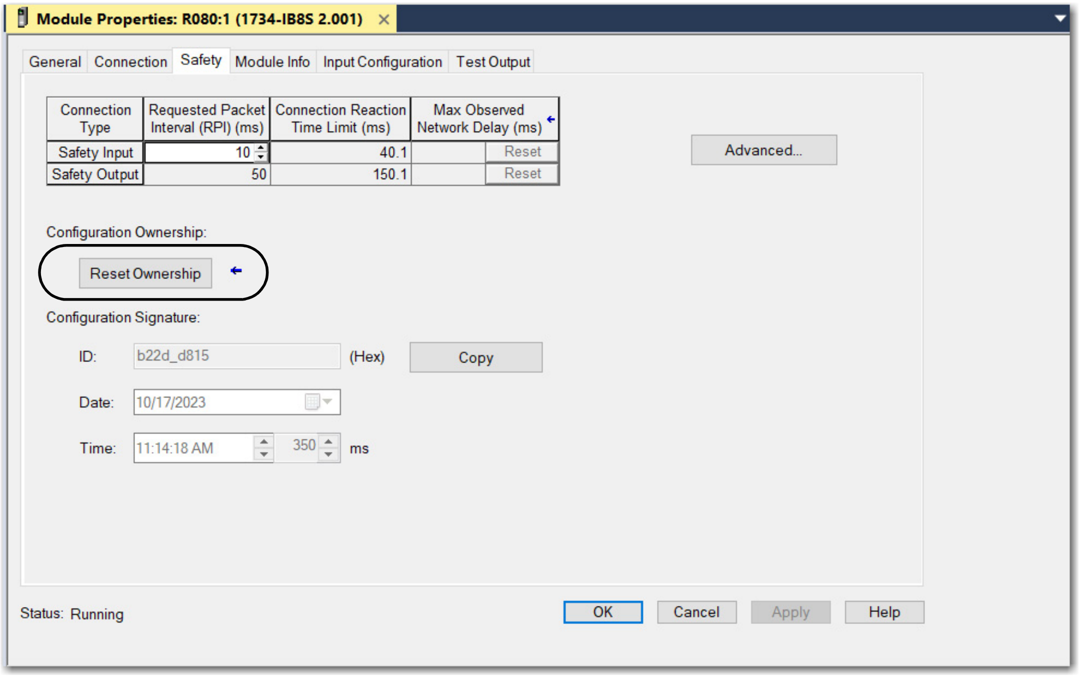
Number:

4293_02FE_EDD0 (Hex)

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

Scenario 2—Replacement Device SNN Is Different from Original and Safety Signature Exists

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



Module Properties: R080:1 (1734-IB8S 2.001)

Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)	
Safety Input	10	40.1		Reset
Safety Output	50	150.1		Reset

Configuration Ownership:

Configuration Signature:

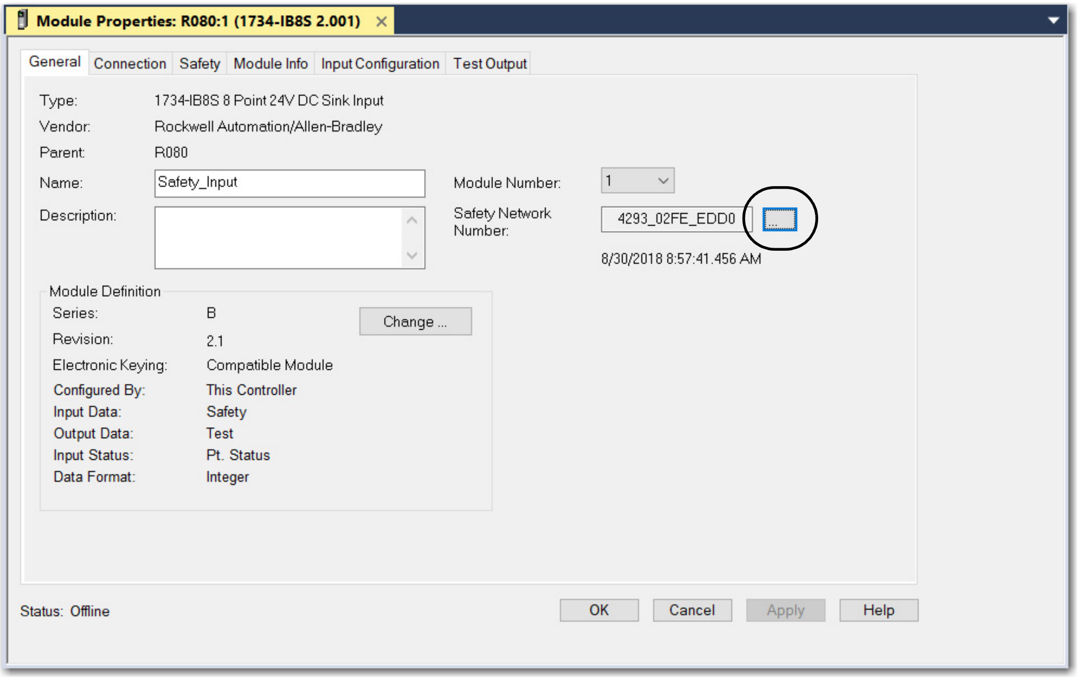
ID: b22d_d815 (Hex)

Date: 10/17/2023

Time: 11:14:18 AM 350 ms

Status: Running

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



Module Properties: R080:1 (1734-IB8S 2.001)

Type: 1734-IB8S 8 Point 24V DC Sink Input

Vendor: Rockwell Automation/Allen-Bradley

Parent: R080

Name: Safety_Input

Description:

Module Number: 1

Safety Network Number: 4293_02FE_EDD0

8/30/2018 8:57:41.456 AM

Module Definition

Series: B

Revision: 2.1

Electronic Keying: Compatible Module

Configured By: This Controller

Input Data: Safety

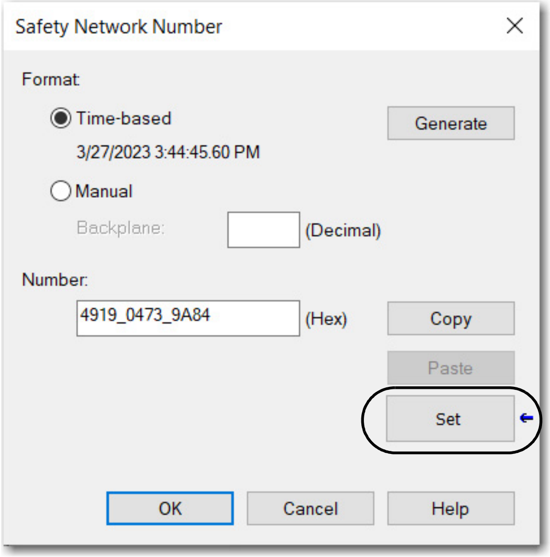
Output Data: Test

Input Status: Pt. Status

Data Format: Integer

Status: Offline

8. Click Set.



Safety Network Number

Format

● Time-based

3/27/2023 3:44:45.60 PM

○ Manual

Backplane: (Decimal)

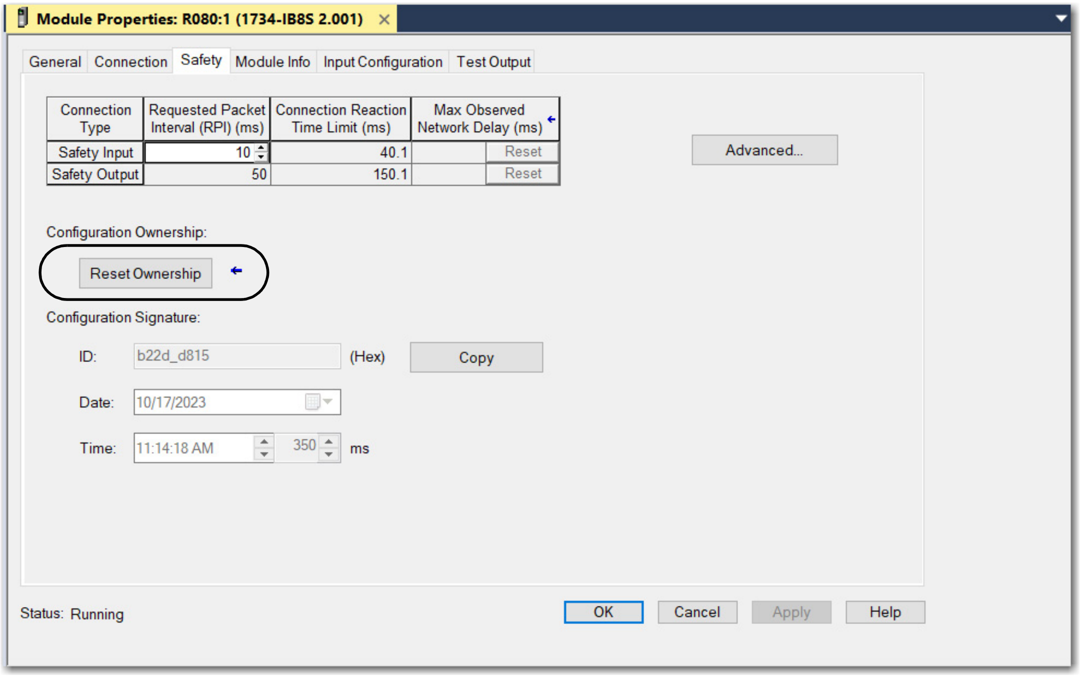
Number: 4919_0473_9A84 (Hex)

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

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

Scenario 3—Replacement Device SNN Is Different from Original and No Safety Signature Exists

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



Module Properties: R080:1 (1734-IB8S 2.001)

Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)
Safety Input	10	40.1	Reset
Safety Output	50	150.1	Reset

Configuration Ownership:

Configuration Signature:

ID: b22d_d815 (Hex)

Date: 10/17/2023

Time: 11:14:18 AM 350 ms

Status: Running

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

Always Allow Automatic Configuration

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

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

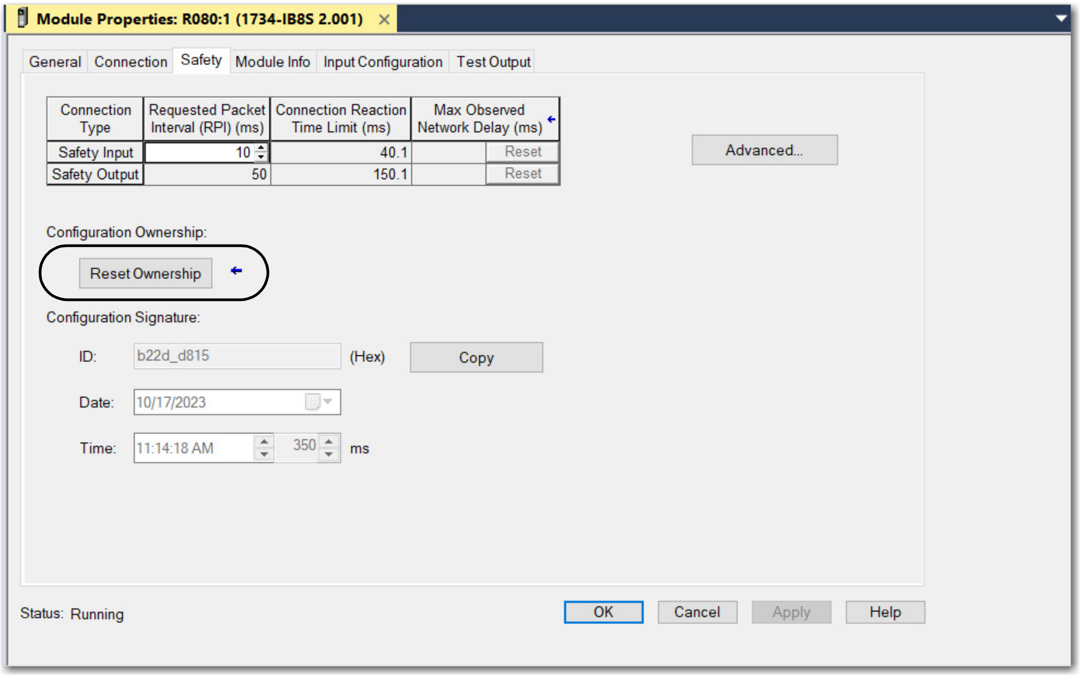
- The controller has configuration data for a compatible device at that network address.
- The device is in out-of-box condition or has an SNN that matches the configuration.

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

1. Remove the old I/O device and install the new device.
   a. If the device is in out-of-box condition, go to step 5.

      No action is needed for the Compact GuardLogix controller to take ownership of the device.

   b. If an SNN mismatch error occurs, go to the next step to reset the device to out-of-box condition.
2. Right-click the safety I/O device and select Properties.
3. Click the Safety tab.
4. Click Reset Ownership and click OK.



Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)	
Safety Input	10	40.1		Reset
Safety Output	50	150.1		Reset

Configuration Ownership:

Configuration Signature:

ID: b22d_d815 (Hex)

Date: 10/17/2023

Time: 11:14:18 AM 350 ms

Status: Running

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

Develop Standard Applications

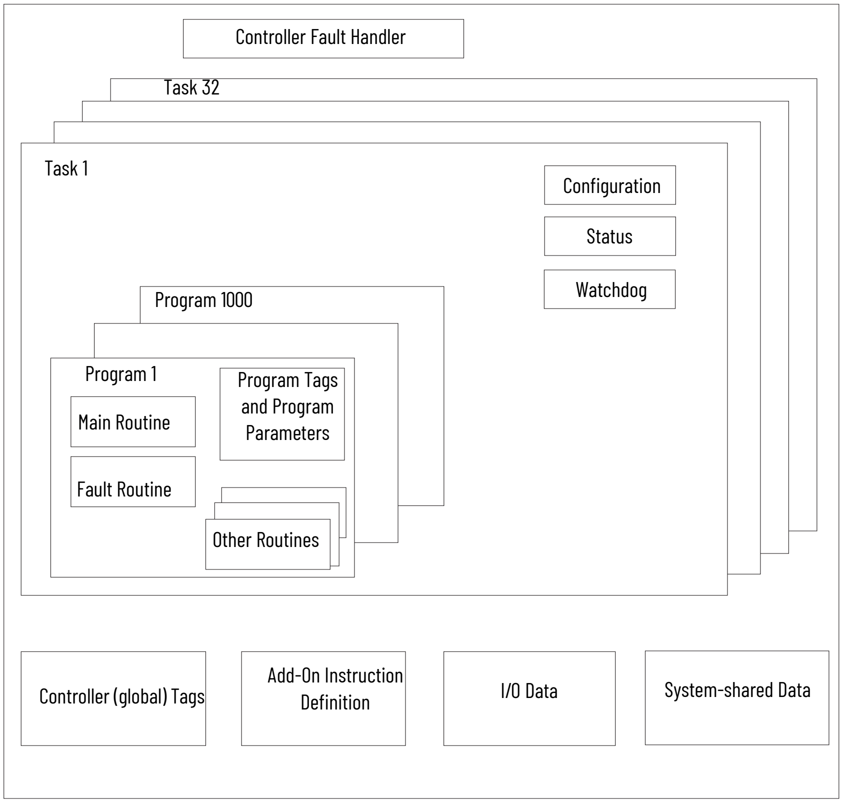
Elements of a Control Application

Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

A large number of tasks can make it difficult to optimally tune your system.

Figure 42 - Task Within a Control Application

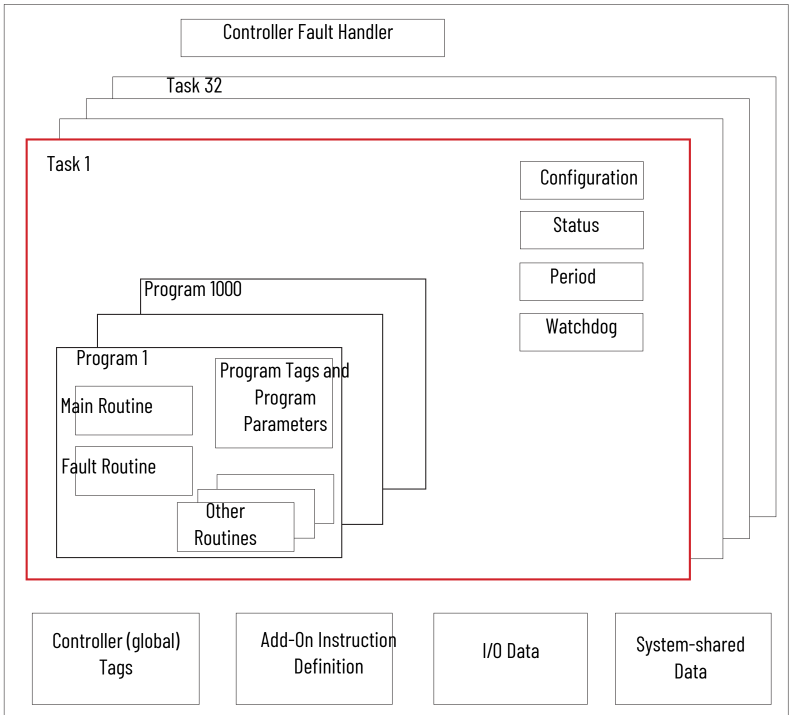
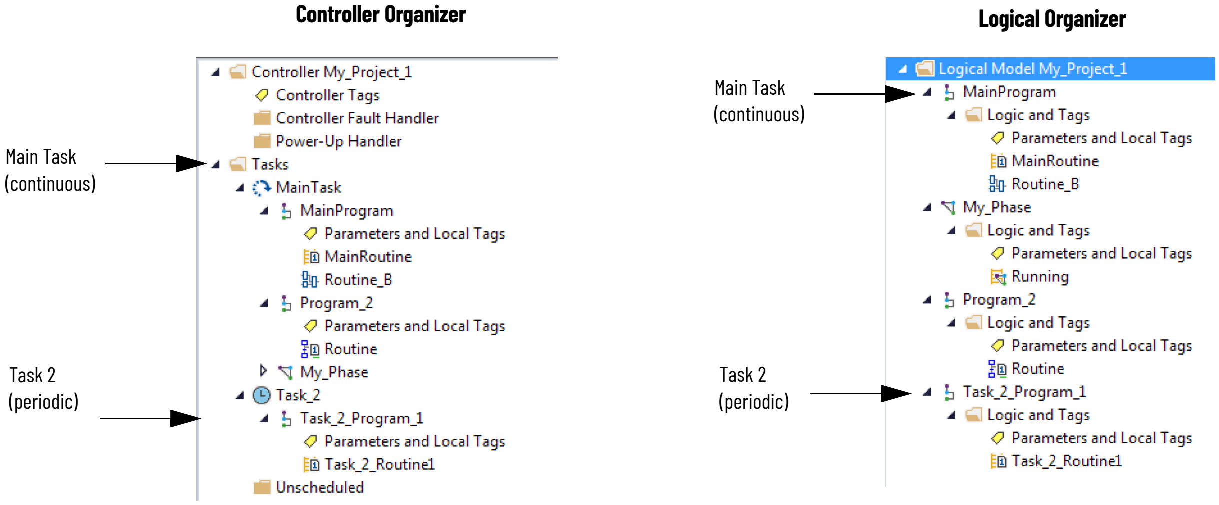


Figure 43 - Tasks



Controller Organizer

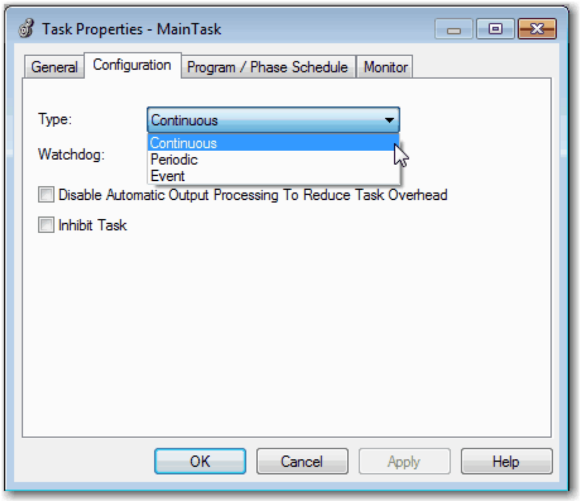
```
Controller My_Project_1
    Controller Tags
    Controller Fault Handler
    Power-Up Handler
Tasks
    MainTask
        MainProgram
            Parameters and Local Tags
            MainRoutine
            Routine_B
        Program_2
            Parameters and Local Tags
            Routine
        My_Phase
    Task_2
        Task_2_Program_1
            Parameters and Local Tags
            Task_2_Routine1
    Unscheduled
```

Logical Organizer

```
Logical Model My_Project_1
    MainProgram
        Logic and Tags
            Parameters and Local Tags
            MainRoutine
            Routine_B
    My_Phase
        Logic and Tags
            Parameters and Local Tags
            Running
    Program_2
        Logic and Tags
            Parameters and Local Tags
            Routine
    Task_2_Program_1
        Logic and Tags
            Parameters and Local Tags
            Task_2_Routine1
```

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

Figure 44 - Configuring the Task Type



Type: Continuous

Watchdog:

☐ Disable Automatic Output Processing To Reduce Task Overhead

☐ Inhibit Task

Table 25 explains the types of tasks you can configure.

Table 25 - Task Types and Execution Frequency

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

The CompactLogix 5380 and Compact GuardLogix 5380 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.

Event Task with Compact 5000 I/O Modules

Compact 5000™ I/O safety input modules cannot trigger events.

Some Compact 5000 I/O digital input modules can trigger an Event task. For example, complete these steps to configure an Event task with a 5069-IB16F module input state change that triggers the event.

1. Configure the 5069-IB16F input module to trigger the Event task. The following tasks are required.
   a. Use the **Data with Events** connection type in the 5069-IB16F module definition.
   b. Enable the Event.
   c. Select at least one point on the module to participate in the event.
   d. Define what constitutes an event, for example, a state change from Off to On.
   e. Choose which edge of the event triggers the event. That is, the rising edge, the falling edge, or both can trigger an event.

   You can also latch an event and enable independent point triggers.
2. Create an Event task in your project.
3. Configure the Event task.
   - You must choose the event trigger. For example, you can choose Module Input Data State Change as the trigger.
   - Link the task to the appropriate Event Input tag on the module.

For more information on how to use event tasks with Compact 5000 I/O modules, see the Compact 5000 I/O Digital and Safety Module User Manual, publication 5000-UM004

For more information on how to use event tasks in general, see the Logix 5000 Controllers Tasks, Programs, and Routines Programming Manual, publication 1756-PM005.

Task Priority

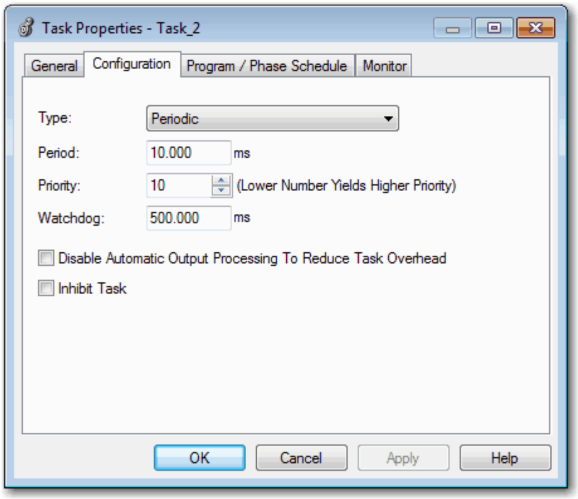
Each task in the controller has a priority level. The operating system uses the priority level to determine which task to execute when multiple tasks are triggered. A higher priority task interrupts any lower priority task. The continuous task has the lowest priority and a periodic or event task interrupts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

The continuous task runs whenever a periodic task is not running. Depending on the application, the continuous task could run more frequently than the periodic tasks, or much less frequently. There can also be large variability in the frequency that the task is called, and its scan time (due to the effect of the other periodic tasks).

IMPORTANT If you configure multiple tasks with the same priority, the controller timeslices them, which de-optimizes their application. This is not recommended.

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

Figure 45 - Configure Task Priority



Type: Periodic

Period: 10.000 ms

Priority: 10 (Lower Number Yields Higher Priority)

Watchdog: 500.000 ms

□ Disable Automatic Output Processing To Reduce Task Overhead

□ Inhibit Task

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 46 - Program Within a Control Application

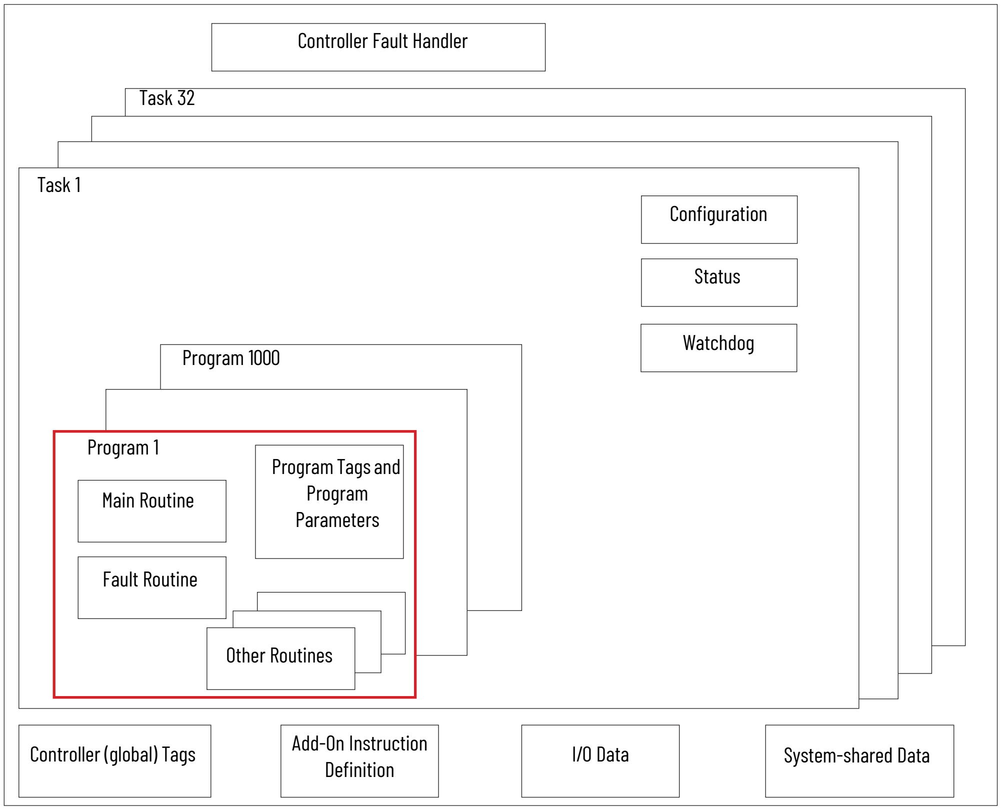
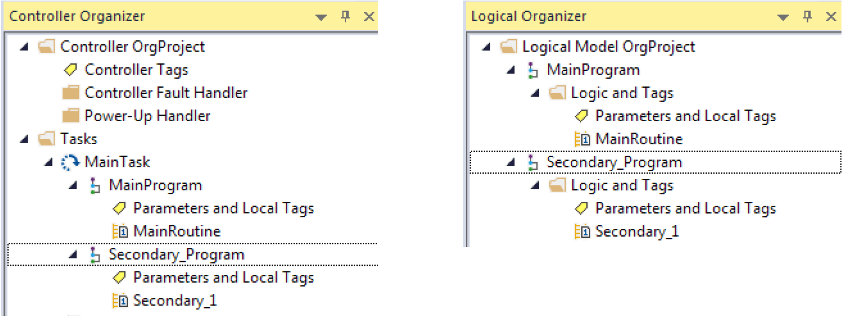


Figure 47 - Programs


Controller Organizer
- Controller OrgProject
  - Controller Tags
  - Controller Fault Handler
  - Power-Up Handler
- Tasks
  - MainTask
    - MainProgram
      - Parameters and Local Tags
      - MainRoutine
    - Secondary_Program
      - Parameters and Local Tags
      - Secondary_1

Logical Organizer
- Logical Model OrgProject
  - MainProgram
    - Logic and Tags
      - Parameters and Local Tags
      - MainRoutine
  - Secondary_Program
    - Logic and Tags
      - Parameters and Local Tags
      - Secondary_1

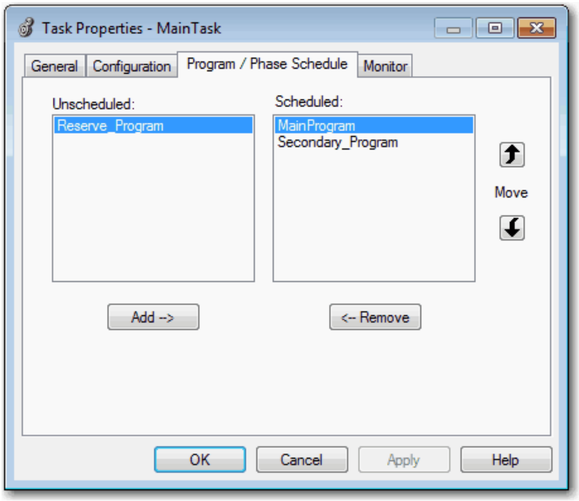
Scheduled and Unscheduled Programs

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 48 - Scheduling an Unscheduled Program



Unscheduled:
Reserve_Program

Scheduled:
MainProgram
Secondary_Program

Routines

A routine is a set of logic instructions in one programming language, such as Ladder Diagram. 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 49 - Routines in a Control Application

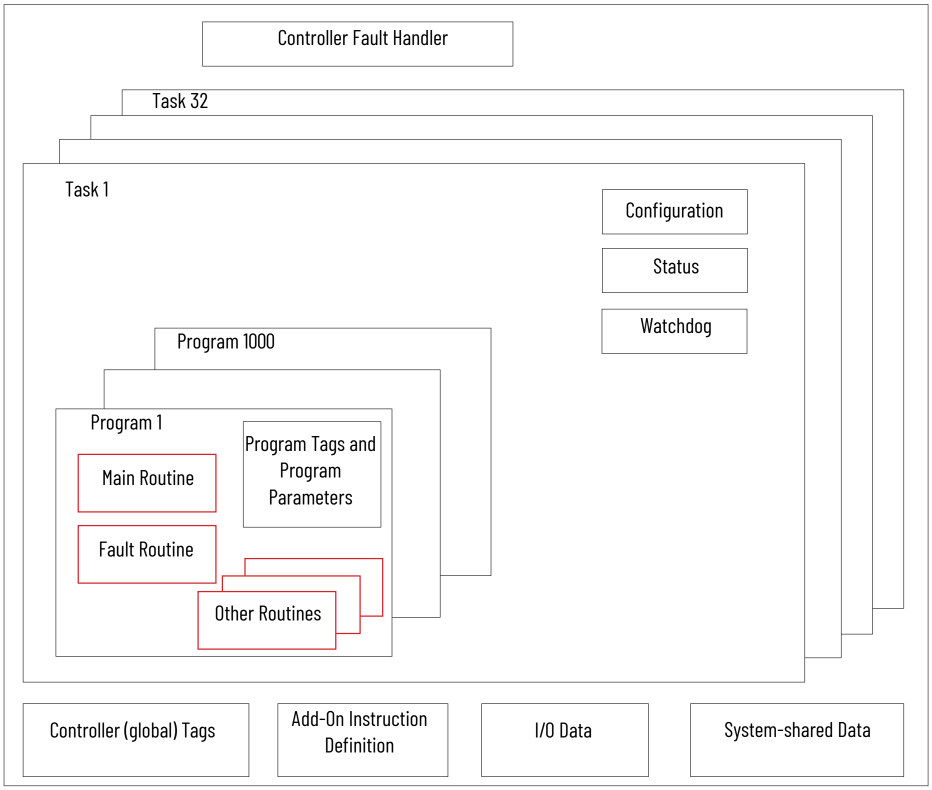
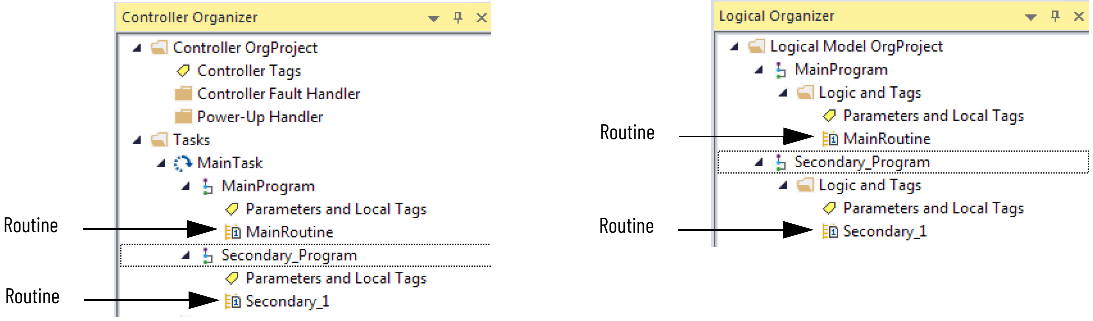


Figure 50 - Routines



Controller Organizer

```
◢ Controller OrgProject
    Controller Tags
    Controller Fault Handler
    Power-Up Handler
◢ Tasks
  ◢ MainTask
    ◢ MainProgram
        Parameters and Local Tags
        MainRoutine
    ◢ Secondary_Program
        Parameters and Local Tags
        Secondary_1
```

Logical Organizer

```
◢ Logical Model OrgProject
  ◢ MainProgram
    ◢ Logic and Tags
        Parameters and Local Tags
        MainRoutine
  ◢ Secondary_Program
    ◢ Logic and Tags
        Parameters and Local Tags
        Secondary_1
```

Parameters and Local Tags

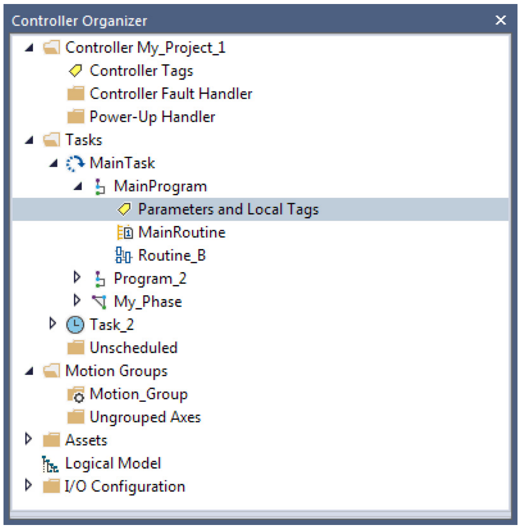
With a Logix 5000™ controller, you use a tag (alphanumeric name) to address data (variables). In Logix 5000 controllers, there is no fixed, numeric format. The tag name identifies the data and lets you do the following:

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

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

Figure 51 - Tags Example

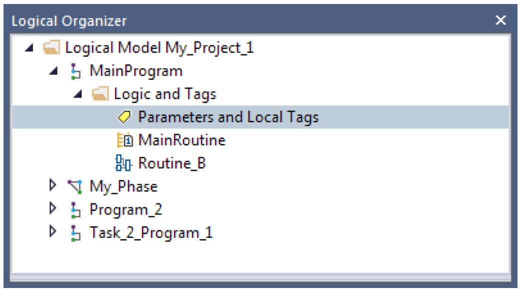
Controller Organizer —Main Program Parameters and Local Tags



Controller Organizer

- Controller My_Project_1
  - Controller Tags
  - Controller Fault Handler
  - Power-Up Handler
- Tasks
  - MainTask
    - MainProgram
      - Parameters and Local Tags
      - MainRoutine
      - Routine_B
    - Program_2
    - My_Phase
  - Task_2
  - Unscheduled
- Motion Groups
  - Motion_Group
  - Ungrouped Axes
- Assets
- Logical Model
- I/O Configuration

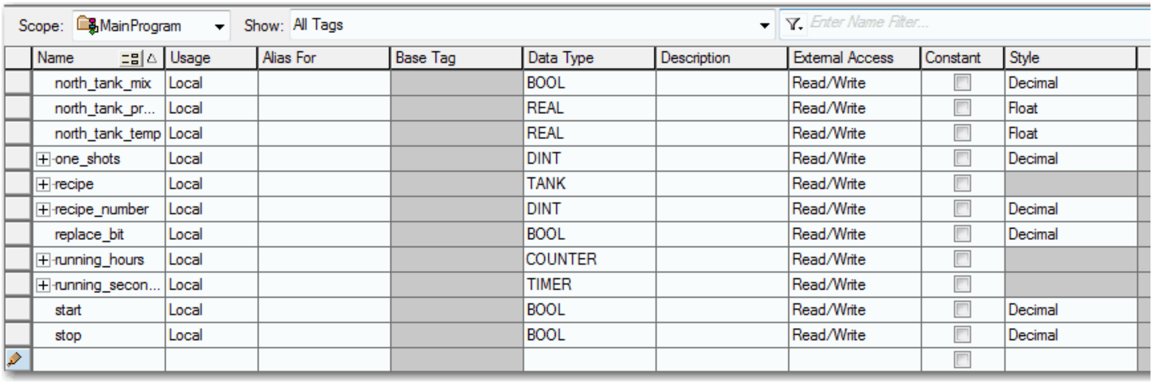
Logical Organizer —Main Program Parameters and Local Tags



Logical Organizer

- Logical Model My_Project_1
  - MainProgram
    - Logic and Tags
      - Parameters and Local Tags
      - MainRoutine
      - Routine_B
  - My_Phase
  - Program_2
  - Task_2_Program_1

Program Tags Window—Main Program Parameters and Local Tags



Scope: MainProgram Show: All Tags Enter Name Filter...

Name	Usage	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
north_tank_mix	Local			BOOL		Read/Write	☐	Decimal
north_tank_pr...	Local			REAL		Read/Write	☐	Float
north_tank_temp	Local			REAL		Read/Write	☐	Float
+one_shots	Local			DINT		Read/Write	☐	Decimal
+recipe	Local			TANK		Read/Write	☐	
+recipe_number	Local			DINT		Read/Write	☐	Decimal
replace_bit	Local			BOOL		Read/Write	☐	Decimal
+running_hours	Local			COUNTER		Read/Write	☐	
+running_secon...	Local			TIMER		Read/Write	☐	
start	Local			BOOL		Read/Write	☐	Decimal
stop	Local			BOOL		Read/Write	☐	Decimal
							☐	

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. You can achieve data sharing between programs through either 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 how to create and configure parameters and local tags for optimal task and program execution:

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

Programming Languages

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

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 Compact GuardLogix 5380 controllers.
Function Block Diagram (FBD)	Continuous process and drive control
	Loop control
	Calculations in circuit flow
Sequential Function Chart (SFC)	High-level management of multiple operations
	Repetitive sequence of operations
	Batch process
	Motion control that uses Structured Text
	State machine operations
Structured Text (ST)	Complex mathematical operations
	Specialized array or table loop processing
	ASCII string handling or protocol processing

For information about programming in these languages, 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 Logix 5000 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 26 explains some of the capabilities and advantages of use Add-On Instructions.

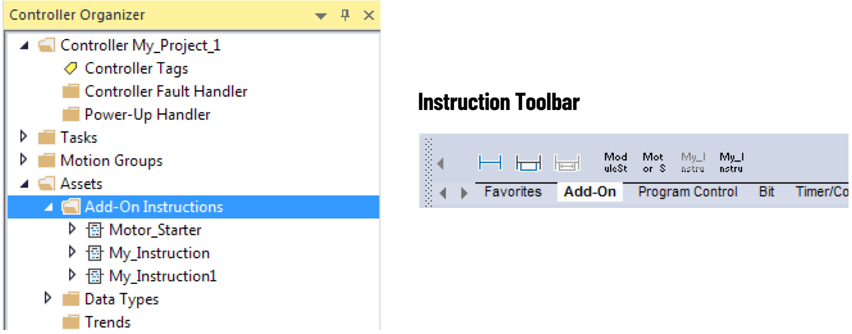
Table 26 - Add-On Instruction Capabilities

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. **IMPORTANT**: You cannot edit AOIs while online. You can overwrite existing AOIs by using the partial import online feature.
Use Standard Editors	You use one of these editors to create Add-On Instructions: • Ladder Diagram • Function Block Diagram • Structured Text
Export Add-On Instructions	You can export 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 to perform instant and simple 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.
Apply Source Protection	When you create Add-On Instructions, you can limit users of your instructions to read-only access. You can also bar access to the internal logic or local parameters that the instructions use. This source protection lets you stop unwanted changes to your instructions and helps protect your intellectual property.

Once defined in a project, Add-On Instructions behave similarly to the built-in instructions in Logix 5000 controllers.

With Studio 5000 Logix Designer Version 31 and greater, Add-On Instructions appear under the Assets folder in the organizer. They appear on the instruction tool bar for easy access along with internal instructions.

Figure 52 - Add-On Instructions (Studio 5000 Logix Designer Version 31 Example)



Controller Organizer

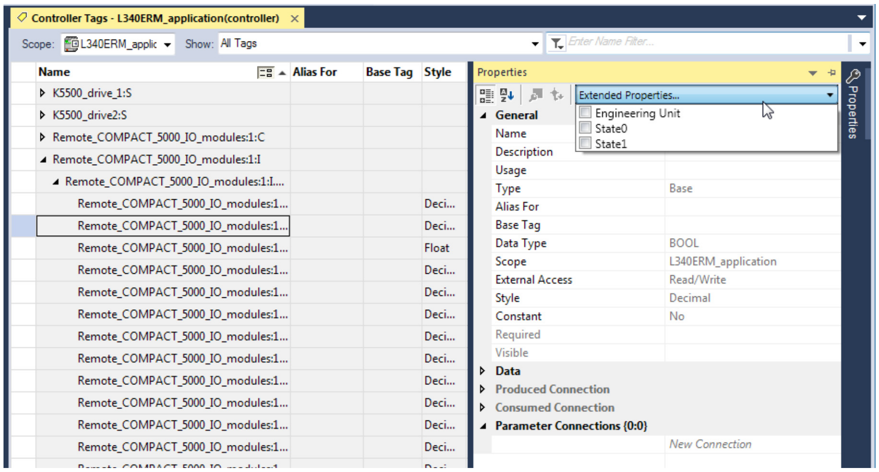
- Controller My_Project_1
  - Controller Tags
  - Controller Fault Handler
  - Power-Up Handler
- Tasks
- Motion Groups
- Assets
  - Add-On Instructions
    - Motor_Starter
    - My_Instruction
    - My_Instruction1
  - Data Types
  - Trends

Instruction Toolbar

Extended Properties

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



Controller Tags - L340ERM_application(controller)

Scope: L340ERM_applic Show: All Tags Enter Name Filter...

Name	Alias For	Base Tag	Style
K5500_drive_1:S			
K5500_drive2:S			
Remote_COMPACT_5000_IO_modules:1:C			
Remote_COMPACT_5000_IO_modules:1:I			
Remote_COMPACT_5000_IO_modules:1:I....			
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Float
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...
Remote_COMPACT_5000_IO_modules:1...			Deci...

Properties

Extended Properties...

- □ Engineering Unit
- □ State0
- □ State1

General	
Name	
Description	
Usage	
Type	Base
Alias For	
Base Tag	
Data Type	BOOL
Scope	L340ERM_application
External Access	Read/Write
Style	Decimal
Constant	No
Required	
Visible	
Data	
Produced Connection	
Consumed Connection	
Parameter Connections {0:0}	
	New Connection

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 are 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. There is no indication in the tag browser that limits 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 the .@Min and .@Max syntax defines. However, you cannot write to extended properties values in logic.

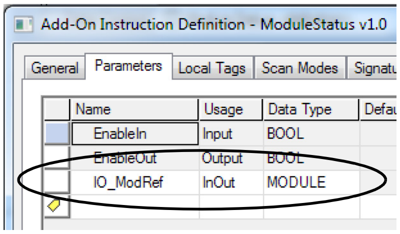
For more information on Extended Properties, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

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.

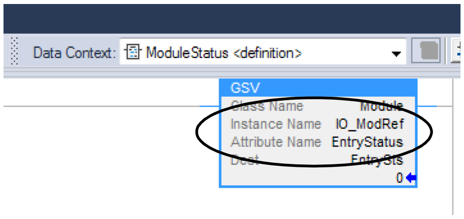
You can access a MODULE object directly from an Add-On Instruction. Previously, you could access the MODULE object data but not from within an Add-On Instruction.

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.



Add-On Instruction Definition - ModuleStatus v1.0

Name	Usage	Data Type	Defau
EnableIn	Input	BOOL	
EnableOut	Output	BOOL	
IO_ModRef	InOut	MODULE	



Data Context: ModuleStatus <definition>

GSV
Class Name Module
Instance Name IO_ModRef
Attribute Name EntryStatus
Dest EntrySts
0

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 these attributes to provide status information:

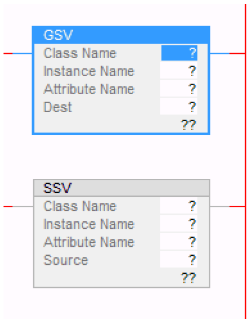
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

Monitor Controller Status

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

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

Figure 53 - GSV and SSV Instructions for Monitoring and Setting Attributes



GSV
Class Name ?
Instance Name ?
Attribute Name ?
Dest ?
??

SSV
Class Name ?
Instance Name ?
Attribute Name ?
Source ?
??

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 that 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 the 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. You can access the fault code via the following:
  - The Module Properties dialog box
  - A GSV instruction

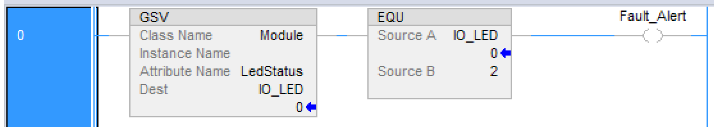
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication 1756-PM014.

Determine If I/O Communication Has Timed Out

This example can be used with the CompactLogix 5380 or Compact GuardLogix 5380 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, at least one I/O connection has been lost and the Fault_Alert is set.

Figure 54 - GSV Used to Identify I/O Timeout



GSV
Class Name Module
Instance Name
Attribute Name LedStatus
Dest IO_LED
0

EQU
Source A IO_LED
0
Source B 2

Fault_Alert

IMPORTANT	**Safety Consideration** Each Safety I/O module has a connection status in the module defined 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 the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

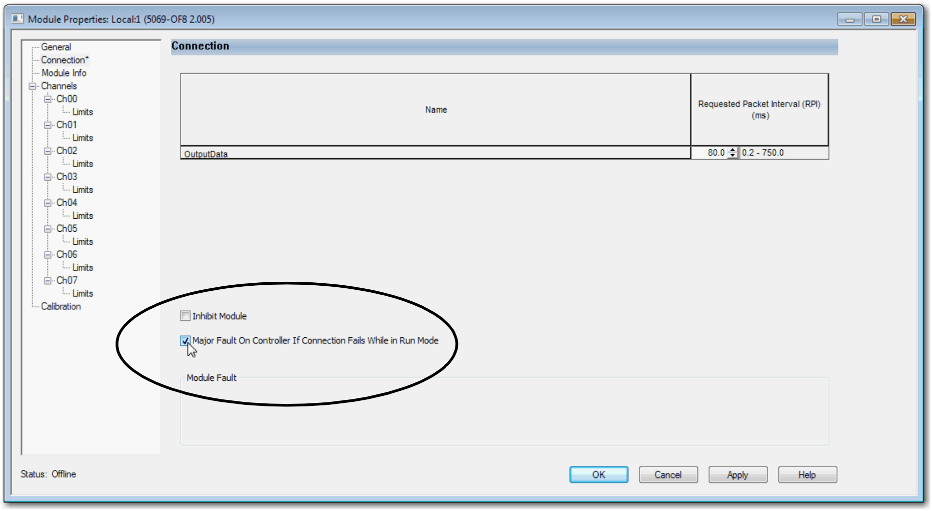
Automatic Handling of I/O Module Connection Faults

You can use 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.

IMPORTANT	You cannot program Safety I/O module connections or safety produce/consume connections to automatically cause a major fault on the controller. See Develop Standard Applications on page 177.

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

Figure 55 - I/O Connection Fault Causes Major Fault



Module Properties: Local:1 (5069-OF8 2.005)

Name	Requested Packet Interval (RPI) (ms)	
OutputData	80.0	0.2 - 750.0

☐ Inhibit Module

☑ Major Fault On Controller If Connection Fails While in Run Mode

Status: Offline

You can configure the application so that a response to a failed I/O module connection can wait until the next program scan. In this case, put the logic in a normal routine and use the GSV technique that is described on page 190 to call the logic.

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

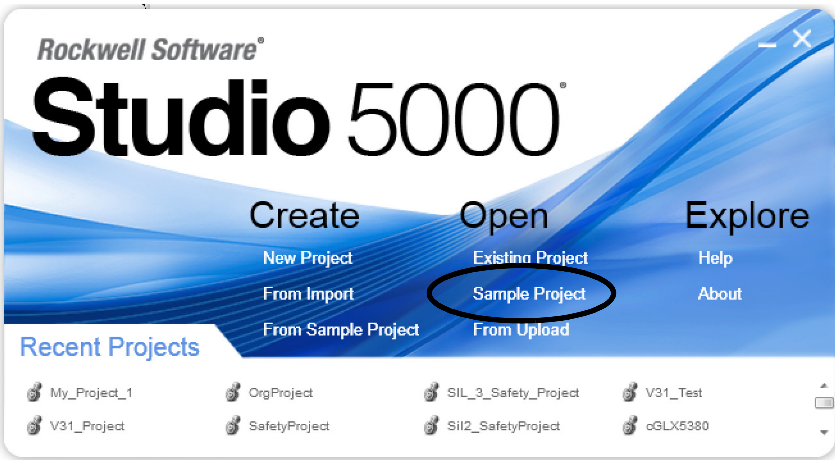
It takes at least 100 milliseconds to detect an I/O connection loss, even if the Controller Fault Handler is used.

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

Sample Controller Projects

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

Figure 56 - Opening Sample Projects



Notes:

Chapter 14

Develop Safety Applications

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

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

- GuardLogix 5580 controllers support both SIL 2 and SIL 3 levels of safety control with the safety task.
- Compact GuardLogix 5380 controllers support SIL 2 or SIL 3 levels[1] of safety control with the safety task.

Safety Overview

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

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

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

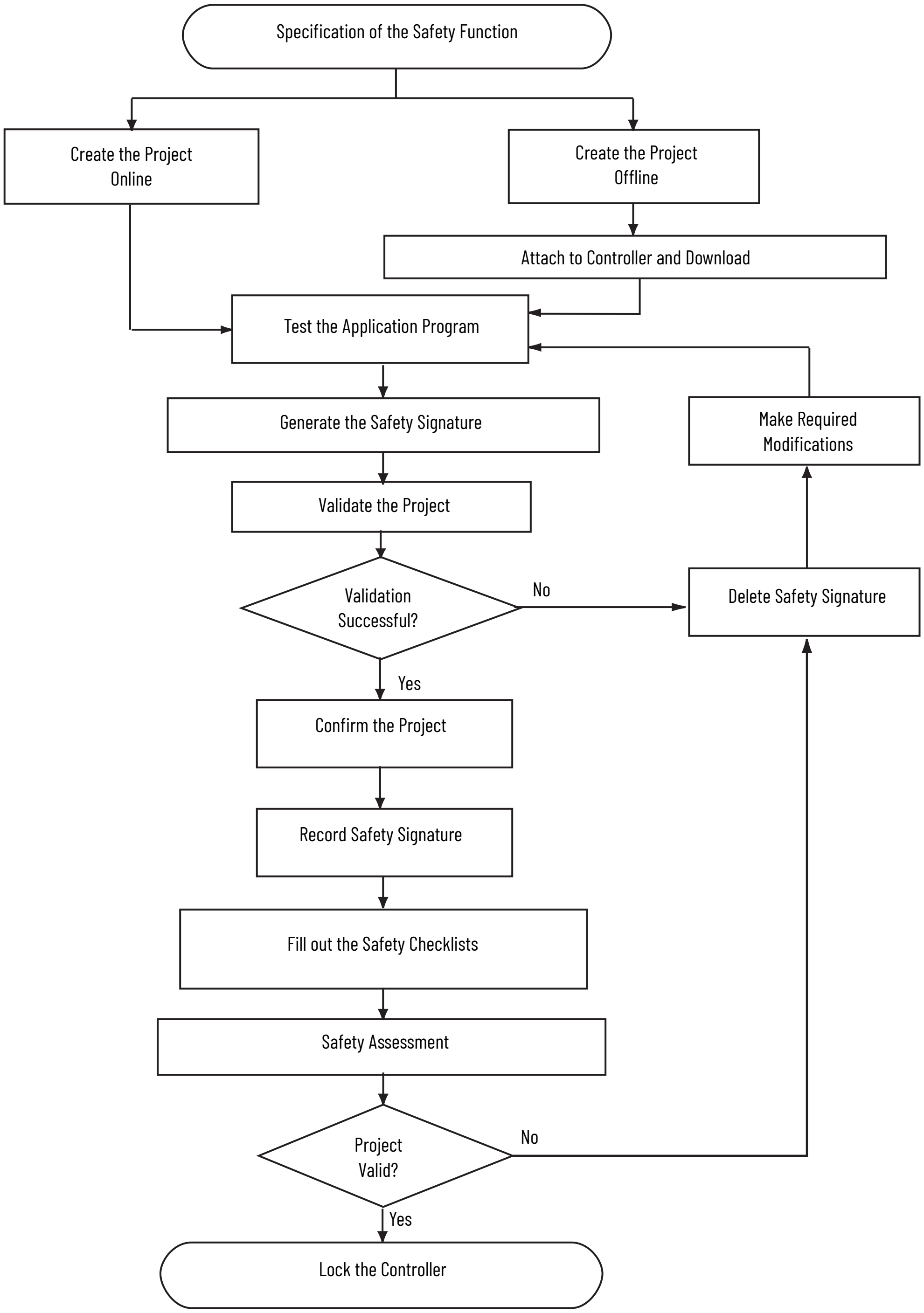
⚠ **ATTENTION:** Performing an on-line modification (to logic, data, or configuration) can affect the Safety Functions of the system if the modification is performed while the application is running. A modification should only be attempted if absolutely necessary. Also, if the modification is not performed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

[1] SIL level support depends on the catalog number. See the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Reference Manual, 1756-RM012.

Program Safety Applications

Figure 57 shows the steps that are required for commissioning a GuardLogix system. For an explanation of those steps, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

Figure 57 - Commission the System


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

Develop Secure Applications

Applies to these controllers:
CompactLogix 5380

These CompactLogix™ 5380 controllers support IEC-62443-4-2 SL 1 security requirements:

- CompactLogix 5380 standard controllers, firmware revision 36 or later
- CompactLogix 5380 NSE, XT, K, and Process controllers, firmware revision 36 or later

Compact GuardLogix® 5380 safety controllers **do not** support IEC-62443-4-2 SL 1 security requirements.

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

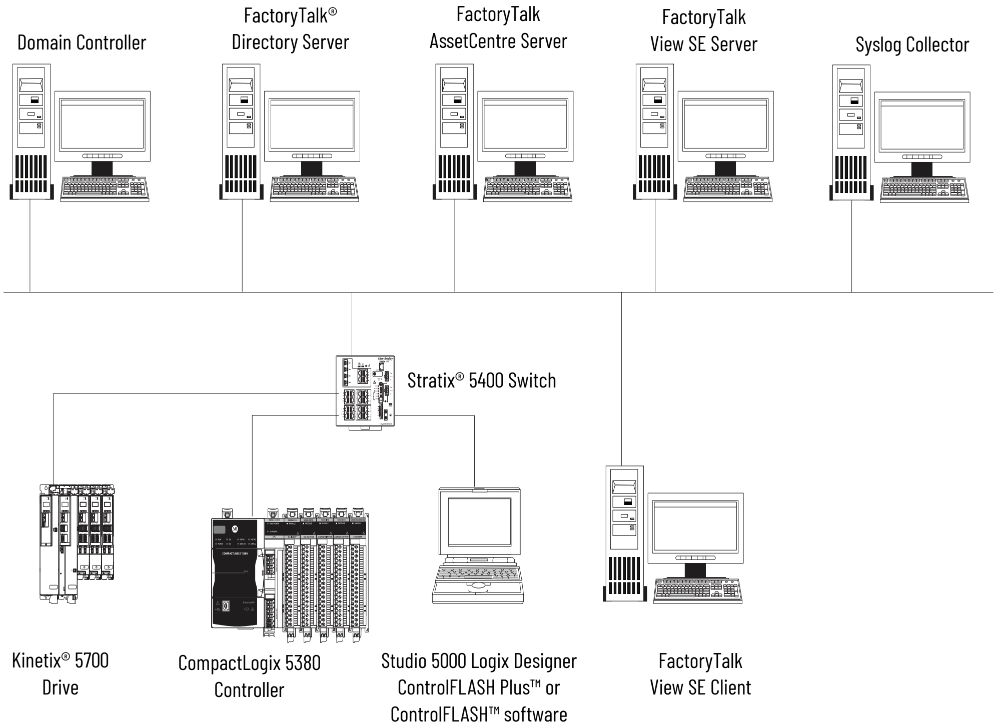
The controller accepts all values appropriate for a tag data type, and it is the responsibility of the user program to specify valid ranges and perform validity to check for those ranges. The controller verifies incoming messages for syntax, length, and format.

You can apply these same measures to other CompactLogix and Compact 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 CompactLogix controller to comply with the certification requirements, implement the control system with these other security-focused products.



Security Checklists

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

Table 27 - Requirements for Identification and Authorization

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

Table 28 - Requirements for Use Control

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	Studio 5000 Logix Designer application	May be required based on system design, threat model, and risk assessment.	Configure the controller project in the Studio 5000 Logix Designer application to use these user access methods: • License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. • License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. • Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. • The Studio 5000 Logix Designer application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag. For more information, see Logix 5000 Controllers Security Programming Manual, 1756-PM016.
	FactoryTalk Security software Studio 5000 Logix Designer application	Yes	Configure FactoryTalk Security to define policies, user groups, and other permission sets. • The Studio 5000 Logix Designer application enforces the policy based on the access policies that are provided to it by FactoryTalk Security for the software authenticated user. Once authenticated, the Studio 5000 Logix Designer application acts as your interface to the controller, including all protected CIP™ communications to the controller, whether from Ethernet, backplane, or USB. • The FactoryTalk Services Platform offers feature access control to manage user access to product features, such as controller download, project import, project create, and firmware update. • In FactoryTalk Security, define which users can change controller modes and download projects to the controller. • Security authority binding restricts the controller to a specific FactoryTalk Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. For more information, see Configure System Security Features User Manual, SECURE-UM001.
	Controller 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 controller Ethernet port	May be required based on system design, threat model, and risk assessment.	The Ethernet port is enabled by default. Disable the Ethernet port if required by the system design, threat model, or risk assessment. For more information, see page 208.
	Disable the controller CIP Security™ ports	May be required based on system design, threat model, and risk assessment.	CIP Security ports on the controller are enabled by default. Disable the CIP Security ports if required by the system design, threat model, or risk assessment. For more information, see page 212.

Table 28 - Requirements for Use Control (Continued)

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	Disable the controller USB ports	May be required based on system design, threat model, and risk assessment.	The USB port on the controller is enabled by default. Disable the USB port if required by the system design, threat model, or risk assessment. For more information, see page 215.
	Disable the controller SD card	May be required based on system design, threat model, and risk assessment.	The SD card is enabled by default. Disable the SD card if required by the system design, threat model, or risk assessment. For more information, see page 216.
	Disable controller webpages	May be required based on system design, threat model, and risk assessment.	Controller webpages for diagnostics are read-only. With Studio 5000 Logix Designer application version 33 or later, controller webpages are disabled by default. Disable the controller webpages if required by the system design, threat model, or risk assessment. For more information, see page 222.

Table 29 - Requirements for System Integrity

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	The FactoryTalk AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes based on FactoryTalk Security settings. This server functionality assists with diagnostics and troubleshooting and reduces maintenance time for production assets. Configure the Device Monitor - Change Detect operation for the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001.
	FactoryTalk Security software		
	ControlFLASH Plus™ or ControlFLASH™ software	Yes	Use ControlFLASH Plus™ or ControlFLASH™ software to update controller firmware. Digitally signed firmware files have a .DMK (Device Management Kit) extension. ControlFLASH software authenticates the origin of a DMK file and validates the file before download in the device.
	Studio 5000 Logix Designer application	Yes	You can generate a signature on an Add-On Instruction. This signature seals (encrypts) the Add-On Instruction to help prevent modification.
	Controller firmware update	Yes	To meet IEC-62443-4-2 SL 1 security requirements, you must use a certified version of the controller firmware. We recommend that you use the latest minor revision of your firmware. The controller is designed such that: • 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 54.
	User-definable major controller faults	May be required based on system design, threat model, and risk assessment.	If your application requires a major fault in addition to those already monitored by the controller, define a predetermined state with a major fault so that outputs are off. For more information, see page 208.

Table 30 - Requirements for Data Confidentiality

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk Security software	Yes	Configure FactoryTalk Security to define policies, user groups, and other permission sets. • The FactoryTalk Services Platform offers feature access control to manage user access to product features such as controller download, project import, project create, and firmware update. • In FactoryTalk Security, define which users can change controller modes and download projects to the controller. • Security authority binding restricts the controller to a specific FactoryTalk Security instance. This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access. For more information, see Configure System Security Features User Manual, SECURE-UM001.

Table 30 - Requirements for Data Confidentiality (Continued)

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk Policy Manager software	Yes	Use the FactoryTalk Policy Manager software to define a secure data transport over an EtherNet/IP™ network to the controller. For more information, see Configure System Security Features User Manual, SECURE-UM001.
	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 94.
	License-based source and execution protection	May be required based on system design, threat model, and risk assessment.	Configure licenses to manage access to controller source logic and execution of that logic. These licenses are not enabled by default. • License-based source protection limits access to projects to only users with the required license. Users without the required license cannot open the project or import components that are protected by the license. • License-based execution protection allows execution of the component only on a specific controller family, or only on controllers in a specific controller family that contain the execution license. • Password-based protection uses a source key (password) to help protect source logic. All source keys are stored in the sk.dat file. • The Studio 5000 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 202.

Table 31 - Requirements for Restricted Data Flow

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

Table 32 - Requirements for Timely Response to Events

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Audit log accessibility • Continuous monitoring For more information, see the following: • Configure System Security Features User Manual, SECURE-UM001. • System Security Design Guidelines Reference Manual, SECURE-RM001
	Syslog collector	Yes, if not using FactoryTalk AssetCentre for logging	The controller supports syslog event logging. Choose a syslog collector that supports the following: • RFC-5424 syslog protocol • Ability to receive messages from the controller **IMPORTANT:** The controller sends events to a syslog collector through its front Ethernet port. The Ethernet port must be connected to the same network as the syslog collector. To set the IP address of the syslog collector, use FactoryTalk Policy Manager software. For more information, see CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001. To view a list of syslog messages and their descriptions, see 1756-RD001.

Table 32 - Requirements for Timely Response to Events

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	Controller change detection	Yes	Enable the change detection feature to monitor program components to determine whether they change. The change detection feature is not enabled by default. For more information, see page 205.
	Controller component tracking	May be required based on system design, threat model, and risk assessment	Enable component tracking to monitor configurable program components to determine whether they change. Component tracking is not enabled by default. For more information, see page 206.
	Disabled controller log auto-write	Yes	The controller log stores security-related events that can be accessed via FactoryTalk AssetCentre software. To help prevent the potential loss of controller logs before FactoryTalk AssetCentre can access them, follow these guidelines: • Do not use a Message to Self (MSG with a Path of THIS) to auto-write controller logs to the SD card. • Do not manually force a write of controller logs to the SD card. By default, the controller log auto-write is disabled. For more information, see page 207.

Table 33 - Requirements for Resource Availability

✓	Product	Required to Meet IEC-62443-4-2 SL 1	Details
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Asset inventory • Control system backup • Disaster recovery For more information, see Configure System Security Features User Manual, SECURE-UM001.
	UPS	Yes	Provide your own UPS with separate battery unit and redundant power supplies. Size the UPS so that is correctly supports the system and provides enough power to properly shut down servers and workstations.

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

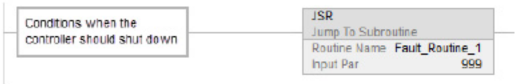
To configure the program to use the fault routine, do the following:

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.

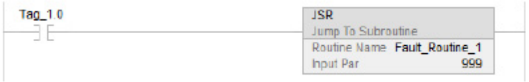
Jump to the Fault Routine

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.


Conditions when the controller should shut down
JSR
Jump To Subroutine
Routine Name Fault_Routine_1
Input Par 999

When Tag_1.0 = 1, execution jumps to name_of_fault_routine, a major fault occurs and the controller enters the faulted mode. Outputs go to the faulted state. The Controller Properties dialog box, Major Faults tab, displays the code 999.

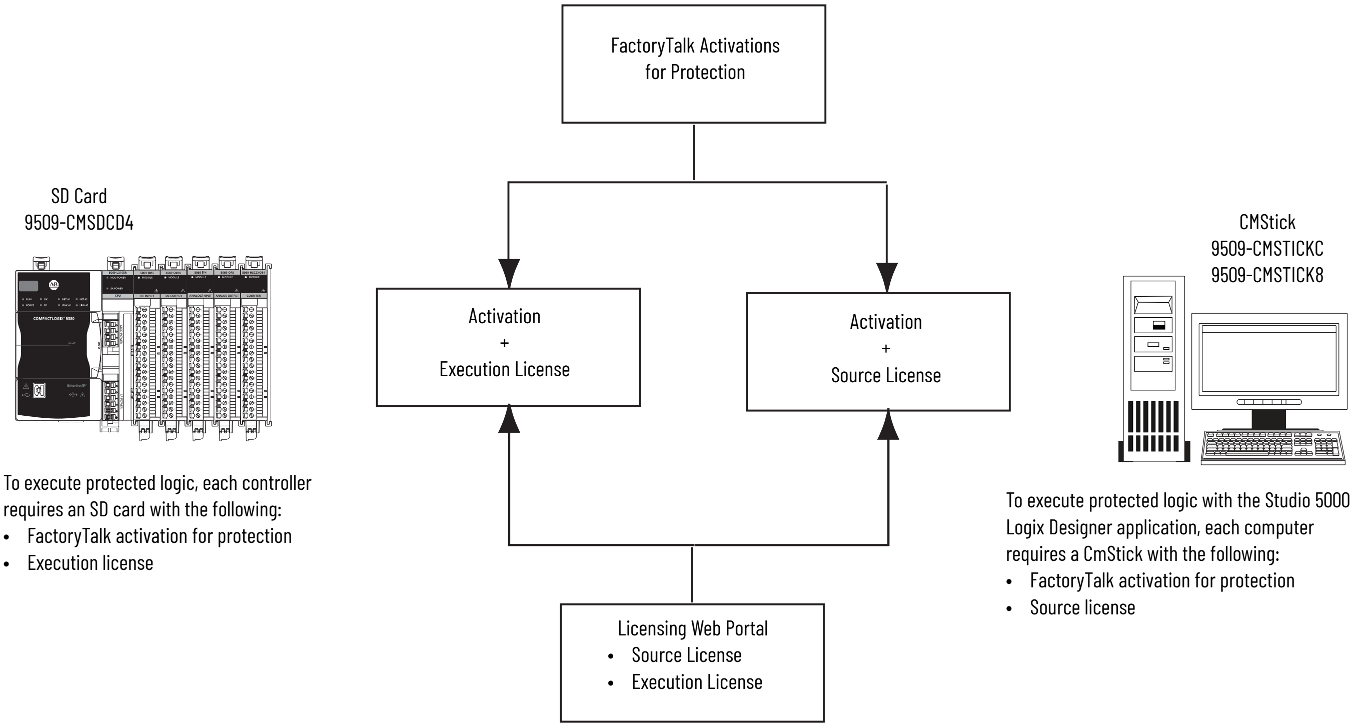


License-based Source and Execution Protection

Source protection helps prevent logic components from being modified based on a license.

Execution protection adds additional protection to controller logic. Execution protection makes sure that the right controller has access to execute the protected program. Use this with source protection to make sure that the right programmer has access to modify the logic.

Each controller or computer requires an activation to access protection features. Each logic component or program requires a license to be accessed or executed.



To execute protected logic, each controller requires an SD card with the following:

- FactoryTalk activation for protection
- Execution license

To execute protected logic with the Studio 5000 Logix Designer application, each computer requires a CmStick with the following:

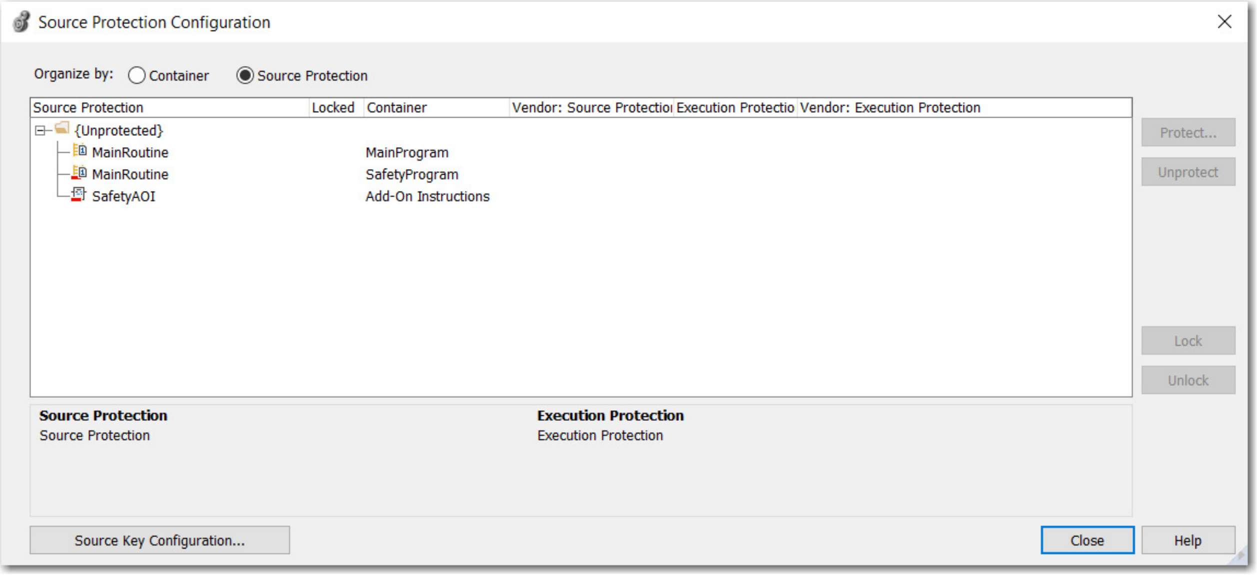
- FactoryTalk activation for protection
- Source license

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.



Source Protection Configuration

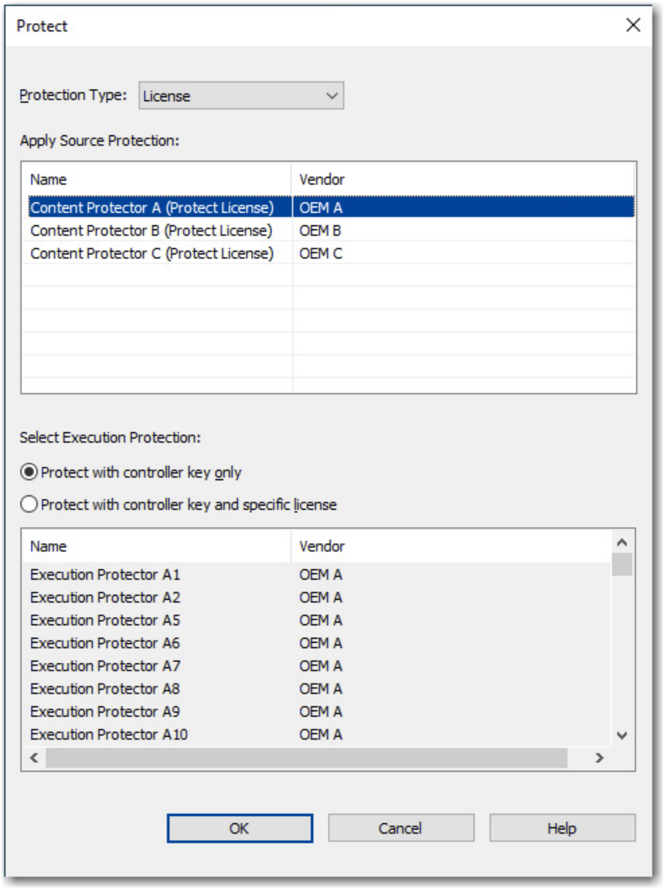
Organize by: ○ Container ● Source Protection

Source Protection	Locked	Container	Vendor: Source Protectio	Execution Protectio	Vendor: Execution Protection
{Unprotected}					
MainRoutine		MainProgram			
MainRoutine		SafetyProgram			
SafetyAOI		Add-On Instructions			

Source Protection
Source Protection

Execution Protection
Execution Protection

2. Insert the CmStick that contains the license that you want to use to help protect the component into the USB port on the computer. Licenses must contain the Protect permission to be used to protect components. If a license does not contain the Protect permission, it does not appear in the list of licenses.
3. In the Source Protection Configuration dialog box, select the component to be protected and click Protect.
4. In the Protect dialog box, select the license to apply.



Protect

Protection Type: License

Apply Source Protection:

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

Select Execution Protection:

● Protect with controller key only

○ Protect with controller key and specific license

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

5. Select the execution protection type:
   - Protect with controller key only. This option is selected by default. With this option selected, the component, when locked, runs only on a controller in the same family as the one specified for the project. For example, if you lock a License-based Protected component for a project on a CompactLogix 5380 controller, the component can only be executed on another CompactLogix 5380 controller.
   - Protect with controller key and specific license. When you select this option, the component runs only on a controller in the same family as the one specified for the project and that contains a CmCard with the execution license that you select. If you select Protect with controller key and specific license, select the execution license from the list of available licenses.

   After components are protected, they can also be locked. When you lock a component, it helps prevent users from viewing or editing the component, but allows authorized users to run it.
6. To return to the Source Protection Configuration dialog box, click OK.

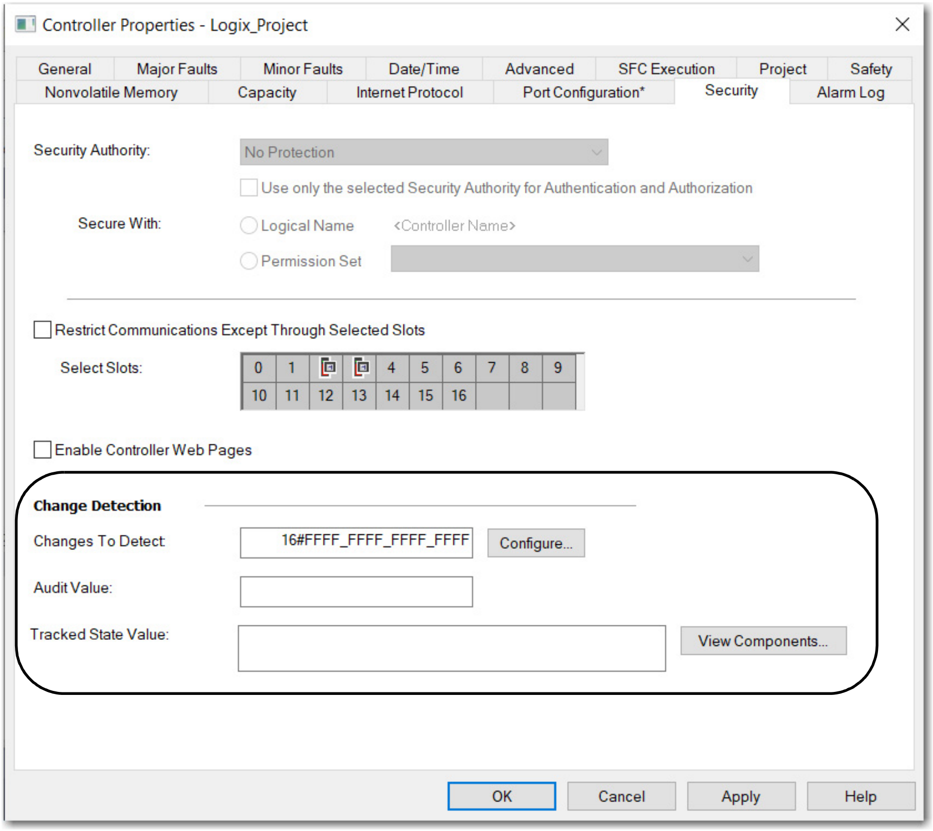
To save changes to a component that is protected with License-Based Source Protection, a CmStick that contains the required license must be plugged into the computer that runs the Studio 5000 Logix Designer application.

Make sure that you save your edits to the project or lock the protected components before removing the CmStick that contains the required license. If the license is not present, you could lose your edits to the project.

Configure Change Detection

On the Security tab of the controller properties, the Change Detection feature tracks changes to a controller and generates an audit value when a monitored change occurs.

For more information about change detection, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.



Controller Properties - Logix_Project

Security Authority: No Protection

□ Use only the selected Security Authority for Authentication and Authorization

Secure With: ○ Logical Name <Controller Name>

○ Permission Set

□ Restrict Communications Except Through Selected Slots

Select Slots:

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

□ Enable Controller Web Pages

Change Detection

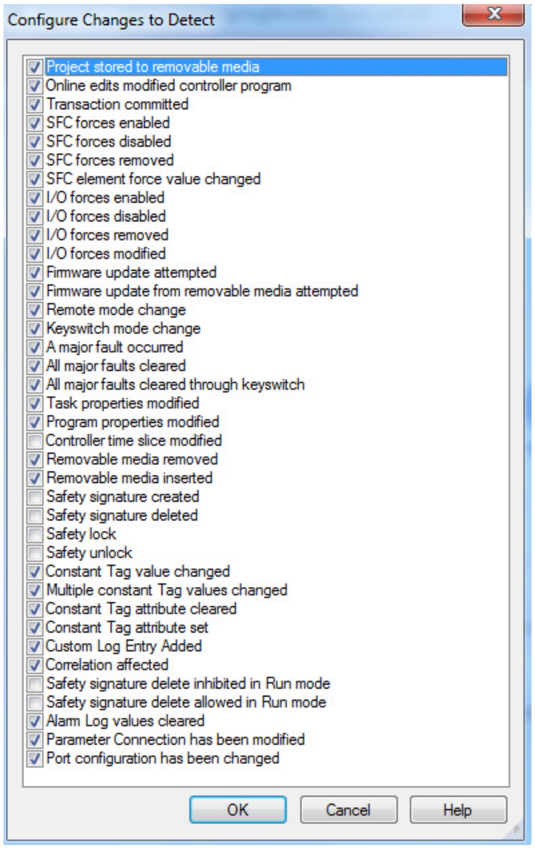
Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

Tracked State Value:

Changes to Detect

Click Configure to open the Configure Changes to Detect dialog box. We recommend tracking the changes that are shown in the following image for a standard CompactLogix 5380 controller. By default, all event types can cause the audit value to change, resulting in a default value of 0xFFFFFFFFFFFFFFFF.



Configure Changes to Detect

- ☑ Project stored to removable media
- ☑ Online edits modified controller program
- ☑ Transaction committed
- ☑ SFC forces enabled
- ☑ SFC forces disabled
- ☑ SFC forces removed
- ☑ SFC element force value changed
- ☑ I/O forces enabled
- ☑ I/O forces disabled
- ☑ I/O forces removed
- ☑ I/O forces modified
- ☑ Firmware update attempted
- ☑ Firmware update from removable media attempted
- ☑ Remote mode change
- ☑ Keyswitch mode change
- ☑ A major fault occurred
- ☑ All major faults cleared
- ☑ All major faults cleared through keyswitch
- ☑ Task properties modified
- ☑ Program properties modified
- □ Controller time slice modified
- ☑ Removable media removed
- ☑ Removable media inserted
- □ Safety signature created
- □ Safety signature deleted
- □ Safety lock
- □ Safety unlock
- ☑ Constant Tag value changed
- ☑ Multiple constant Tag values changed
- ☑ Constant Tag attribute cleared
- ☑ Constant Tag attribute set
- ☑ Custom Log Entry Added
- ☑ Correlation affected
- □ Safety signature delete inhibited in Run mode
- □ Safety signature delete allowed in Run mode
- ☑ Alarm Log values cleared
- ☑ Parameter Connection has been modified
- ☑ Port configuration has been changed

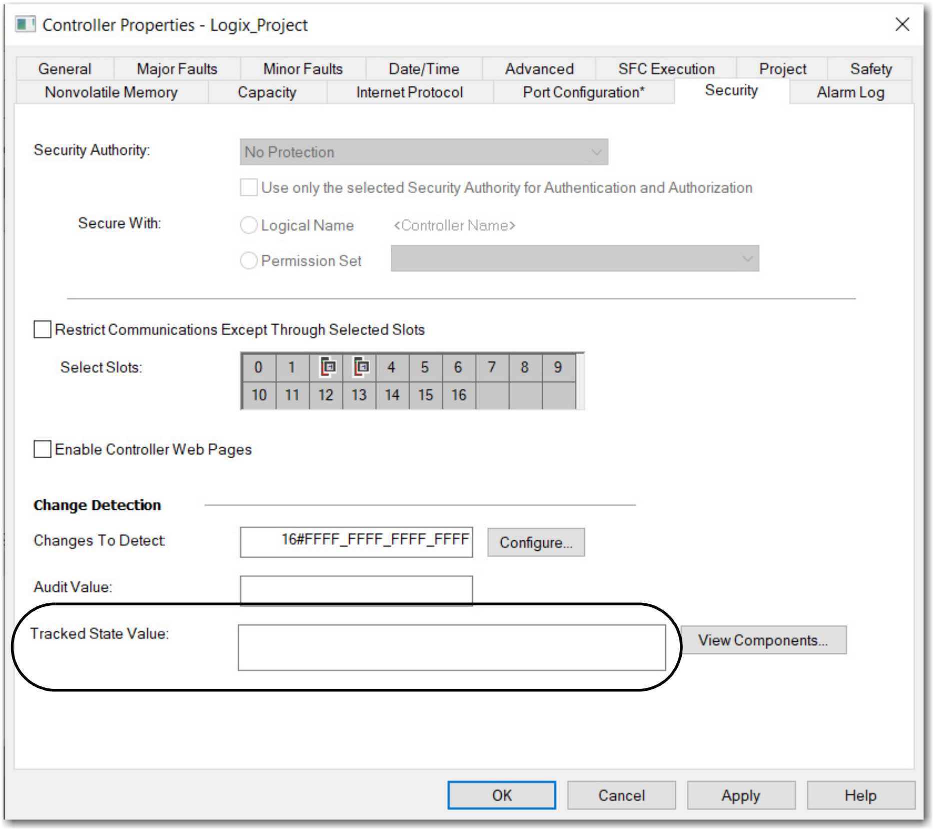
Audit Value

A unique value that is generated when a project is downloaded to the controller or loaded from a storage device. This value is updated when a change to an event occurs. Some events always cause an Audit Value change, while others are selectable in the Configure Changes to Detect dialog box. When the controller is offline, the Audit Value box is blank.

Configure Component Tracking

On the Security tab of the controller properties, component tracking enables you to determine whether tracked routines, Add-On Instructions, I/O modules, and constant tags have been changed. The Logix Designer application creates a tracked state value to indicate the current state of all components.

For more information about component tracking, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.



Security Authority: No Protection

□ Use only the selected Security Authority for Authentication and Authorization

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

□ Restrict Communications Except Through Selected Slots

Select Slots:

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

□ Enable Controller Web Pages

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

Tracked State Value:

Configure Controller Logging

The controller log stores various security-related events that can be written to an SD card or accessed via FactoryTalk Asset Center or a third-party syslog collector. Some of these events are Studio 5000 Logix Designer application request errors, control system events, backup/restore events, and configuration changes.

For more information on how to access the controller log, see the Logix 5000 Controller Information and Status Programming Manual, publication 1756-PM015.

For more robust logging and to help prevent rollover, use FactoryTalk AssetCentre or a syslog collector.

Disable Controller Ethernet Ports

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

IMPORTANT	Remember the following: • When you use the Studio 5000 Logix Designer application, version 29 or later, you can disable either of the Ethernet ports whether the controller uses Dual-IP mode or Linear/DLR mode. • Once an Ethernet port is disabled, you lose any connection that is established through that port. • You cannot disable Ethernet ports if the controller is in Run mode or if the FactoryTalk® Security settings deny this editing option.

Ethernet ports return to the default setting after the following occur 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 - The following are examples of what clears 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.

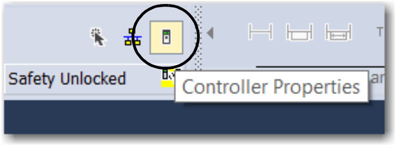
There are two ways to disable the Ethernet port:

- Disable the Ethernet Port on the Port Configuration Tab on page 209
- Disable the Ethernet Port with a MSG Instruction on page 210

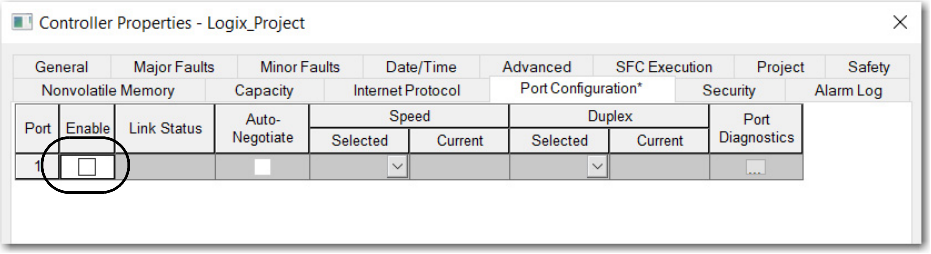
Disable the Ethernet Port on the Port Configuration Tab

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.



Port	Enable	Link Status	Auto-Negotiate	Speed		Duplex		Port Diagnostics
				Selected	Current	Selected	Current	
1	☐		☐					...

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

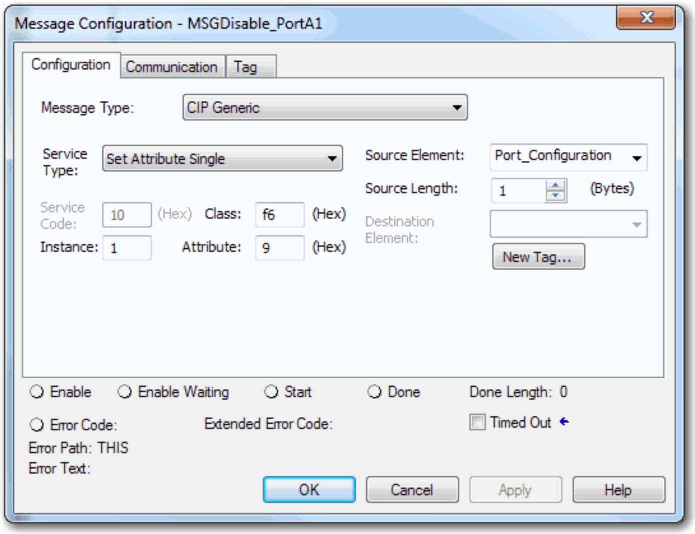
You use a CIP™ Generic MSG with a Path of THIS to execute this option. You cannot use this MSG instruction to disable the Ethernet port on a different controller.

1. Add a MSG instruction to your program.

   This message only needs 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 is in Run mode or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 34.



Message Configuration - MSGDisable_PortA1

Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex) Class: f6 (Hex)

Instance: 1 Attribute: 9 (Hex)

Source Element: Port_Configuration

Source Length: 1 (Bytes)

Destination Element:

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out ←

Error Path: THIS

Error Text:

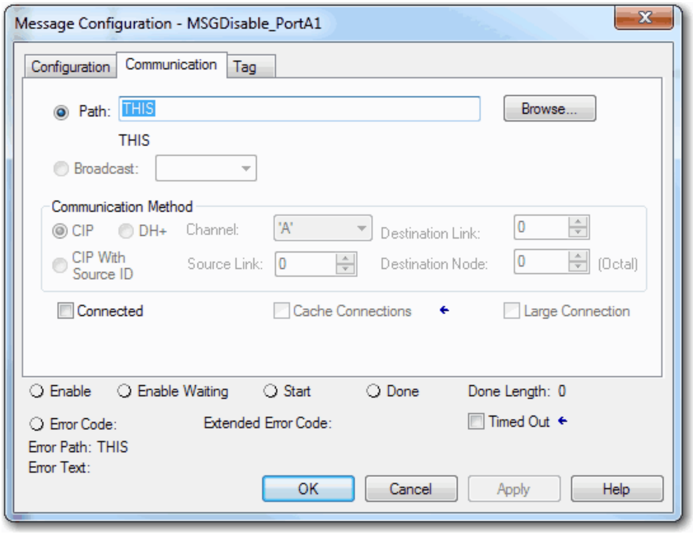
IMPORTANT	The values that are listed below are stored to NVS memory in such a way that the MSG instruction is not required to be executed each time the controller powers up.

Table 34 - Disable an Ethernet Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1 to disable Port A1 2 to disable Port A2
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.



Message Configuration - MSGDisable_PortA1

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

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.

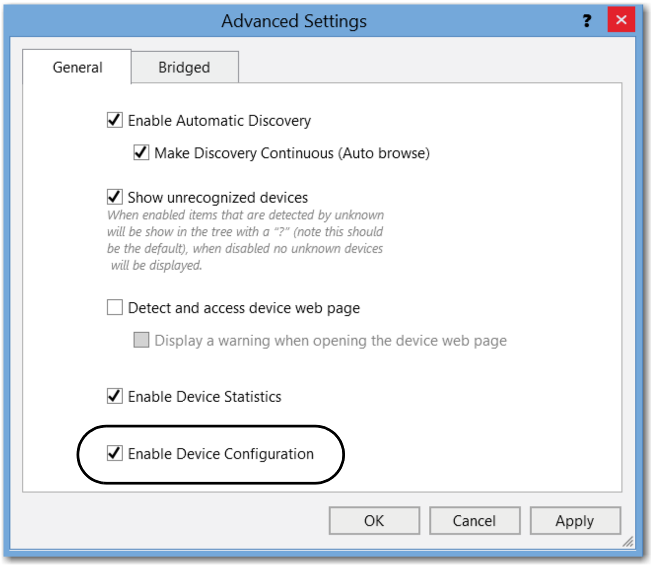
Disable the Controller CIP Security Ports

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

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

Use the Disable CIP Security Checkbox in FactoryTalk Linx

1. If the Device Configuration menu in FactoryTalk Linx is not enabled, go to the Advanced Settings dialog box and select Enable Device Configuration.



Advanced Settings

General | Bridged

☑ Enable Automatic Discovery

☑ Make Discovery Continuous (Auto browse)

☑ Show unrecognized devices

When enabled items that are detected by unknown will be show in the tree with a "?" (note this should be the default), when disabled no unknown devices will be displayed.

□ Detect and access device web page

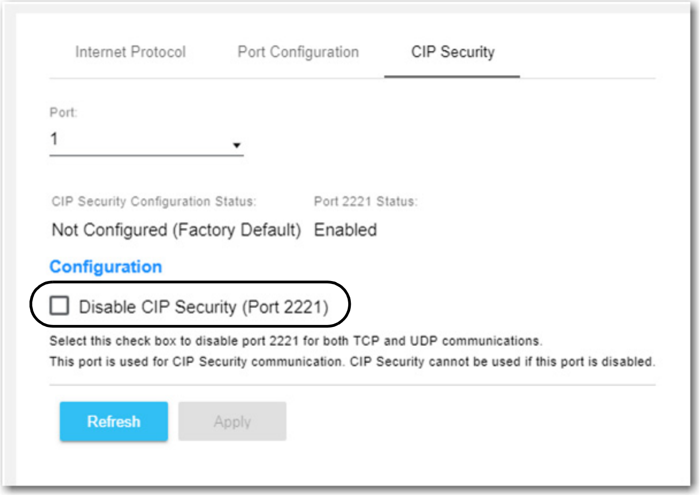
□ Display a warning when opening the device web page

☑ Enable Device Statistics

☑ Enable Device Configuration

OK | Cancel | Apply

2. From the Device Configuration menu, click the CIP Security tab, and then select Disable CIP Security (Port 2221).



Internet Protocol | Port Configuration | CIP Security

Port:
1

CIP Security Configuration Status: Not Configured (Factory Default)

Port 2221 Status: Enabled

Configuration

□ Disable CIP Security (Port 2221)

Select this check box to disable port 2221 for both TCP and UDP communications.
This port is used for CIP Security communication. CIP Security cannot be used if this port is disabled.

Refresh | Apply

Use a CIP Generic MSG Instruction in the Studio 5000 Logix Designer Application

IMPORTANT This procedure disables CIP Security ports. To re-enable the ports, use the controller reset button to perform a Stage 2 reset, which returns the controller to a factory default state.

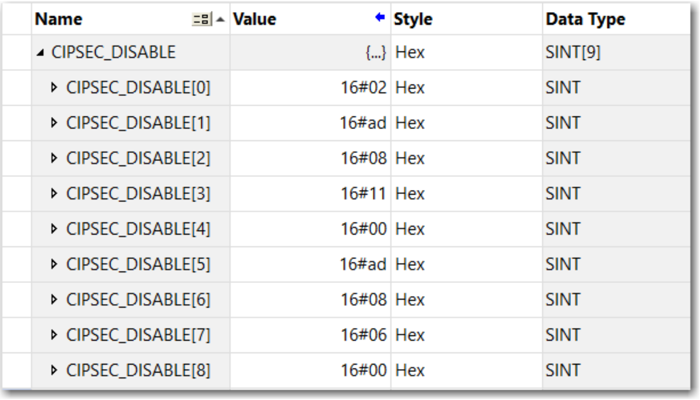
See Stage 2 Reset on page 88.

You cannot use this MSG instruction to disable the CIP Security ports on another controller.

The message only has to execute once rather than with every program scan.

1. Create a controller tag with the SINT[9] data type.

   In this example, the controller tag is named CIPSEC_DISABLE and must match the following image.



Name	Value	Style	Data Type
CIPSEC_DISABLE	{...}	Hex	SINT[9]
CIPSEC_DISABLE[0]	16#02	Hex	SINT
CIPSEC_DISABLE[1]	16#ad	Hex	SINT
CIPSEC_DISABLE[2]	16#08	Hex	SINT
CIPSEC_DISABLE[3]	16#11	Hex	SINT
CIPSEC_DISABLE[4]	16#00	Hex	SINT
CIPSEC_DISABLE[5]	16#ad	Hex	SINT
CIPSEC_DISABLE[6]	16#08	Hex	SINT
CIPSEC_DISABLE[7]	16#06	Hex	SINT
CIPSEC_DISABLE[8]	16#00	Hex	SINT

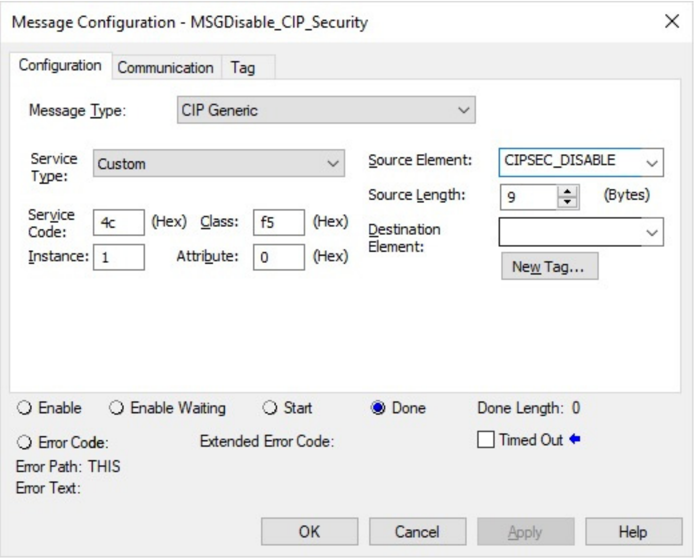
   Before you enable the MSG instruction, consider the following:

   - The element CIPSEC_DISABLE[4] is responsible for disabling UDP port 2221 and EtherNet/IP™ over DTLS, transport class 0/1.
   - The element CIPSEC_DISABLE[8] is responsible for disabling TCP port 2221 and EtherNet/IP over TLS, UCMM, and transport class 3.
   - To disable the controller CIP Security ports, the elements CIPSEC_DISABLE[4] and CIPSEC_DISABLE[8] in the SINT array for the Source Element CIPSEC_DISABLE must be 0.

2. Add an MSG instruction to your program.

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

3. Configure the Configuration tab on the Message Configuration dialog box as described in Table 35 on page 214.



Message Configuration - MSGDisable_CIP_Security

Configuration | Communication | Tag

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex)

Instance: 1 Attribute: 0 (Hex)

Source Element: CIPSEC_DISABLE

Source Length: 9 (Bytes)

Destination Element:

New Tag...

○ Enable ○ Enable Waiting ○ Start ● Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

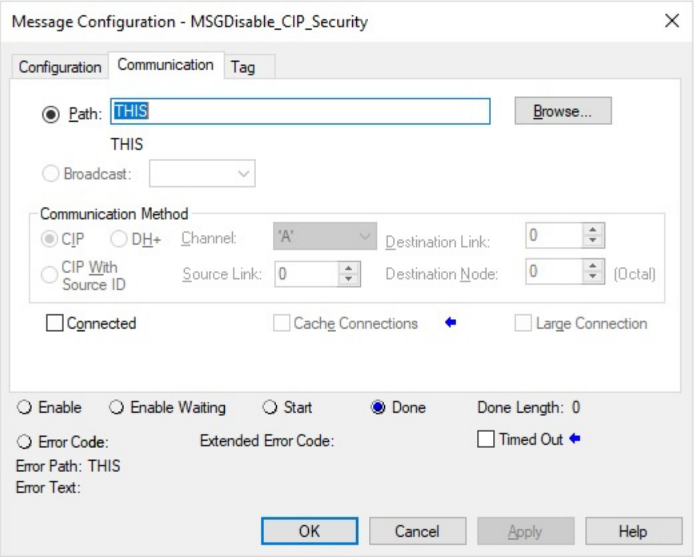
Error Text:

Table 35 - Disable the CIP Security Ports

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1
Class	f5
Attribute	0
Source Element	Controller tag of SINT[9] data type. This is the controller tag that you created in step 1.
Source Length	9

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

IMPORTANT Messages to THIS must be unconnected messages.



Message Configuration - MSGDisable_CIP_Security

Configuration | Communication | Tag

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ● Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

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

Disable the Controller USB Port

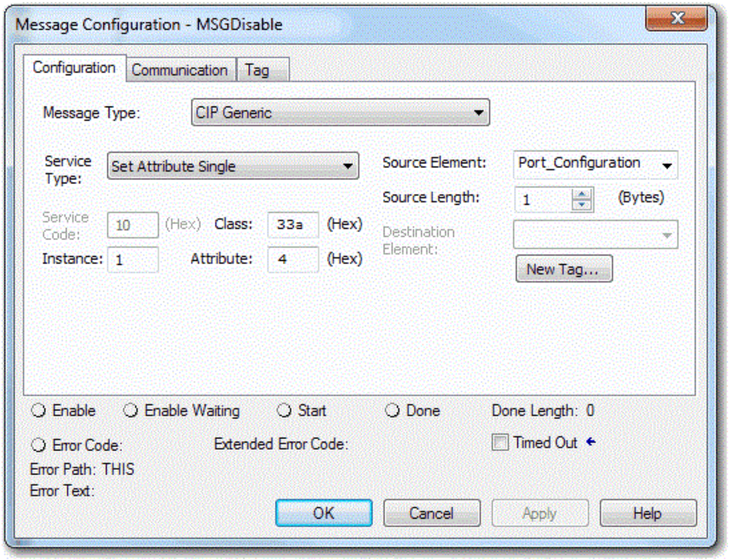
With the Studio 5000 Logix Designer application, version 32 or later, you can use a CIP Generic MSG with a Path of THIS to execute this option.

1. Add an MSG instruction to your program.

   This message has to execute only once and not with every program scan.

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

2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 36.



Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex)

Class: 33a (Hex)

Instance: 1

Attribute: 4 (Hex)

Source Element: Port_Configuration

Source Length: 1 (Bytes)

Destination Element:

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

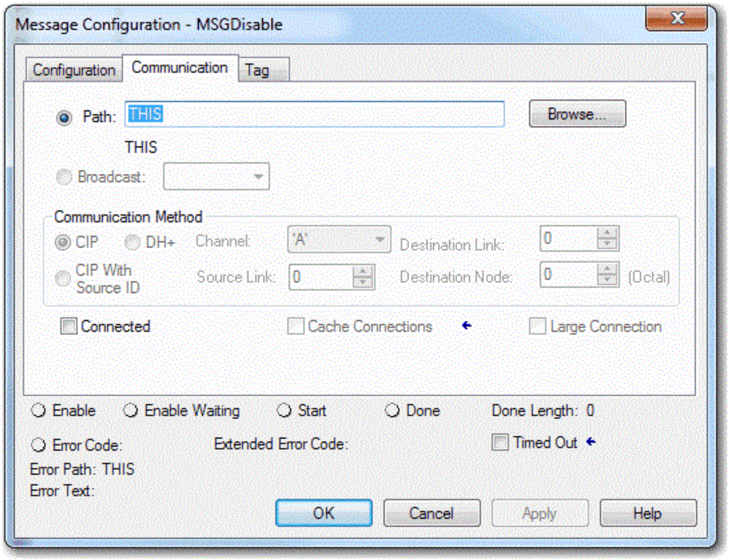
IMPORTANT	These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute up each time the controller powers up.

Table 36 - Disable the USB Port

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	33a
Attribute	4
Source Element	Controller tag of SINT data type. In this example, the Source Element is named Port_Configuration.
Source Length	1

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

IMPORTANT	Messages to THIS must be unconnected messages.


Message Configuration - MSGDisable

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

Disable the Controller SD Card

With the Studio 5000 Logix Designer application, version 32 or later, you can use a CIP Generic MSG with a Path of THIS to execute this option.

IMPORTANT Remember the following:

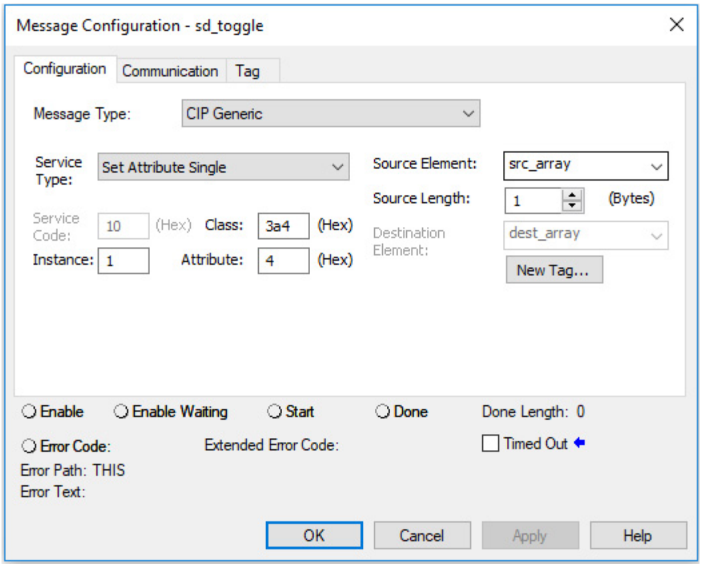
- An SD card can only be disabled with a Message to Self.
- Once an SD slot is disabled, you lose all ability to communicate to an SD card inserted into the slot. This includes any diagnostic information.

1. Add an MSG instruction to your program.

   This message only has to execute once, it does not need to execute with every program scan.

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

2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 37 on page 217.



Message Configuration - sd_toggle

Configuration | Communication | Tag

Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex) Class: 3a4 (Hex)

Instance: 1 Attribute: 4 (Hex)

Source Element: src_array

Source Length: 1 (Bytes)

Destination Element: dest_array

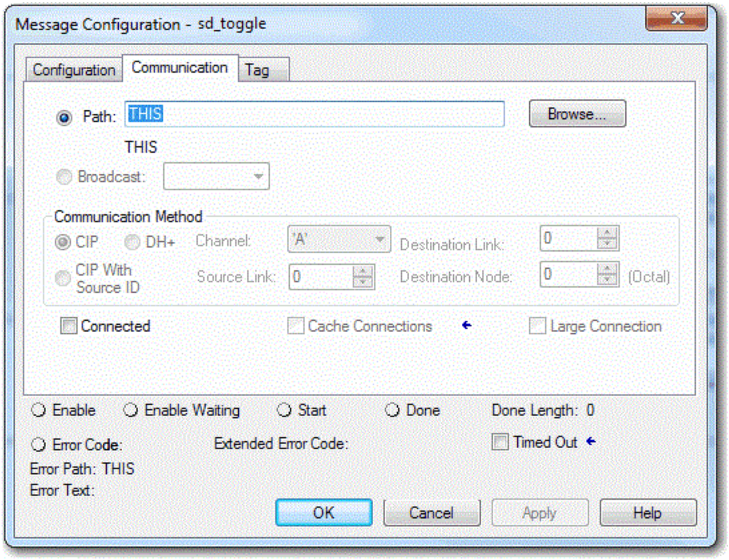
IMPORTANT These values are stored to non-volatile controller memory in such a way that the MSG instruction is not required to execute each time the controller powers up.

Table 37 - Disable the SD Card

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a4
Attribute	4
Source Element	Controller tag of SINT Array. In this example, the Source Element is named src_array.
Source Length	1

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

IMPORTANT Messages to THIS must be unconnected messages.



Message Configuration - sd_toggle

Configuration | Communication | Tag

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

Disable the 4-character Status Display

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

- Disable All Categories of Messages on page 218
- Disable Individual Categories of Messages on page 220

You use a CIP Generic MSG to execute each option.

IMPORTANT	You cannot disable these system messages, and they will always display: • Power-up messages, such as TEST, PASS, CHRG • Catalog number message • Firmware revision message • Major/Critical failure messages

The 4-character status display returns to the default setting after one of these actions occurs on the controller:

- Stage 1 reset
- Stage 2 reset
- New project is downloaded - In this case, the settings in the new project take effect.
- Program is cleared from the controller - these examples can clear the program from a controller:
  - A major nonrecoverable fault occurs.
  - A firmware update occurs.

You must reconfigure the settings to disable the 4-character status display after it returns to its default settings.

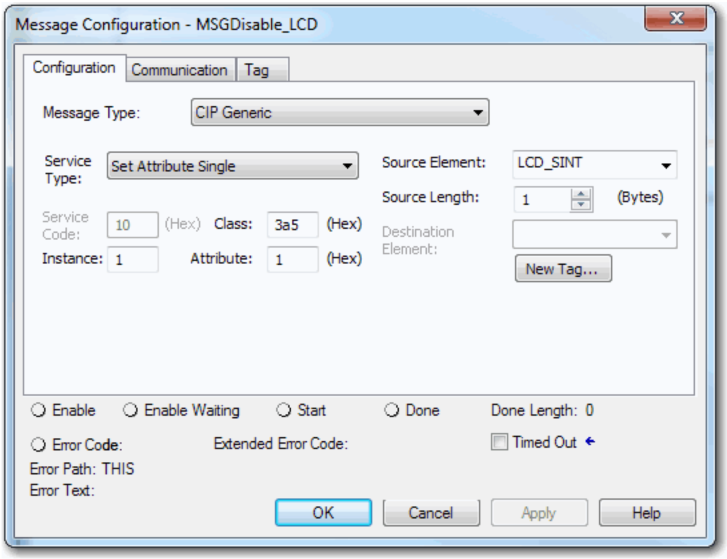
Disable All Categories of Messages

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

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

Complete these steps.

1. Add an MSG instruction to your program.
2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 38.



Message Configuration - MSGDisable_LCD

Configuration | Communication | Tag

Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex) Class: 3a5 (Hex)

Instance: 1 Attribute: 1 (Hex)

Source Element: LCD_SINT

Source Length: 1 (Bytes)

Destination Element:

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

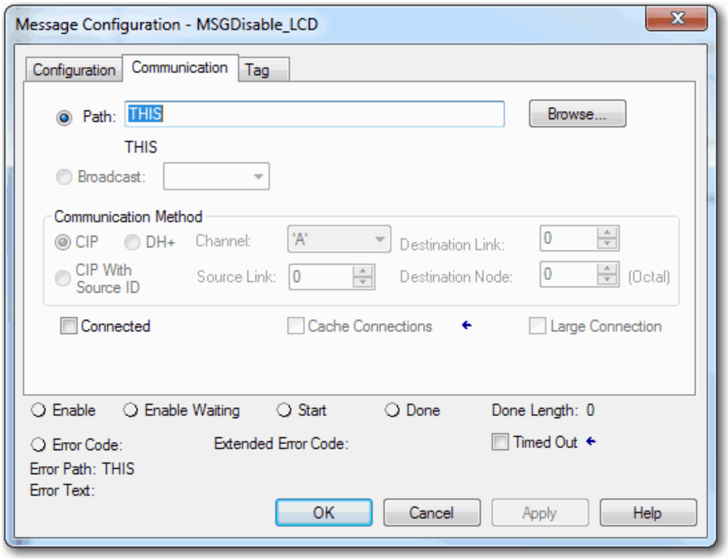
Error Text:

Table 38 - Disable All Categories of Messages

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

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

IMPORTANT Messages to THIS must be unconnected messages.



Message Configuration - MSGDisable_LCD

Configuration | Communication | Tag

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

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

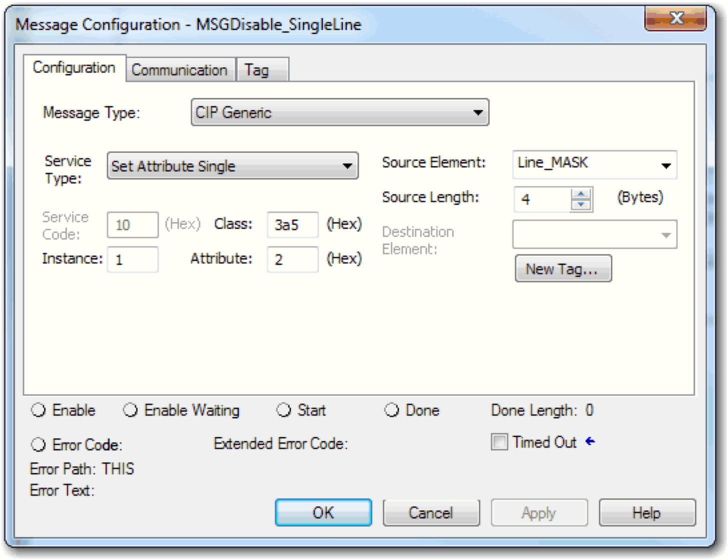
Complete these steps.

1. Add an MSG instruction to your program.

   This message only has to execute once, it does not need to execute with every program scan.

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

2. Configure the Configuration tab on the Message Configuration dialog box as described in Table 39.



Message Configuration - MSGDisable_SingleLine

Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex) Class: 3a5 (Hex)

Instance: 1 Attribute: 2 (Hex)

Source Element: Line_MASK

Source Length: 4 (Bytes)

Destination Element:

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

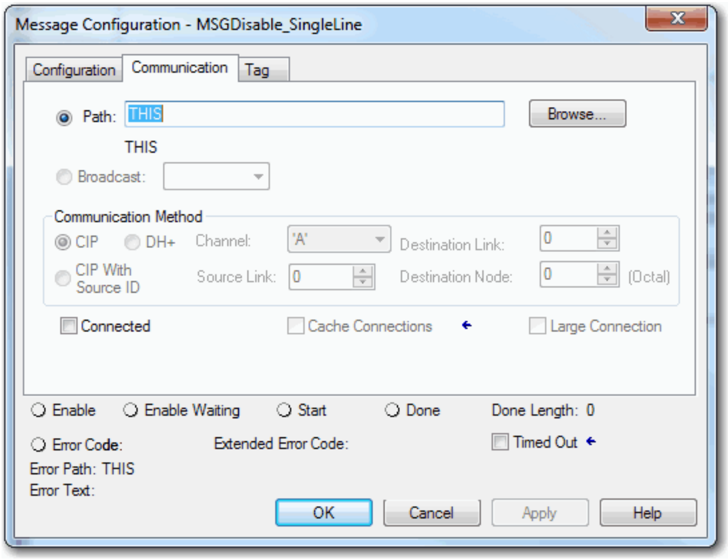
Error Text:

Table 39 - Disable Individual Categories of Messages

Field	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Instance	1
Class	3a5
Attribute	2
Source Element	Controller tag of DINT data type. In this example, the controller tag is named Line_MASK.
Source Length	4

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

IMPORTANT	Messages to THIS must be unconnected messages.



Message Configuration - MSGDisable_SingleLine

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

4. Before you enable the MSG instruction, make sure that the Source Element uses one of the following tag values that are based on what information that you want to disable:
   - Project name and link status - Bit 0 of the Source Element = 1
   - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT	You can re-enable the subsets of information on the 4-character display after they are disabled. To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, be sure that the appropriate bit in the Source Element tag value is 0.

Disable Controller Webpages

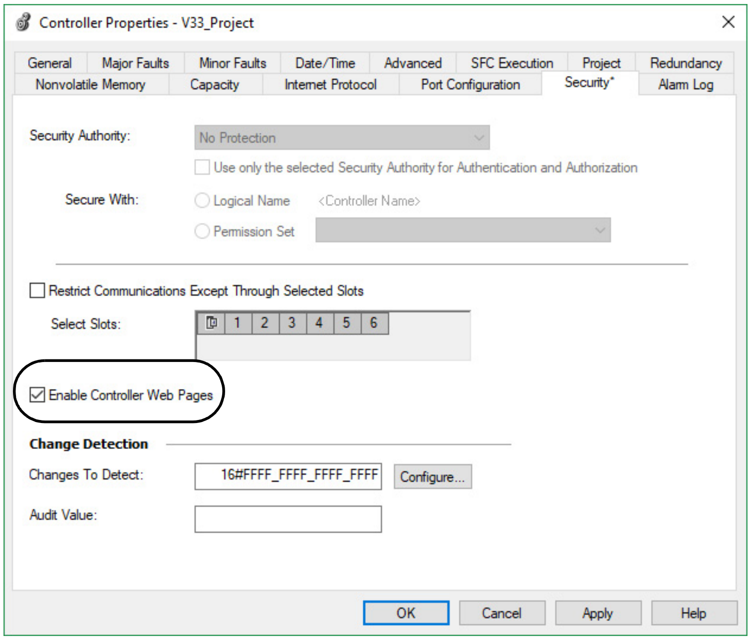
You can disable the controller webpages with the Studio 5000 Logix Designer application, version 28 or later.

Studio 5000 Logix Designer Application Version 33 or Later

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

While using a CIP Generic MSG to disable controller web pages is supported in version 33 or later, Rockwell Automation recommends the following method to disable the controller web pages.

If the controller web pages are enabled, disable them by clearing the Enable Controller Web Pages check box on the Security tab for the controller properties.



Controller Properties - V33_Project

Security Authority: No Protection

□ Use only the selected Security Authority for Authentication and Authorization

Secure With: ○ Logical Name <Controller Name>

○ Permission Set

□ Restrict Communications Except Through Selected Slots

Select Slots: 1 2 3 4 5 6

☑ Enable Controller Web Pages

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

Studio 5000 Logix Designer Application Version 32 or Earlier

For the Studio 5000 Logix Designer application, version 32 or earlier, use a CIP Generic MSG to enable or disable controller web pages:

- Use a CIP Generic MSG to Disable the Controller Web Pages on page 223
- Use a CIP Generic MSG to Enable the Controller Web Pages on page 226

Controller Web Page Default Settings

The default settings for controller web pages are as follows:

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

Controller web pages return to the default setting in these situations:

- A stage 1 reset for all versions of the Studio 5000 Logix Designer application.
- A stage 2 reset for all versions of the Studio 5000 Logix Designer application.

IMPORTANT	When you update the controller firmware to revision 33 or later without a reset, the controller retains the previous controller web page configuration (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:

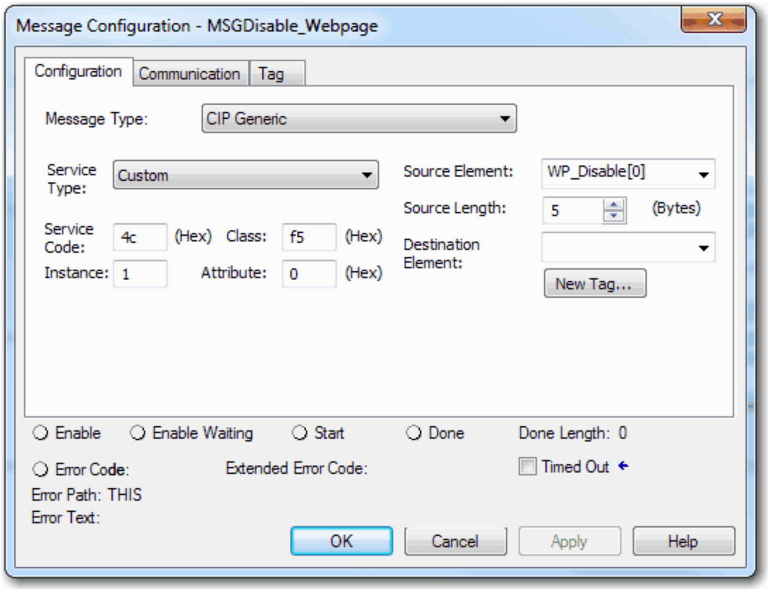
- New project is downloaded—in this case, the settings in the new project take effect.
- When the controller receives a configuration message, it takes the setting from the configuration message.

Use a CIP Generic MSG to Disable the Controller Web Pages

1. Add a MSG instruction to your program.

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

2. On the Configuration tab of the Message Configuration dialog box, complete the fields as described in Table 40.



Message Configuration - MSGDisable_Webpage

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex)

Instance: 1 Attribute: 0 (Hex)

Source Element: WP_Disable[0]

Source Length: 5 (Bytes)

Destination Element:

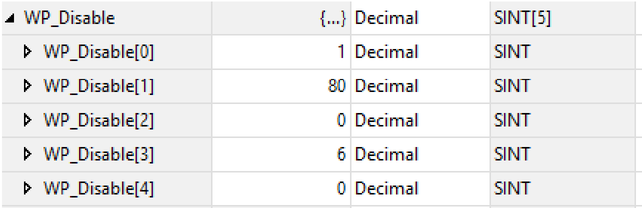
○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

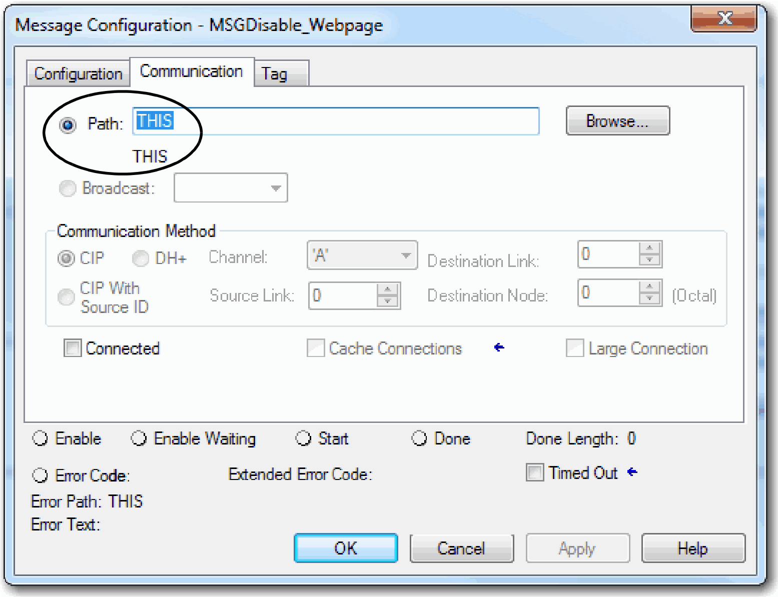
Error Path: THIS

Error Text:

Table 40 - Disable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode
Class	f5
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:  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 **IMPORTANT:** The Source Element tag in your Studio 5000 Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not disabled.
Source Length	5

3. On the Communication tab, configure a communication path of THIS.



Message Configuration - MSGDisable_Webpage

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

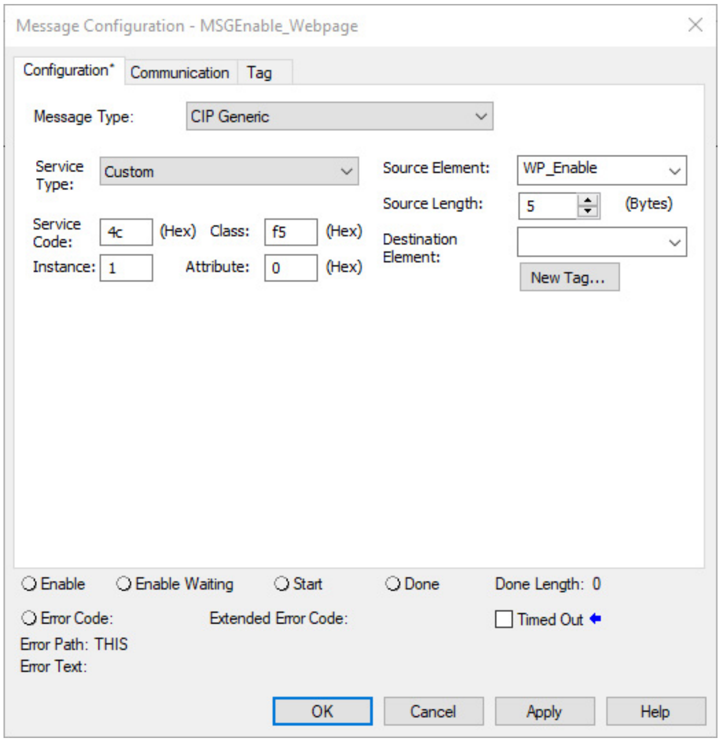
Error Text:

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 mode switch is in RUN mode, or if the FactoryTalk Security settings deny this editing option.

2. On the Configuration tab of the Message Configuration dialog box, complete the fields as described in Table 41.



Message Configuration - MSGEnable_Webpage

Configuration* | Communication | Tag

Message Type: CIP Generic

Service Type: Custom

Service Code: 4c (Hex) Class: f5 (Hex)

Instance: 1 Attribute: 0 (Hex)

Source Element: WP_Enable

Source Length: 5 (Bytes)

Destination Element:

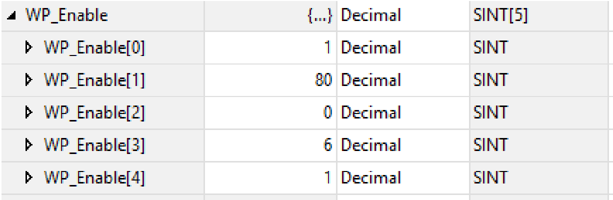
○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

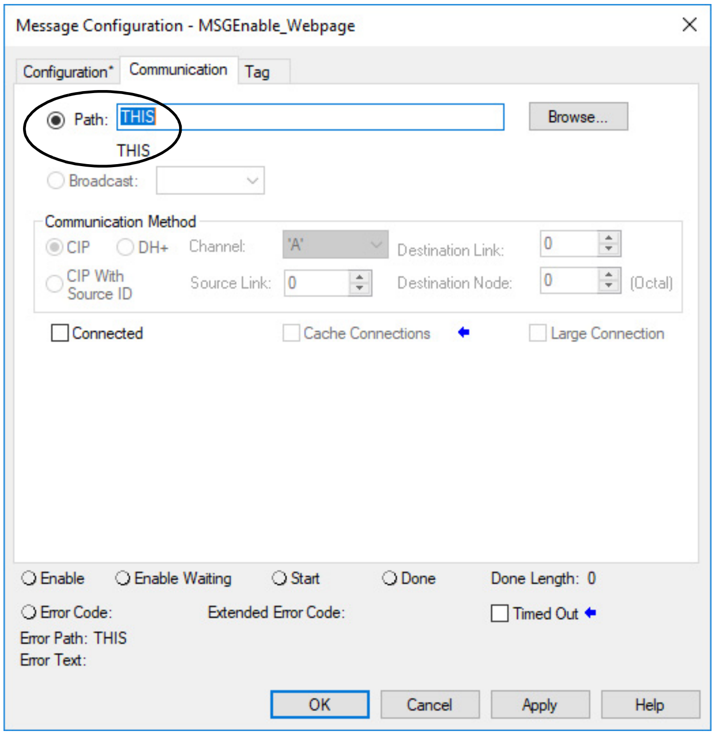
Error Text:

Table 41 - Enable the Webpages

Field	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Instance	1 for Linear/DLR mode 2 for Dual-IP mode
Class	f5
Attribute	0
Source Element	Controller tag of SINT[5] data type. In this example, the controller tag is named WP_Enable and must match the following graphic:  ◢ WP_Enable {...} Decimal SINT[5] ▷ WP_Enable[0] 1 Decimal SINT ▷ WP_Enable[1] 80 Decimal SINT ▷ WP_Enable[2] 0 Decimal SINT ▷ WP_Enable[3] 6 Decimal SINT ▷ WP_Enable[4] 1 Decimal SINT **IMPORTANT:** The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic. If you use values that are different than the ones shown, the controller webpages are not enabled.
Source Length	5

3. On the Communication tab, configure a communication path of THIS.

IMPORTANT	Messages to THIS must be unconnected messages.



Message Configuration - MSGEnable_Webpage

● Path: THIS

THIS

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destination Link: 0

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

□ Connected □ Cache Connections □ Large Connection

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path: THIS

Error Text:

Notes:

Develop Motion Applications

Overview

Applies to these controllers:
CompactLogix 5380 Motion Controllers
Compact GuardLogix 5380 SIL 2 Motion Controllers
Compact GuardLogix 5380 SIL 3 Motion Controllers

Some CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers support Integrated Motion over an EtherNet/IP™ network on digital and integrated motion interfaces.

- The controllers support these numbers of integrated motion axes:

CompactLogix 5380 Controllers	
5069-L306ERM	2
5069-L310ERM, 5069-L310ERMK	4
5069-L320ERM, 5069-L320ERP	8
5069-L330ERM	16
5069-L340ERM, 5069-L340ERP	20
5069-L350ERM	24
5069-L380ERM	28
5069-L3100ERM	32

Compact GuardLogix 5380 Controllers	
5069-L306ERMS2, 5069-L306ERMS3	2
5069-L310ERMS2, 5069-L310ERMS2K, 5069-L310ERMS3, 5069-L310ERMS3K	4
5069-L320ERMS2, 5069-L320ERMS2K, 5069-L320ERMS3, 5069-L320ERMS3K	8
5069-L330ERMS2, 5069-L330ERMS2K, 5069-L330ERMS3, 5069-L330ERMS3K	16
5069-L340ERMS2, 5069-L340ERMS3	20
5069-L350ERMS2, 5069-L350ERMS2K, 5069-L350ERMS3, 5069-L350ERMS3K	24
5069-L380ERMS2, 5069-L380ERMS3	28
5069-L3100ERMS2, 5069-L3100ERMS3	32

- Digital drive interfaces include EtherNet/IP connected drives.
- Integrated Motion over an EtherNet/IP network supports some Kinetix® drives and some PowerFlex® drives. For example, Kinetix 5700 and PowerFlex 755 drives.
- All CompactLogix 5380 and Compact GuardLogix 5380 controllers support single-axis motor control with PowerFlex variable frequency drives over an EtherNet/IP network.

  This functionality is available on CompactLogix 5380 and Compact GuardLogix 5380 controllers that do not support other aspects of Integrated Motion over an EtherNet/IP network.

For more information, see the following:

- 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.

Motion Overview

Applies to these controllers:
CompactLogix 5380 Motion Controllers
Compact GuardLogix 5380 SIL 2 Motion Controllers
Compact GuardLogix 5380 SIL 3 Motion Controllers

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. You can associate Integrated Motion axes to any appropriate drive.

The controllers do not support Analog or SERCOS motion.

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.
3. Create axis tags as needed.
4. Configure the drive.
5. Create axes as needed.

Program Motion Control

Applies to these controllers:
CompactLogix 5380 Motion Controllers
Compact GuardLogix 5380 SIL 2 Motion Controllers
Compact GuardLogix 5380 SIL 3 Motion Controllers

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

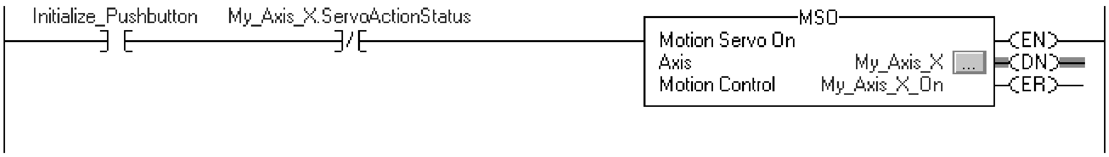
- The controller uses these instructions just like the rest of the Logix 5000™ instructions.
- Each motion instruction works on one or more axes.
- You can use motion control instructions in these programming languages:
  - Ladder Diagram (LD)
  - Structured Text (ST)
  - Sequential Function Chart (SFC)
- 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.

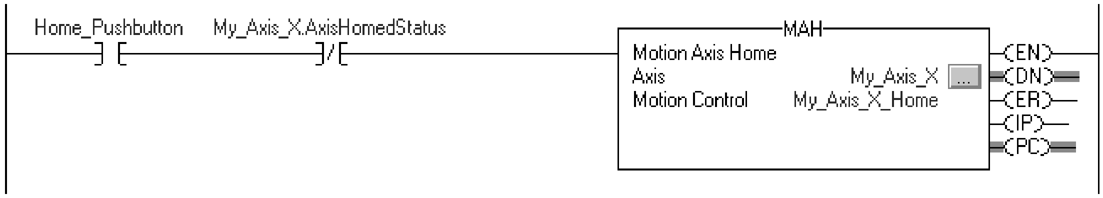
ATTENTION: Use each motion control tag in only one motion instruction. Unintended operation can result if you reuse the same motion control tag in other motion instructions, or if you write to any of the motion control tag elements.

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

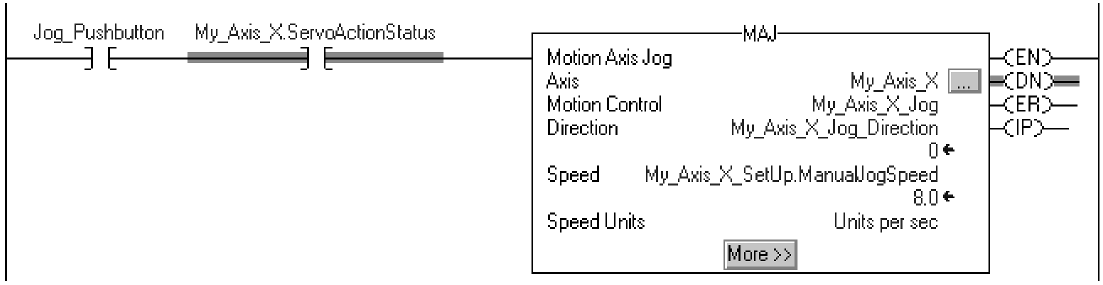
If Initialize_Pushbutton = on and the axis = off (My_Axis_X.ServoActionStatus = off), the MSO instruction turns on the axis.


Initialize_Pushbutton
My_Axis_X.ServoActionStatus
MSO
Motion Servo On
Axis My_Axis_X
Motion Control My_Axis_X_On

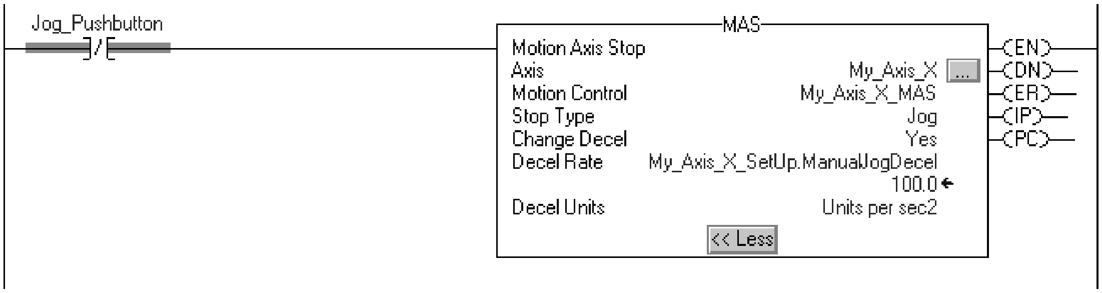
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off), the MAH instruction homes the axis.


Home_Pushbutton
My_Axis_X.AxisHomedStatus
MAH
Motion Axis Home
Axis My_Axis_X
Motion Control My_Axis_X_Home

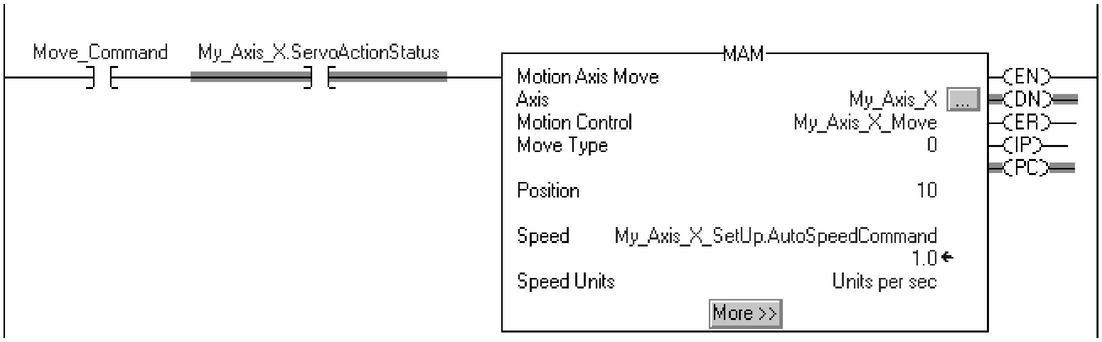
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on), the MAJ instruction jogs the axis forward at 8 units/second.


Jog_Pushbutton
My_Axis_X.ServoActionStatus
MAJ
Motion Axis Jog
Axis My_Axis_X
Motion Control My_Axis_X_Jog
Direction My_Axis_X_Jog_Direction
0
Speed My_Axis_X_SetUp.ManualJogSpeed
8.0
Speed Units Units per sec

If Jog_Pushbutton = off, the MAS instruction stops the axis at 100 units/.second^2. Make sure that Change Decel is Yes. Otherwise, the axis decelerates at its maximum speed.



If Move_Command = on and the axis = on (My_Axis_X.ServoActionStatus = on), the MAM instruction moves the axis. The axis moves to the position of 10 units at 1 unit/second.


Move_Command
My_Axis_X.ServoActionStatus
MAM
Motion Axis Move
Axis My_Axis_X
Motion Control My_Axis_X_Move
Move Type 0
Position 10
Speed My_Axis_X_SetUp.AutoSpeedCommand
1.0
Speed Units Units per sec
More >>
EN
DN
ER
IP
PC

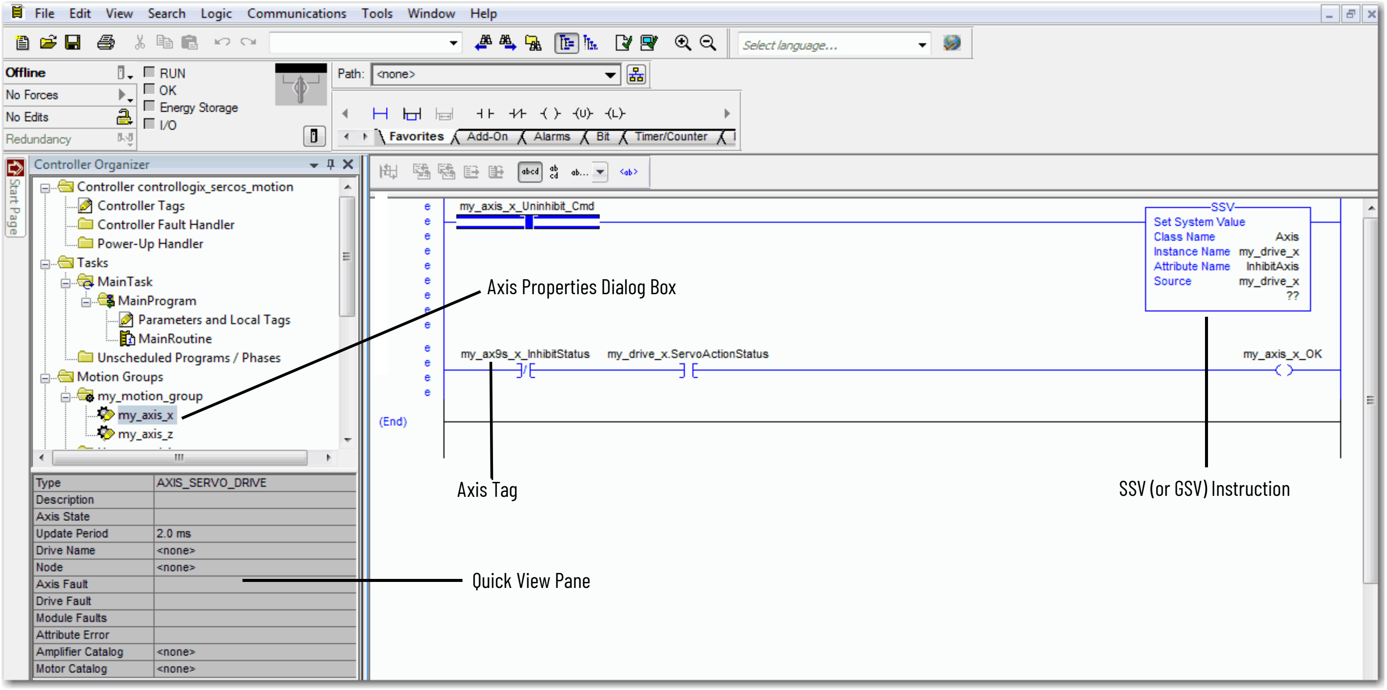
Obtain Axis Information

Applies to these controllers:
CompactLogix 5380 Motion Controllers
Compact GuardLogix 5380 SIL 2 Motion Controllers
Compact GuardLogix 5380 SIL 3 Motion Controllers

You can obtain axis information via 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 Quick View pane to see the state and faults of an axis.
- Use an axis tag for status and faults.

Figure 58 - Obtain Axis Information



Type	AXIS_SERVO_DRIVE
Description	
Axis State	
Update Period	2.0 ms
Drive Name	<none>
Node	<none>
Axis Fault	
Drive Fault	
Module Faults	
Attribute Error	
Amplifier Catalog	<none>
Motor Catalog	<none>

Notes:

Troubleshoot the Controller

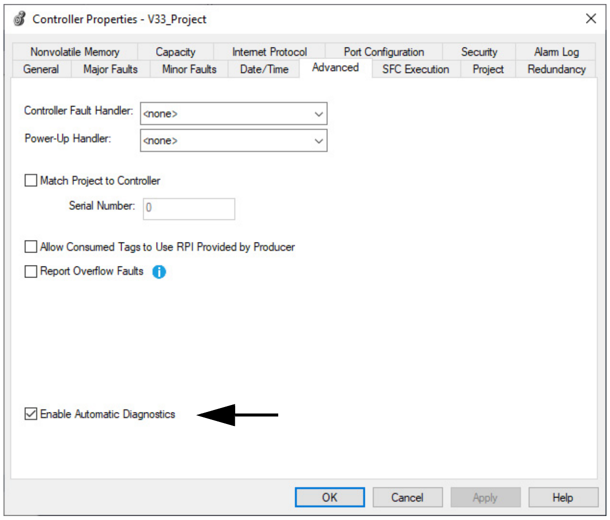
This chapter describes how to troubleshoot the controller if issues occur during normal operation.

You can use messages on the 4-character display to troubleshoot the controller. For more information, see Appendix A, Status Indicators on page 253.

Automatic Diagnostics

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

Automatic Diagnostics is enabled by default in Logix 5000 controllers with firmware revision 33 and 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.



Controller Fault Handler: <none>

Power-Up Handler: <none>

☐ Match Project to Controller

Serial Number: 0

☐ Allow Consumed Tags to Use RPI Provided by Producer

☐ Report Overflow Faults

☑ Enable Automatic Diagnostics

Considerations for Communication Loss Diagnostics

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

Type of Connection	Device Behavior
Direct connection to a Logix 5000 controller	Device reports communication loss.The device communication loss can be replaced by the diagnostics of a communication adapter
No connection to a Logix 5000 controller	Communication adapters that do not have a connection to the controller do not report communication loss diagnostics. To enable timely reporting of any communication loss, we recommend that you configure communication adapters for a status connection.
Data connection	Device reports communication loss. The device communication loss can be replaced by the diagnostics of a communication adapter
Rack-optimized connection	Device does not report communication loss diagnostics. The communication adapter reports communication loss diagnostics. A device with a rack optimized connection has a reduced set of diagnostics as compared to a direct connection.

When enabled, the Automatic Diagnostics feature enables:

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

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

Controller Diagnostics with Logix Designer

Table 42 -

Applies to these controllers:
CompactLogix™ 5380
Compact GuardLogix® 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can use the Controller Properties in the Studio 5000 Logix Designer® application to view fault conditions in these ways:

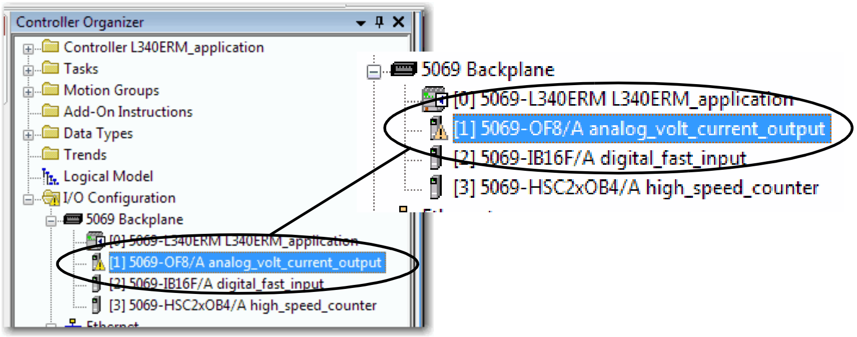
- Warning Symbol in the I/O Configuration Tree
- Categories on I/O Module Properties Dialog
- Notification in the Tag Monitor
- Fault Information in the Controller Properties Dialog Box
- Port Diagnostics
- Advanced Time Sync

Warning Symbol in the I/O Configuration Tree

IMPORTANT	**Safety Consideration** You cannot configure safety connections to automatically fault the controller.

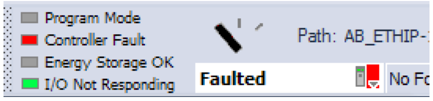
A warning symbol appears in the controller organizer next to the I/O module. This occurs when there are faults or other conditions in the I/O module, or if the connection to the I/O module fails while in run mode.

Figure 59 - Warning Symbol on I/O Module


Controller Organizer
Controller L340ERM_application
Tasks
Motion Groups
Add-On Instructions
Data Types
Trends
Logical Model
I/O Configuration
5069 Backplane
[0] 5069-L340ERM L340ERM_application
[1] 5069-OF8/A analog_volt_current_output
[2] 5069-IB16F/A digital_fast_input
[3] 5069-HSC2xOB4/A high_speed_counter
Ethernet
5069 Backplane
[0] 5069-L340ERM L340ERM_application
[1] 5069-OF8/A analog_volt_current_output
[2] 5069-IB16F/A digital_fast_input
[3] 5069-HSC2xOB4/A high_speed_counter

The following conditions are possible:

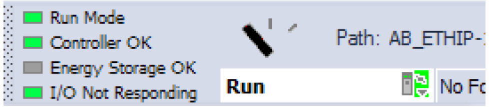
- When the I/O module is configured to cause a major fault on the controller and an I/O module fault occurs, the following can result:
  - Controller state displays Faulted.
  - Controller status displays Controller Fault and is steady red.
  - I/O module status displays I/O Not Responding and blinks green.



IMPORTANT	The descriptions in the Logix Designer application can change based on the controller mode and status.

IMPORTANT	**Safety Consideration** You cannot configure safety connections to automatically fault the controller.

- When the I/O module is not configured to cause a major fault on the controller and an I/O module fault occurs, the following result:
  - Controller state displays the current state, for example, Rem Run.
  - Controller status displays Controller OK and is steady green.
  - I/O module status displays I/O Not Responding and blinks green.



🟩 Run Mode
🟩 Controller OK
▨ Energy Storage OK
🟩 I/O Not Responding

Categories on I/O Module Properties Dialog

The Module Properties dialog for I/O modules includes a series of categories. You can use some of the categories to troubleshoot the controller.

IMPORTANT	The number and type of categories varies by I/O module type.

The following are examples of ways to use categories on the Module Properties dialog box when you troubleshoot a controller:

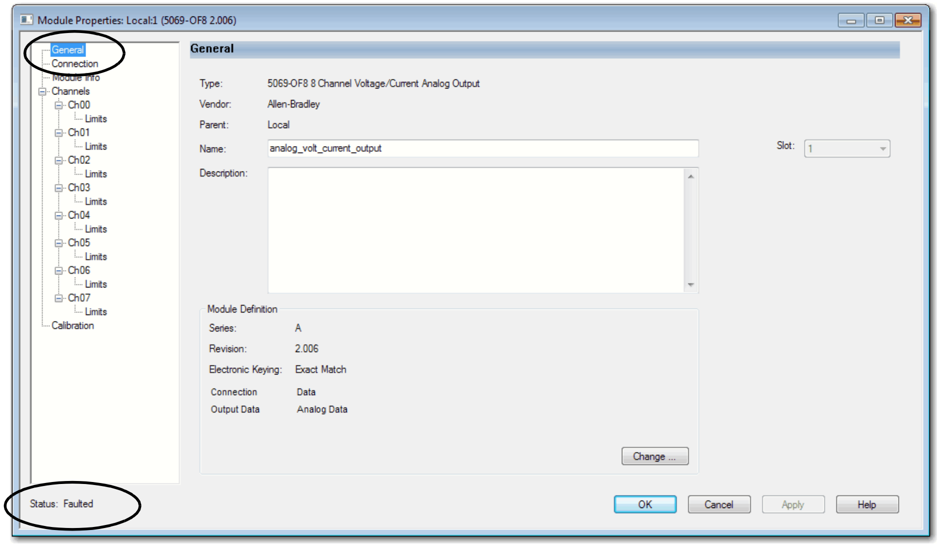
- Module Status on General Category
- Module Fault Descriptions on Connection Category
- Module Fault Descriptions on Module Info Category
- Diagnostics Option on Module Info Category

The categories that are described in this section display the module status. When a fault exists, the text is **Status: Faulted** in the module status line as shown in Figure 60.

Module Status on General Category

The General category displays the module status.

Figure 60 - Module Status in Fault Message Line



Module Properties: Local:1 (5069-OF8 2.006)

General

Type: 5069-OF8 8 Channel Voltage/Current Analog Output
Vendor: Allen-Bradley
Parent: Local
Name: analog_volt_current_output
Slot: 1
Description:

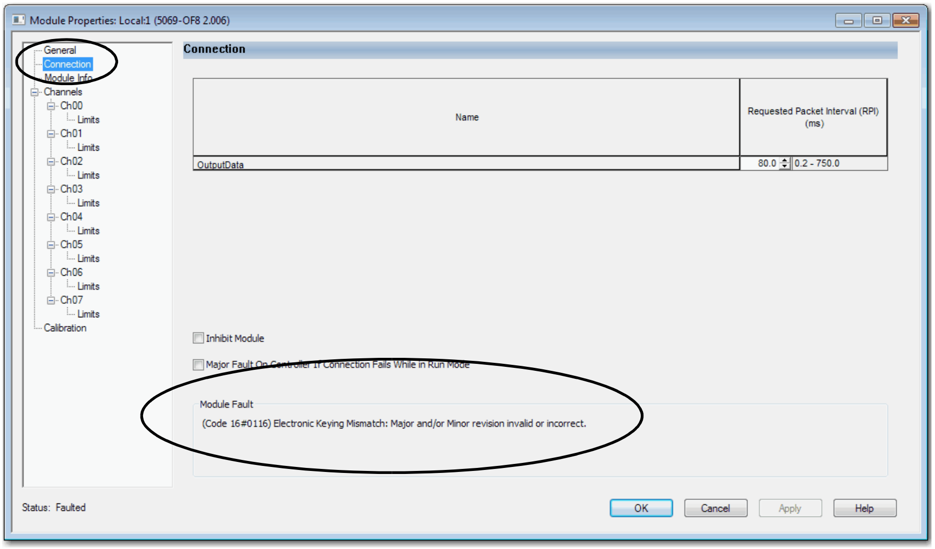
Module Definition
Series: A
Revision: 2.006
Electronic Keying: Exact Match
Connection Data
Output Data Analog Data

Status: Faulted

Module Fault Descriptions on Connection Category

The Connection category displays the module fault description that includes an error code that is associated with the specific fault type.

Figure 61 - Fault Description with Error Code



Module Properties: Local:1 (5069-OF8 2.006)

Connection

Name	Requested Packet Interval (RPI) (ms)	
OutputData	80.0	0.2 - 750.0

□ Inhibit Module

□ Major Fault On Controller If Connection Fails While in Run Mode

Module Fault

(Code 16#0116) Electronic Keying Mismatch: Major and/or Minor revision invalid or incorrect.

Status: Faulted

Module Fault Descriptions on Module Info Category

When you click the Module Info category, a dialog box displays the module fault description and the corresponding fault code. Click OK to access the Module Info category.

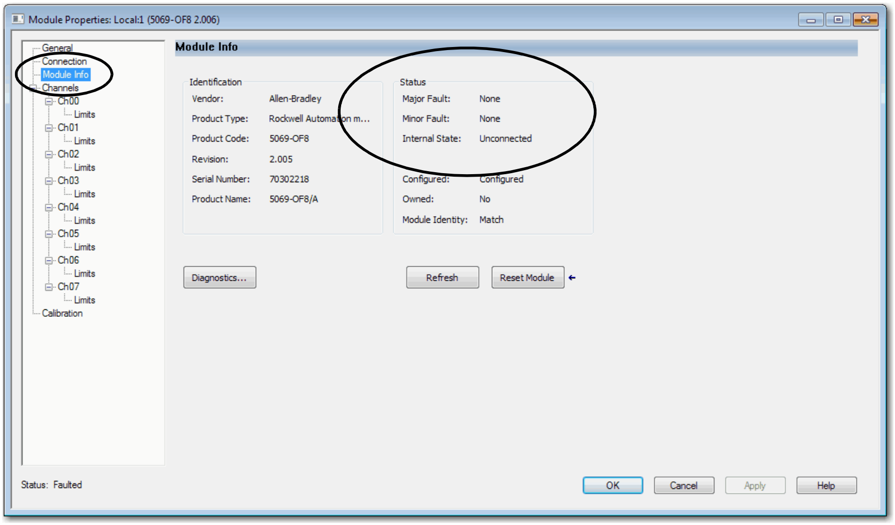
The Module Info tab requires successful communications to help you troubleshoot the fault effectively. Consider the following:

- If communication to the I/O module is OK, but the module is faulted, we recommend that you use the Module Info category to troubleshoot the fault.
- If communication to the I/O module is faulted, we recommend that you use the Connection category to troubleshoot the fault.

On the Module Info category, the Status section displays the following about the I/O module:

- Major and Minor Faults
- Internal State

Figure 62 - Major and Minor Fault Information



Module Properties: Local:1 (5069-OF8 2.006)

Module Info

Identification

Vendor: Allen-Bradley
Product Type: Rockwell Automation m...
Product Code: 5069-OF8
Revision: 2.005
Serial Number: 70302218
Product Name: 5069-OF8/A

Status

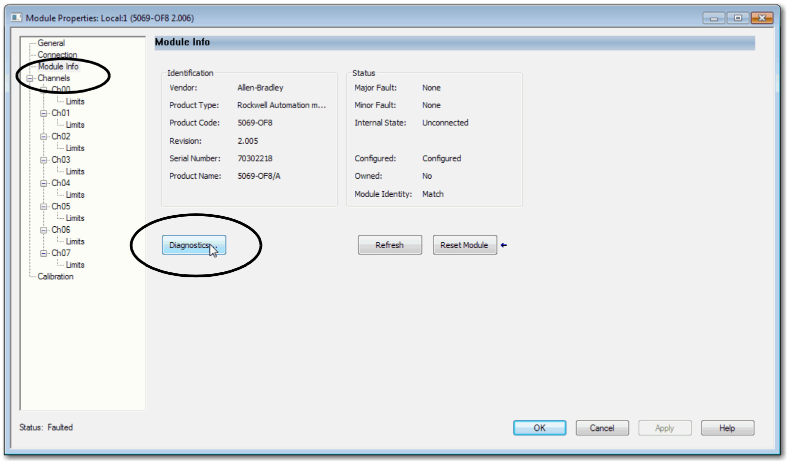
Major Fault: None
Minor Fault: None
Internal State: Unconnected
Configured: Configured
Owned: No
Module Identity: Match

Status: Faulted

Diagnostics Option on Module Info Category

You can access the diagnostics for a module from the Module Info category. Click Diagnostics, to access the Module Diagnostics dialog box.

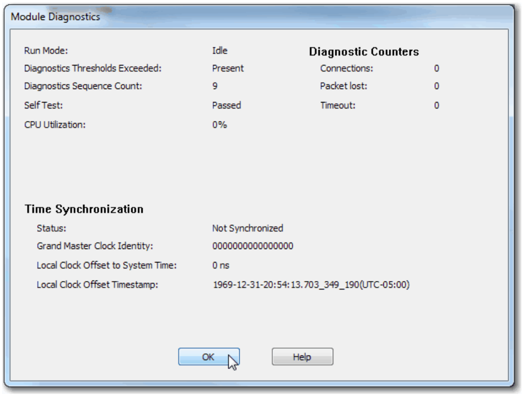
Figure 63 - Module Diagnostics



Identification
Vendor: Allen-Bradley
Product Type: Rockwell Automation m...
Product Code: 5069-OF8
Revision: 2.005
Serial Number: 70302218
Product Name: 5069-OF8/A

Status
Major Fault: None
Minor Fault: None
Internal State: Unconnected
Configured: Configured
Owned: No
Module Identity: Match

Status: Faulted



Run Mode: Idle
Diagnostics Thresholds Exceeded: Present
Diagnostics Sequence Count: 9
Self Test: Passed
CPU Utilization: 0%

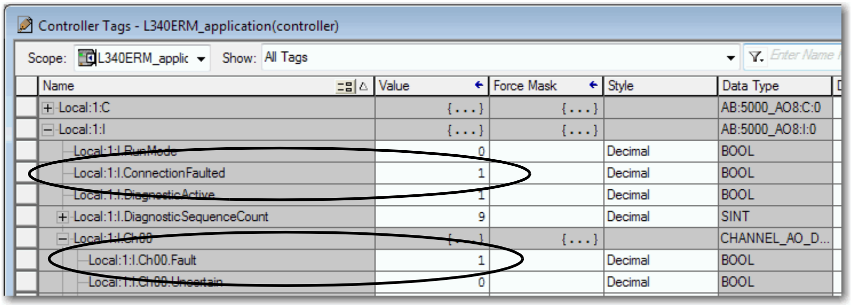
Diagnostic Counters
Connections: 0
Packet lost: 0
Timeout: 0

Time Synchronization
Status: Not Synchronized
Grand Master Clock Identity: 0000000000000000
Local Clock Offset to System Time: 0 ns
Local Clock Offset Timestamp: 1969-12-31-20:54:13.703_349_190(UTC-05:00)

Notification in the Tag Monitor

General and diagnostic module faults are reported in the Tag monitor of your Logix Designer application project.

The Value field indicates a fault with the number 1.



Name	Value	Force Mask	Style	Data Type
+ Local:1:C	{...}	{...}		AB:5000_AO8:C:0
− Local:1:I	{...}	{...}		AB:5000_AO8:I:0
Local:1:I.RunMode	0		Decimal	BOOL
Local:1:I.ConnectionFaulted	1		Decimal	BOOL
Local:1:I.DiagnosticActive	1		Decimal	BOOL
+ Local:1:I.DiagnosticSequenceCount	9		Decimal	SINT
− Local:1:I.Ch00	{...}	{...}		CHANNEL_AO_D...
Local:1:I.Ch00.Fault	1		Decimal	BOOL
Local:1:I.Ch00.Uncertain	0		Decimal	BOOL

Fault Information in the Controller Properties Dialog Box

You can use these tabs on the Controller Properties dialog box to troubleshooting the controller:

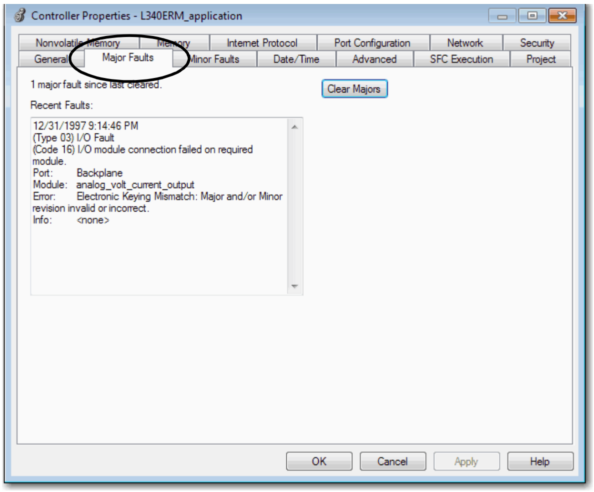
- Major Faults
- Minor Faults
- Network

Major Faults

You can monitor information about recent major faults and also clear major faults on the Major Faults tab.

Figure 64 - Major Faults Tab in Controller Properties Dialog Box

CompactLogix 5380 Controller



1 major fault since last cleared.

Recent Faults:

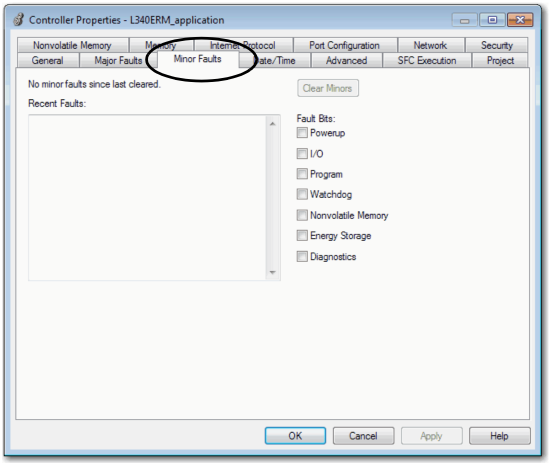
```
12/31/1997 9:14:46 PM
(Type 03) I/O Fault
(Code 16) I/O module connection failed on required
module.
Port:      Backplane
Module:    analog_volt_current_output
Error:     Electronic Keying Mismatch: Major and/or Minor
revision invalid or incorrect.
Info:      <none>
```

Minor Faults

You can monitor information about recent minor faults and also clear minor faults on the Minor Faults tab.

Figure 65 - Minor Faults Tab in Controller Properties Dialog Box

CompactLogix 5380 Controller



No minor faults since last cleared.

Recent Faults:

Fault Bits:

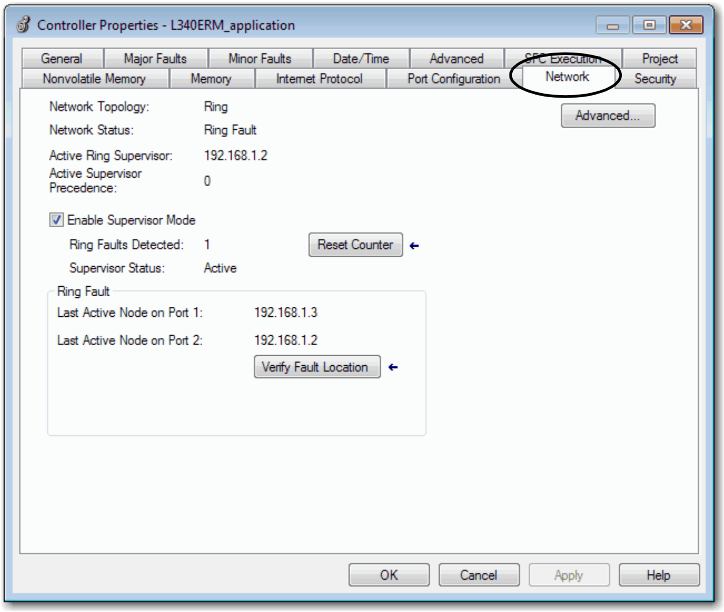
□ Powerup
□ I/O
□ Program
□ Watchdog
□ Nonvolatile Memory
□ Energy Storage
□ Diagnostics

Network

Typically, the Network tab is used to monitor for faults that occur when the controller is used in a DLR network.

IMPORTANT The Network tab is not available when the controller operates in Dual-IP mode.

Figure 66 - Network Tab in Controller Properties Dialog Box



Network Topology: Ring
Network Status: Ring Fault
Active Ring Supervisor: 192.168.1.2
Active Supervisor Precedence: 0

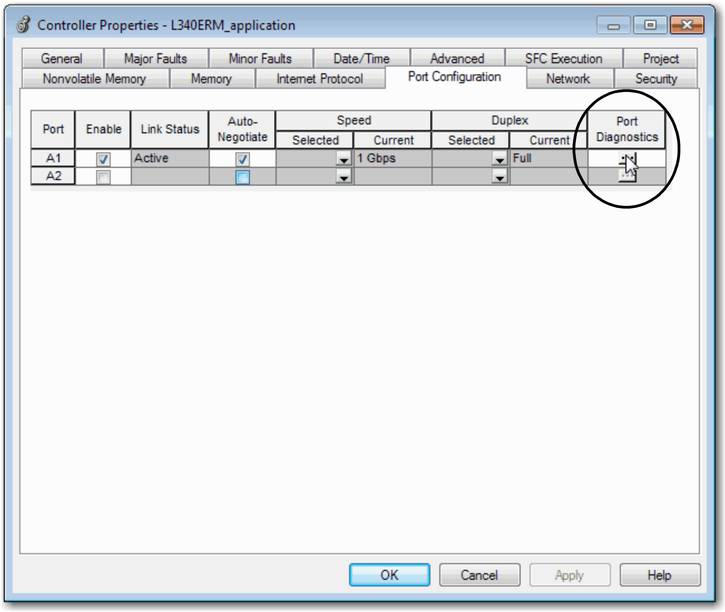
☑ Enable Supervisor Mode
Ring Faults Detected: 1
Supervisor Status: Active

Ring Fault
Last Active Node on Port 1: 192.168.1.3
Last Active Node on Port 2: 192.168.1.2

Port Diagnostics

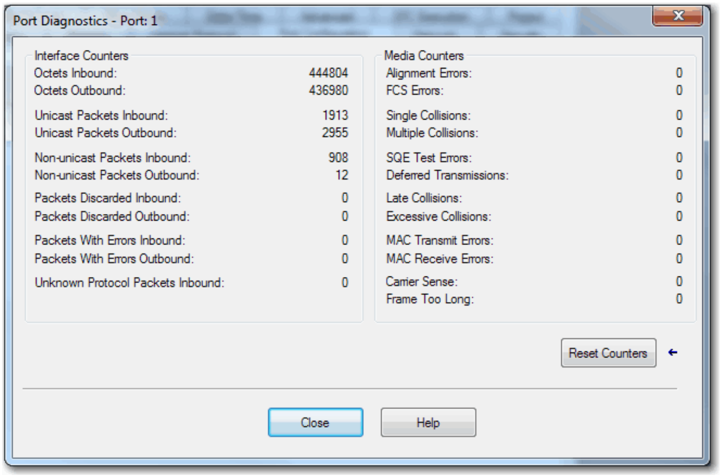
When your project is online, you can view the status of the embedded Ethernet ports on the controller.

1. Access the Controller Properties.
2. Click the Port Configuration tab.
3. On the Port Configuration tab, click the Port Diagnostics button for an active port.



Port	Enable	Link Status	Auto-Negotiate	Speed		Duplex		Port Diagnostics
				Selected	Current	Selected	Current	
A1	☑	Active	☑		1 Gbps		Full	
A2	☐		☐					

The Port Diagnostics page, displays information for the port. See Table 43 on page 240 for parameter descriptions.


Port Diagnostics - Port: 1

Interface Counters
Octets Inbound: 444804
Octets Outbound: 436980
Unicast Packets Inbound: 1913
Unicast Packets Outbound: 2955
Non-unicast Packets Inbound: 908
Non-unicast Packets Outbound: 12
Packets Discarded Inbound: 0
Packets Discarded Outbound: 0
Packets With Errors Inbound: 0
Packets With Errors Outbound: 0
Unknown Protocol Packets Inbound: 0

Media Counters
Alignment Errors: 0
FCS Errors: 0
Single Collisions: 0
Multiple Collisions: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
MAC Transmit Errors: 0
MAC Receive Errors: 0
Carrier Sense: 0
Frame Too Long: 0

Table 43 - Port Diagnostics Parameters - Logix Designer

Parameter	Description
Interface Counters	The Interface Counters values have no value when you cannot communicate out of the port.
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.

Table 43 - Port Diagnostics Parameters - Logix Designer (Continued)

Parameter	Description
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. Reset Counter appears dimmed when: • offline • online and a communication error has occurred

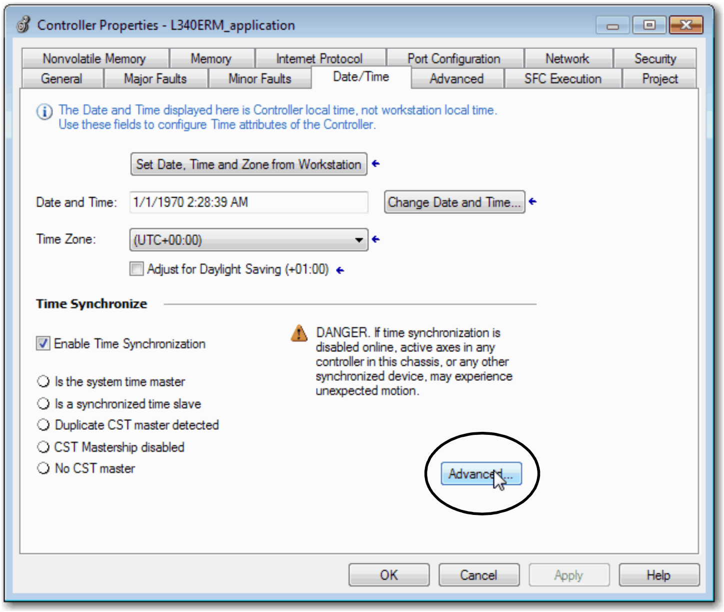
Advanced Time Sync

The Advanced Time Sync dialog displays information that is related to CIP Sync™ time synchronization, also known as Precision Time Protocol (PTP). The information appears only if the project is online and Enable Time Synchronization is selected on the Date/Time tab. Also, when the controller operates in Dual-IP mode, the Advanced Time Sync tab provides data for each port.

IMPORTANT

- Access to software that manages/updates the PTP 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 tab, click the Advanced button.



Controller Properties - L340ERM_application

The Date and Time displayed here is Controller local time, not workstation local time. Use these fields to configure Time attributes of the Controller.

Date and Time: 1/1/1970 2:28:39 AM

Time Zone: (UTC+00:00)

□ Adjust for Daylight Saving (+01:00)

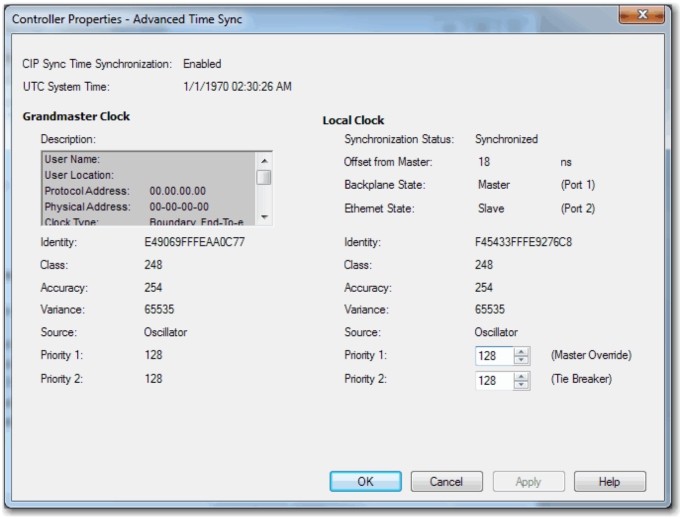
Time Synchronize

☑ Enable Time Synchronization

○ Is the system time master
○ Is a synchronized time slave
○ Duplicate CST master detected
○ CST Mastership disabled
○ No CST master

DANGER. If time synchronization is disabled online, active axes in any controller in this chassis, or any other synchronized device, may experience unexpected motion.

The Advanced Time Sync dialog box opens. See Table 44 for parameter descriptions.



Controller Properties - Advanced Time Sync

CIP Sync Time Synchronization: Enabled
UTC System Time: 1/1/1970 02:30:26 AM

Grandmaster Clock

Description:
User Name:
User Location:
Protocol Address: 00.00.00.00
Physical Address: 00-00-00-00
Clock Type: Boundary End-To-e

Identity: E49069FFFEAA0C77
Class: 248
Accuracy: 254
Variance: 65535
Source: Oscillator
Priority 1: 128
Priority 2: 128

Local Clock

Synchronization Status: Synchronized
Offset from Master: 18 ns
Backplane State: Master (Port 1)
Ethemet State: Slave (Port 2)

Identity: F45433FFFE9276C8
Class: 248
Accuracy: 254
Variance: 65535
Source: Oscillator
Priority 1: 128 (Master Override)
Priority 2: 128 (Tie Breaker)

Table 44 - Time Sync Parameters

Grandmaster Clock	
Description	Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified: • User Name • User Location • Protocol Address • Physical Address • Clock Type • Manufacturer Name • Model • Serial Number • Hardware Revision • Firmware Revision • Software Version • Profile Identity • Physical Protocol • Network Protocol • Port Number Use the vertical scroll bar to view the data.
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol. Ethernet network encodes the MAC address into the identifier.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0…255 with zero as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to the PTP epoch. The accuracy is specified as a graduated scale that starts at 25 nsec and ends at greater than 10 seconds or unknown. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the time source of the Grandmaster clock. The available values are: • Atomic Clock • GPS • Radio • PTP • NTP • HAND set • Other • Oscillator
Priority 1 / Priority 2	Displays the relative priority of the Grandmaster clock to other clocks in the system. The priority values range from 0…255. The highest priority is zero. The default value for both settings is 128.

Table 44 - Time Sync Parameters (Continued)

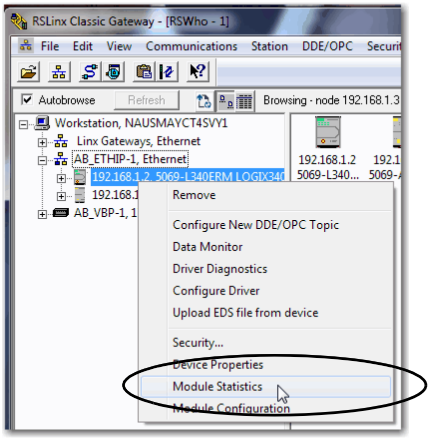
Local Clock	
Synchronization Status	Displays whether the local clock is synchronized or not synchronized with the Grandmaster reference clock. A clock is synchronized if it has one port in the slave state and is receiving updates from the time master.
Offset to Master	Displays the amount of deviation between the local clock and the Grandmaster clock in nanoseconds.
Backplane State	Displays the current state of the backplane. The available values are as follows: • Initializing • Faulty • Disabled • Listening • PreMaster • Master • Passive • Uncalibrating • Slave • None
Ethernet State	Displays the state of the Ethernet port. The available values are as follows: • Initializing • Faulty • Disabled • Listening • PreMaster • Master • Passive • Uncalibrating • Slave • None **IMPORTANT**: When the controller operates in Dual-IP mode, this attribute provides data for each controller port. The fields appear as follows: • A1, Ethernet State • A2, Ethernet State
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: • Atomic Clock • GPS • Terrestrial Radio • PTP • NTP • HAND set • Other • Oscillator

Controller Diagnostics with Linx-based Software

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

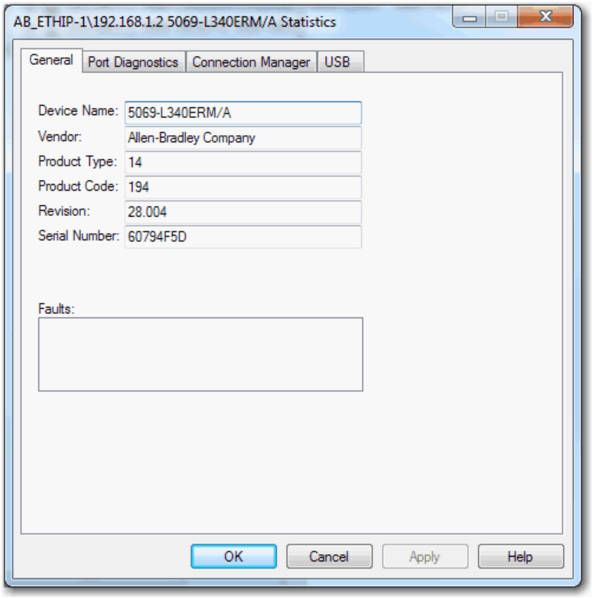
You can also view diagnostic information in Linx-based software.

1. Use the RSWho button to browse.
2. Navigate to the Ethernet network.
3. Right-click the controller and choose Module Statistics.


RSLinx Classic Gateway - [RSWho - 1]
File Edit View Communications Station DDE/OPC Securi
Autobrowse
Refresh
Browsing - node 192.168.1.3
Workstation, NAUSMAYCT4SVY1
Linx Gateways, Ethernet
AB_ETHIP-1, Ethernet
192.168.1.2, 5069-L340ERM LOGIX340
192.168.1
AB_VBP-1, 1
192.168.1.2
5069-L340...
192.1
5069-
Remove
Configure New DDE/OPC Topic
Data Monitor
Driver Diagnostics
Configure Driver
Upload EDS file from device
Security...
Device Properties
Module Statistics
Module Configuration

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 port.
- The Connection Manager Tab shows information on connection requests.
- The USB tab shows information about the USB port.


AB_ETHIP-1\192.168.1.2 5069-L340ERM/A Statistics

General | Port Diagnostics | Connection Manager | USB

Device Name: 5069-L340ERM/A
Vendor: Allen-Bradley Company
Product Type: 14
Product Code: 194
Revision: 28.004
Serial Number: 60794F5D

Faults:

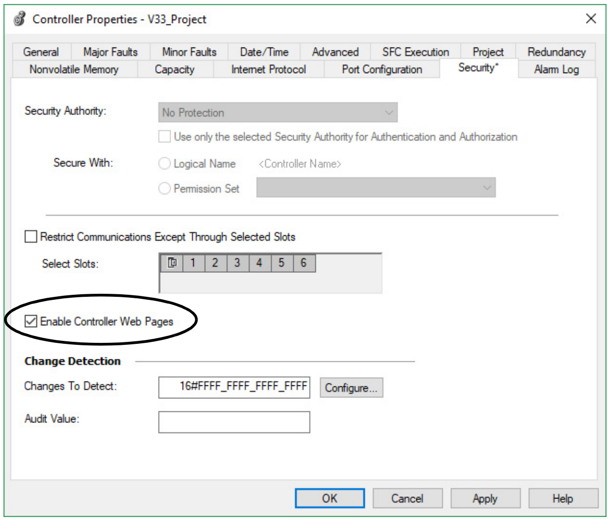
Controller Web Pages

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controller provides diagnostic web pages that track controller perfo rmance, network performance, and backplane performance.

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.


Controller Properties - V33_Project

Security Authority: No Protection

☐ Use only the selected Security Authority for Authentication and Authorization

Secure With: ○ Logical Name <Controller Name>

○ Permission Set

☐ Restrict Communications Except Through Selected Slots

Select Slots: 1 2 3 4 5 6

☑ Enable Controller Web Pages

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

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.
3. To access the information that you need, use the links in the left-side navigation bar.

IMPORTANT The controller web pages are slightly different based on the EtherNet/IP™ mode that is used. The web pages look different and provide different information.

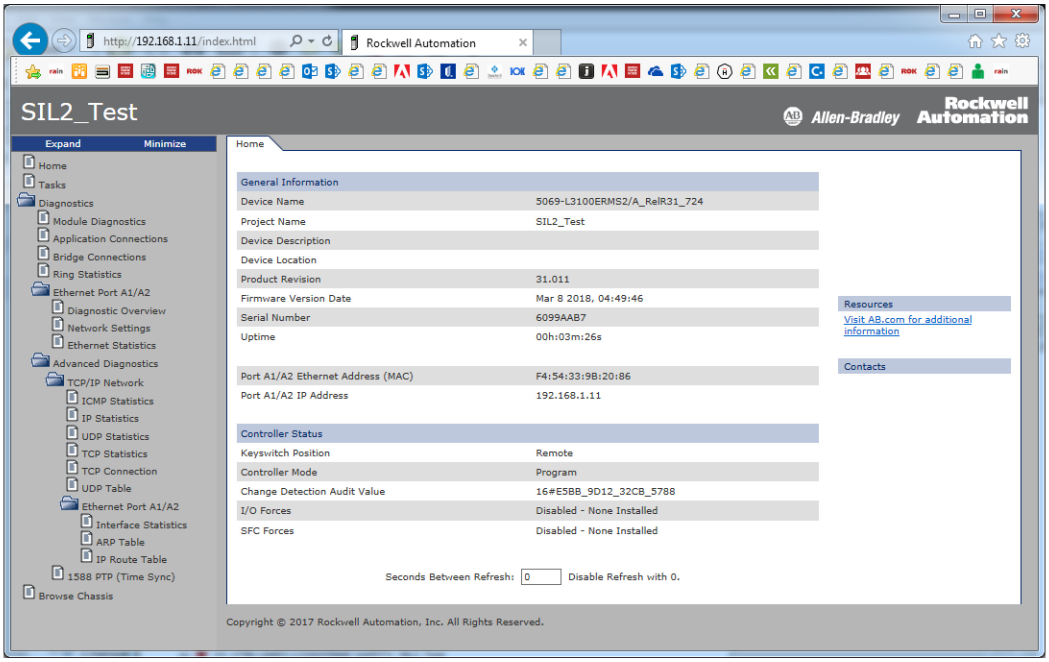
For example, consider the following:

- When the controller operates in Linear/DLR mode, the left-side navigation bar displays a Ethernet Port A1/A2 folder with three tabs. There is one Ethernet Port web page for both ports, and the controller web pages provide one set of Ethernet data.
- When the controller operates in Dual-IP mode, the left-side navigation bar displays an Ethernet Port A1 folder and an Ethernet Port A2 folder. Each folder has three tabs. There is an Ethernet Port web page for each port, and the controller web pages provide one set of Ethernet data for port A1 and another set of Ethernet data for port A2.

Home Web Page

The Home web page provides device information and controller status.

Linear/DLR Mode



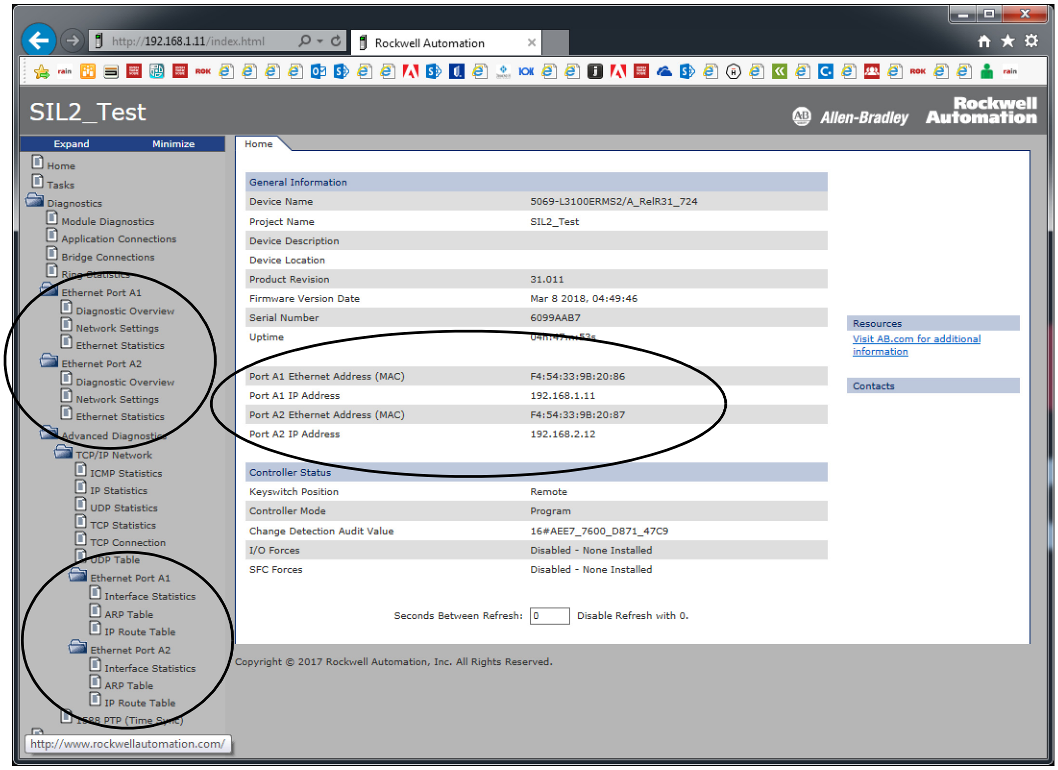
General Information	
Device Name	5069-L3100ERMS2/A_RelR31_724
Project Name	SIL2_Test
Device Description	
Device Location	
Product Revision	31.011
Firmware Version Date	Mar 8 2018, 04:49:46
Serial Number	6099AAB7
Uptime	00h:03m:26s
Port A1/A2 Ethernet Address (MAC)	F4:54:33:9B:20:86
Port A1/A2 IP Address	192.168.1.11

Controller Status	
Keyswitch Position	Remote
Controller Mode	Program
Change Detection Audit Value	16#E5BB_9D12_32CB_5788
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

Seconds Between Refresh: 0 Disable Refresh with 0.

Copyright © 2017 Rockwell Automation, Inc. All Rights Reserved.

Dual-IP Mode



General Information	
Device Name	5069-L3100ERMS2/A_RelR31_724
Project Name	SIL2_Test
Device Description	
Device Location	
Product Revision	31.011
Firmware Version Date	Mar 8 2018, 04:49:46
Serial Number	6099AAB7
Uptime	04h:47m:53s
Port A1 Ethernet Address (MAC)	F4:54:33:9B:20:86
Port A1 IP Address	192.168.1.11
Port A2 Ethernet Address (MAC)	F4:54:33:9B:20:87
Port A2 IP Address	192.168.2.12

Controller Status	
Keyswitch Position	Remote
Controller Mode	Program
Change Detection Audit Value	16#AEE7_7600_D871_47C9
I/O Forces	Disabled - None Installed
SFC Forces	Disabled - None Installed

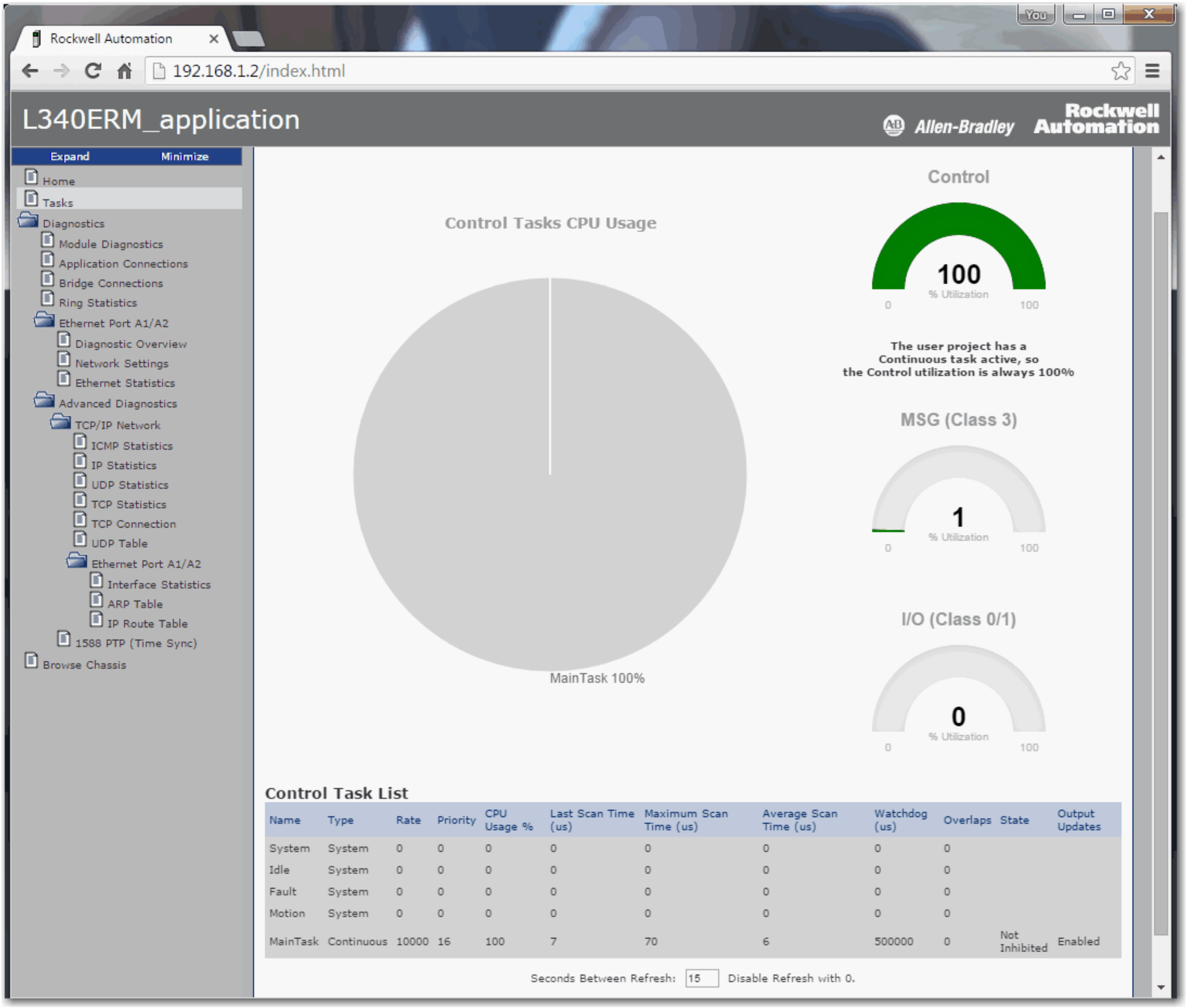
Seconds Between Refresh: 0 Disable Refresh with 0.

Copyright © 2017 Rockwell Automation, Inc. All Rights Reserved.

Tasks Web Page

On the Tasks web page, 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).



The user project has a Continuous task active, so the Control utilization is always 100%

Control Task List

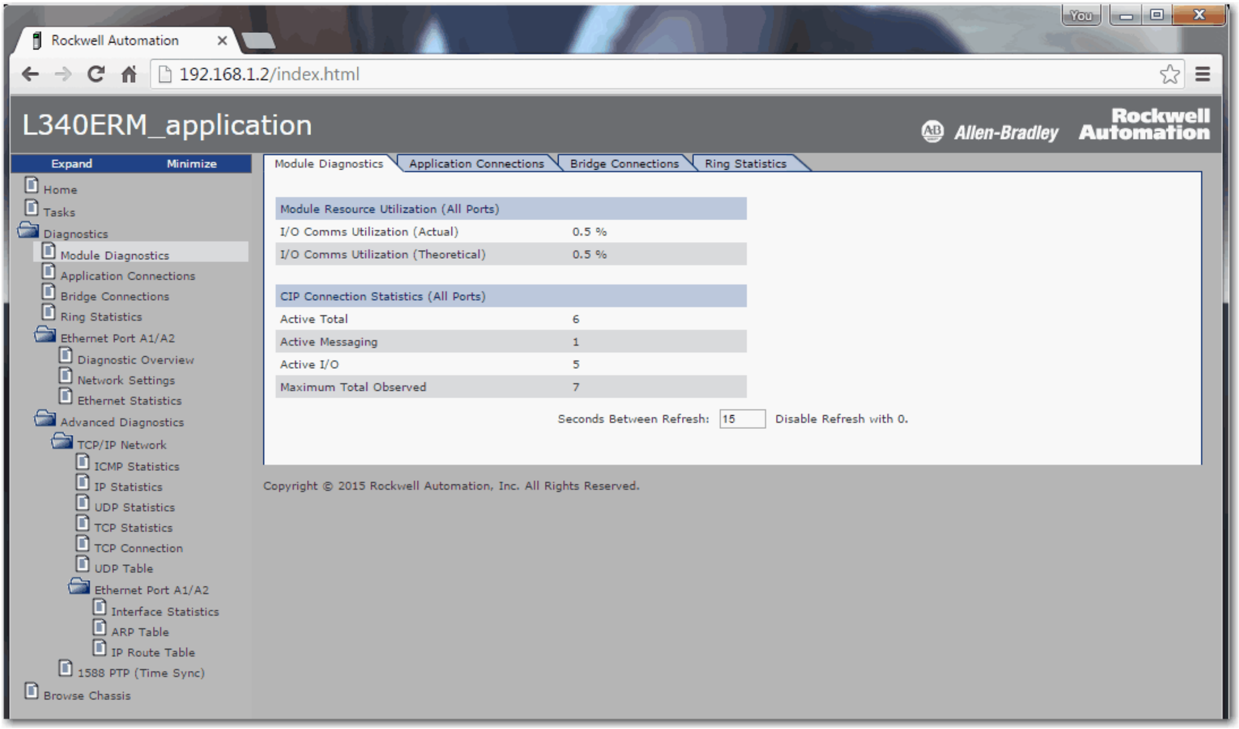
Name	Type	Rate	Priority	CPU Usage %	Last Scan Time (us)	Maximum Scan Time (us)	Average Scan Time (us)	Watchdog (us)	Overlaps	State	Output Updates
System	System	0	0	0	0	0	0	0	0		
Idle	System	0	0	0	0	0	0	0	0		
Fault	System	0	0	0	0	0	0	0	0		
Motion	System	0	0	0	0	0	0	0	0		
MainTask	Continuous	10000	16	100	7	70	6	500000	0	Not Inhibited	Enabled

Seconds Between Refresh: 15 Disable Refresh with 0.

Diagnostics Web Pages

The Diagnostics web pages use a series of tabs to provide information about the following:

- Module Diagnostics
- Application Connections
- Bridge Connections
- Ring Statistics



Module Resource Utilization (All Ports)	
I/O Comms Utilization (Actual)	0.5 %
I/O Comms Utilization (Theoretical)	0.5 %

CIP Connection Statistics (All Ports)	
Active Total	6
Active Messaging	1
Active I/O	5
Maximum Total Observed	7

Seconds Between Refresh: 15 Disable Refresh with 0.

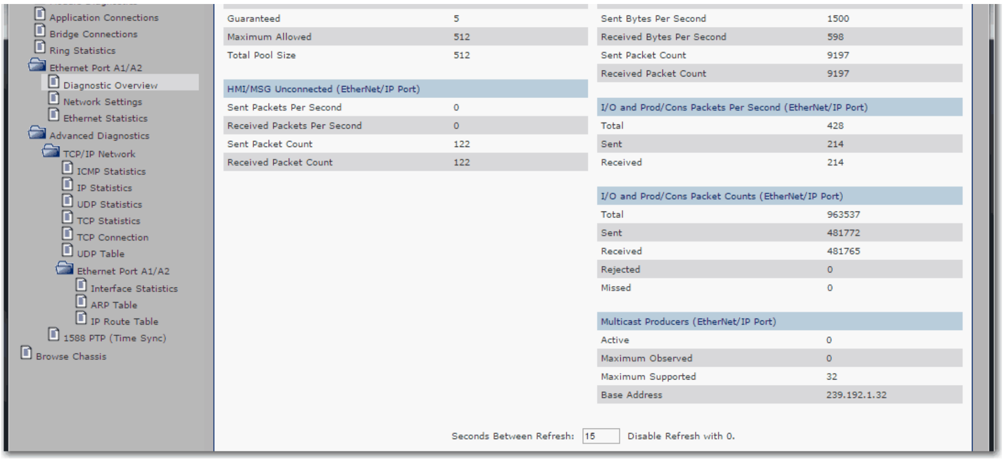
Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

Ethernet Port Web Pages

The Ethernet Port web pages use a series of tabs to provide information about the following:

- Diagnostic Overview
- Network Settings
- Ethernet Statistics

Linear/DLR Mode



Guaranteed	5
Maximum Allowed	512
Total Pool Size	512

HMI/MSG Unconnected (EtherNet/IP Port)	
Sent Packets Per Second	0
Received Packets Per Second	0
Sent Packet Count	122
Received Packet Count	122

Sent Bytes Per Second	1500
Received Bytes Per Second	598
Sent Packet Count	9197
Received Packet Count	9197

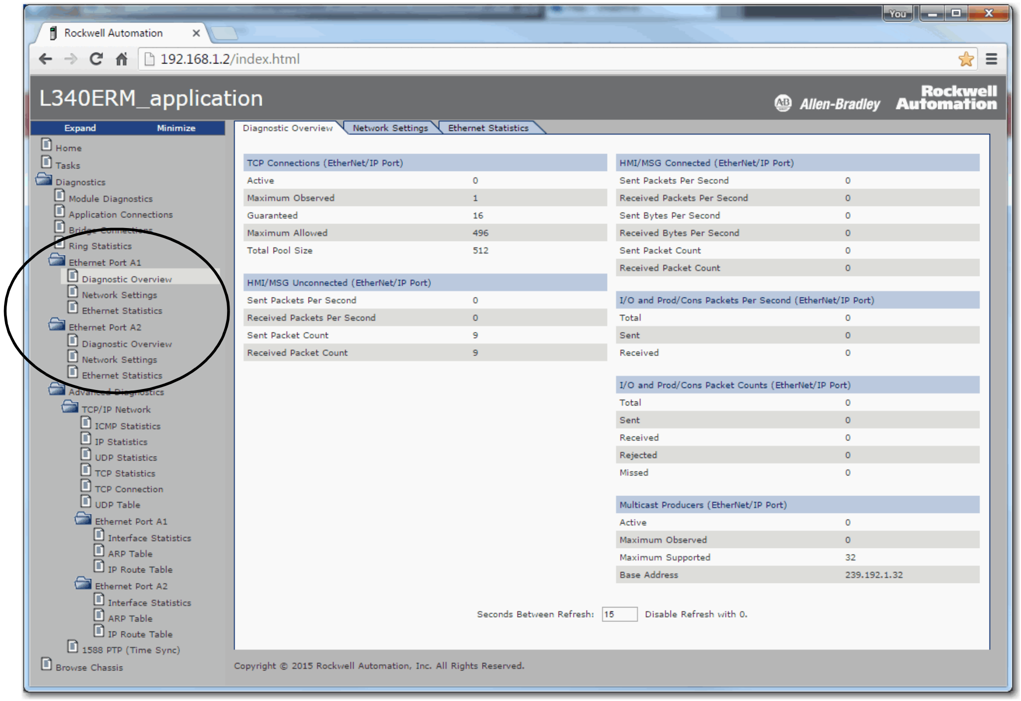
I/O and Prod/Cons Packets Per Second (EtherNet/IP Port)	
Total	428
Sent	214
Received	214

I/O and Prod/Cons Packet Counts (EtherNet/IP Port)	
Total	963537
Sent	481772
Received	481765
Rejected	0
Missed	0

Multicast Producers (EtherNet/IP Port)	
Active	0
Maximum Observed	0
Maximum Supported	32
Base Address	239.192.1.32

Seconds Between Refresh: 15 Disable Refresh with 0.

Dual-IP Mode



TCP Connections (EtherNet/IP Port)	
Active	0
Maximum Observed	1
Guaranteed	16
Maximum Allowed	496
Total Pool Size	512

HMI/MSG Unconnected (EtherNet/IP Port)	
Sent Packets Per Second	0
Received Packets Per Second	0
Sent Packet Count	9
Received Packet Count	9

HMI/MSG Connected (EtherNet/IP Port)	
Sent Packets Per Second	0
Received Packets Per Second	0
Sent Bytes Per Second	0
Received Bytes Per Second	0
Sent Packet Count	0
Received Packet Count	0

I/O and Prod/Cons Packets Per Second (EtherNet/IP Port)	
Total	0
Sent	0
Received	0

I/O and Prod/Cons Packet Counts (EtherNet/IP Port)	
Total	0
Sent	0
Received	0
Rejected	0
Missed	0

Multicast Producers (EtherNet/IP Port)	
Active	0
Maximum Observed	0
Maximum Supported	32
Base Address	239.192.1.32

Seconds Between Refresh: 15 Disable Refresh with 0.

Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

Advanced Diagnostics Web Pages

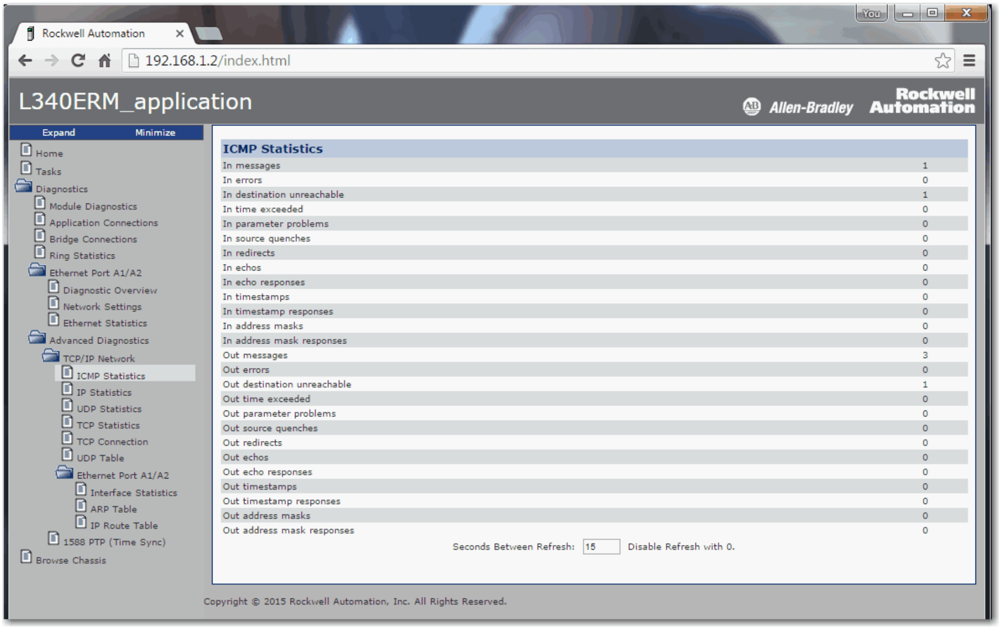
The Advanced Diagnostics web pages provide information about the following:

- TCP/IP Network - Provide information about the following:
    - ICMP Statistics
    - IP Statistics
    - UDP Statistics
    - TCP Statistics
    - TCP Connection
    - UDP Table
- Ethernet Port A1/A2- Provide information about the following:
    - Interface Statistics
    - ARP Table
    - IP Route Table

IMPORTANT	This information is listed separately for, and is unique to, each port when the controller operates in Dual-IP mode.

- 1588 PTP (Time Sync)

Linear/DLR Mode

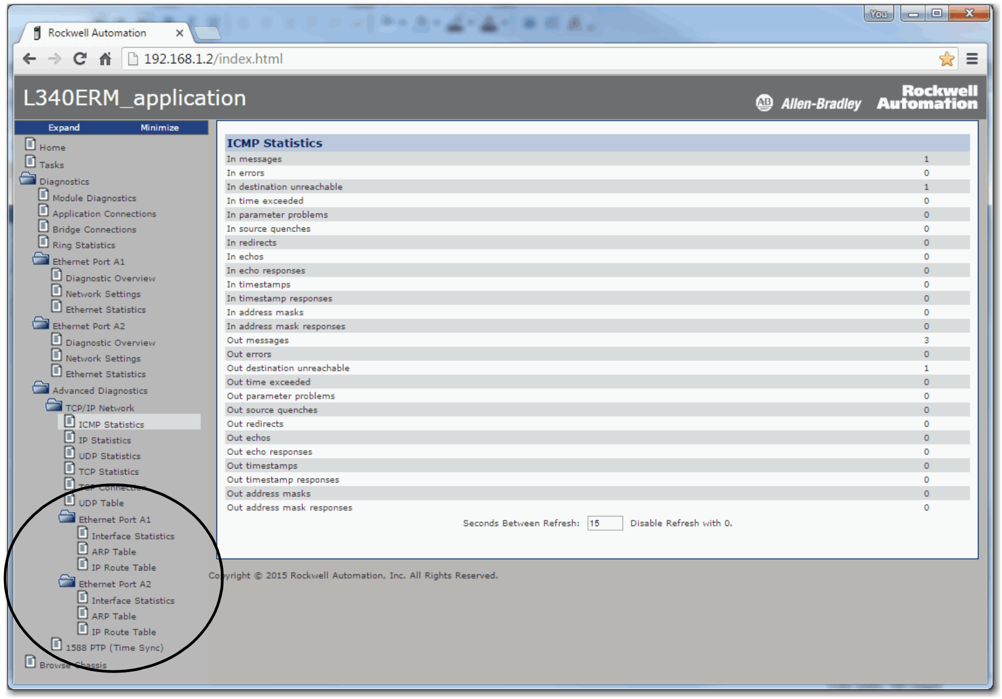


ICMP Statistics	
In messages	1
In errors	0
In destination unreachable	1
In time exceeded	0
In parameter problems	0
In source quenches	0
In redirects	0
In echos	0
In echo responses	0
In timestamps	0
In timestamp responses	0
In address masks	0
In address mask responses	0
Out messages	3
Out errors	0
Out destination unreachable	1
Out time exceeded	0
Out parameter problems	0
Out source quenches	0
Out redirects	0
Out echos	0
Out echo responses	0
Out timestamps	0
Out timestamp responses	0
Out address masks	0
Out address mask responses	0

Seconds Between Refresh: 15 Disable Refresh with 0.

Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

Dual-IP Mode



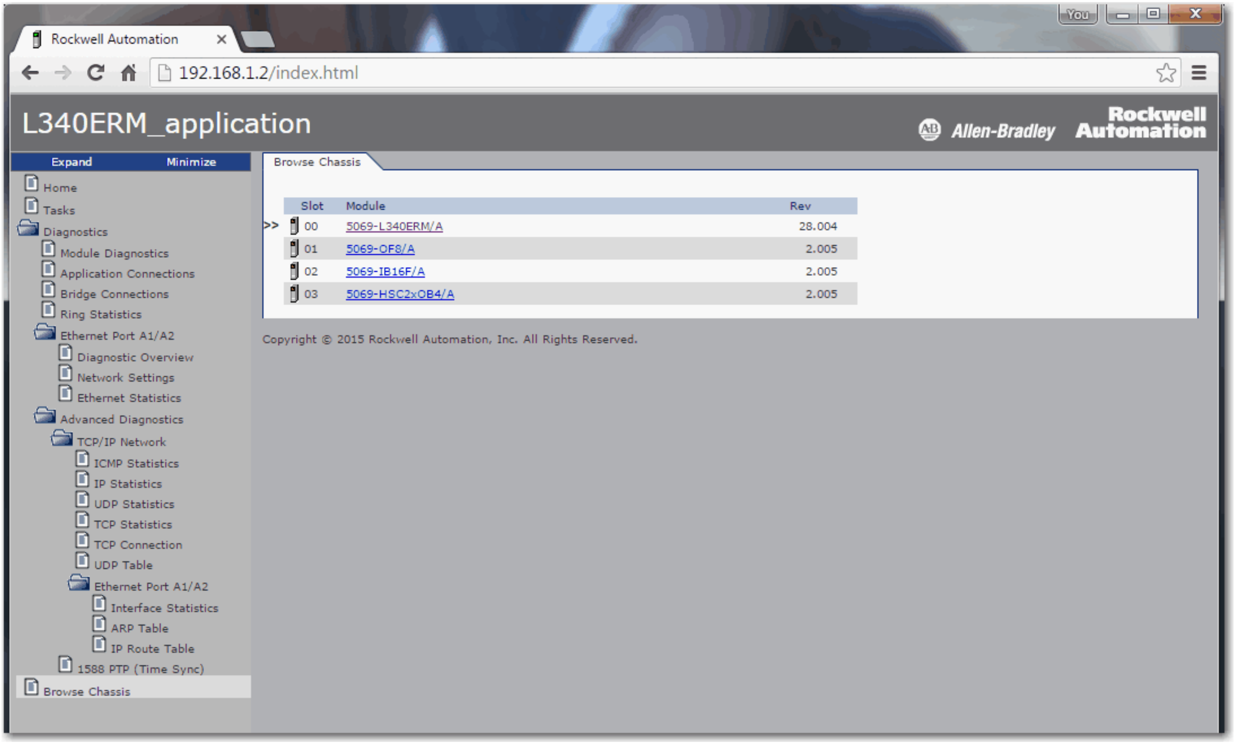
ICMP Statistics	
In messages	1
In errors	0
In destination unreachable	1
In time exceeded	0
In parameter problems	0
In source quenches	0
In redirects	0
In echos	0
In echo responses	0
In timestamps	0
In timestamp responses	0
In address masks	0
In address mask responses	0
Out messages	3
Out errors	0
Out destination unreachable	1
Out time exceeded	0
Out parameter problems	0
Out source quenches	0
Out redirects	0
Out echos	0
Out echo responses	0
Out timestamps	0
Out timestamp responses	0
Out address masks	0
Out address mask responses	0

Seconds Between Refresh: 15 Disable Refresh with 0.

Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

Browse Chassis Web Page

The Browse Chassis provides information about the devices in the system. You can click the link for each catalog number to access more information about that device.



Slot	Module	Rev
>> 00	5069-L340ERM/A	28.004
01	5069-OF8/A	2.005
02	5069-IB16F/A	2.005
03	5069-HSC2xOB4/A	2.005

Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

Other Potential Issues to Troubleshoot

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Your controller can experience other issues that you must troubleshoot.

Continuous Task Sends Output Data at High Rate

A free-running Continuous Task can keep sending outputs at a high rate. If the Continuous Task executes repetitively with a short task execution time, and local output or produced data is changing, the controller can produce data faster than the receiving modules can react. We recommend that you program appropriately to avoid this condition.

Immediate Output Instructions Issued at High Rate

CompactLogix 5380 and Compact GuardLogix 5380 controllers can issue Immediate Output (IOT) instructions faster than I/O modules can react to them. We recommend that you program IOT instructions so that they are sent at a rate appropriate for the I/O module and the corresponding physical devices.

Integrated Motion On an EtherNet/IP Network Traffic Priority Status

When you use a Stratix® managed switch to change the network communication rate from 1 Gbps to 100 Mbps, the system can fail to prioritize the Integrated Motion On an EtherNet/IP network communication higher than standard I/O communication.

For more information on when to use a Stratix managed switch to change the network communication rate from 1 Gbps to 100 Mbps, see page 109.

For more information on managed switches in general, see the EtherNet/IP Network section of the product directory accessible at this address:
http://ab.rockwellautomation.com/networks-and-communications/ethernet-ip-network.

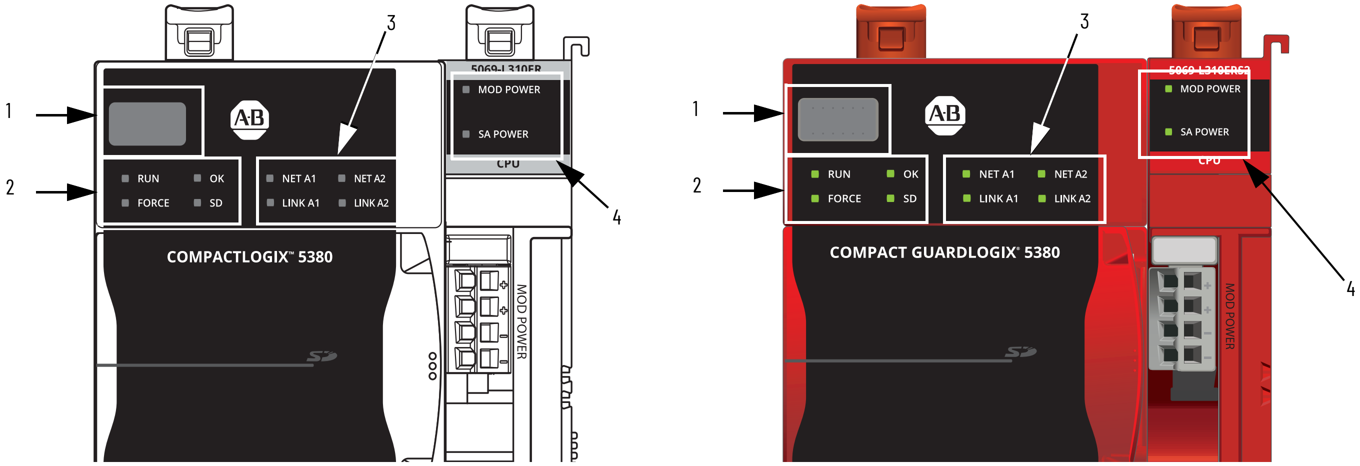
Status Indicators

The CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers have a four-character scrolling status display, controller status indicators, EtherNet/IP™ network status indicators, and power indicators.

Status Display and Indicators

Figure 67 shows the status display and indicators on CompactLogix 5380 and Compact GuardLogix 5380 controllers.

Figure 67 - Status Display and Indicators



Item	Description
1	4-Character Scrolling Status Display, see page 253
2	Controller Status Indicators, see page 257
3	EtherNet/IP™ Status Indicators, see page 258
4	Power Status Indicators, see page 259

General Status Messages

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The scrolling messages that are described in this table are typically indicated upon powerup, powerdown, and while the controller is running to show the status of the controller.

Table 45 - Controller General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Check the MOD POWER status indicator to see if power is applied to the system. Check the OK indicator to determine if the controller is powered and to determine the state of the controller.
Identity Mismatch—Contact Tech Support	Beginning with firmware revision 34.011, if a firmware update identifies the controller as not authentic, the hardware is permanently disabled.
Missing Vendor Certificate—Contact Tech Support	
Bad Vendor Certificate—Contact Tech Support	
TEST	The controller is conducting power-up tests.
CHRG	The embedded energy storage circuit is charging.

Table 45 - Controller General Status Messages (Continued)

Message	Interpretation
PASS	Power-up tests have completed successfully.
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. For more information, see SD Indicator on page 257. Let the save operation complete before you: • Remove the SD card. • Disconnect the power. **IMPORTANT**: Do not remove the SD card while the controller is saving to the SD card. Let the save complete without interruption. If you interrupt the save, data corruption or loss can occur.
One of the following: • LOAD • Loading...Do Not Remove SD Card	A project is being loaded from the SD card. For more information, see SD Indicator on page 257. Let the load operation complete before doing the following: • Remove the SD card • Disconnect the power **IMPORTANT**: Do not remove the SD card while the controller is loading from the SD card. Let the load complete without interruption. If you interrupt the load, data corruption or loss can occur.
UPDT	A firmware update is being conducted from the SD card upon powerup. For more information, see SD Indicator on page 257. If you do not want the firmware to update upon powerup, change the Load Image property of the controller.
Rev *XX.xxx*	The firmware major and minor revision of the controller.
5069-L3xxx	The controller catalog number and series.
Link Down	Message appears when an Ethernet port does not have a network connection. Message scrolls continuously during operation. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for each link, that is, Link A1 and Link A2. The link name appears before the information.
Link Disabled	Message appears when you have disabled an Ethernet port. Message scrolls continuously during operation. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for each link, that is, Link A1 and Link A2. The link name appears before the information.
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. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
Ethernet Port Rate/ Duplex State	The current port rate and duplex state when an Ethernet port has a connection. Message scrolls continuously during operation. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for each link, that is, Link A1 and Link A2. The link name appears before the information.
IP Address	The IP address of the controller. Appears on powerup and scrolls continuously during operation. If the IP address is not yet set, the MAC address appears. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
Duplicate IP - 00:00:XX:XX:XX:XX	Message appears when the controller detects a device with the same IP address on the network. The message shows the MAC address of the device with the duplicate IP address. Message scrolls continuously during operation. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
DHCP-Address Lost	The controller communicated with the DHCP server to renew the IP address. The server either did not reply or did not renew the IP address. The controller continues to operate, but with no Ethernet connectivity out of this port. **IMPORTANT**: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
IP Address/Mask/ Gateway/DNS Invalid	The DHCP server responded with an unusable combination. IMPORTANT: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
IP Address Invalid	The IP Address that is used in the port configuration is not valid. IMPORTANT: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
Mask Invalid	The Subnet/Network Mask used in the port configuration is not valid. IMPORTANT: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.

Table 45 - Controller General Status Messages (Continued)

Message	Interpretation
Gateway Invalid	The Gateway Address that is used in the port IP configuration is not valid. IMPORTANT: When the controller operates in Dual-IP mode, this information is provided for Port A1 and Port A2. The port name appears before the information.
DNS Invalid	The DNS used in the port IP configuration is not valid.
No Project	No project is loaded on the controller. To load a project: • Use the Studio 5000 Logix Designer® application to download the 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. Let powerup and I/O module self-testing complete.
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 to which you are trying to update. 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 to which you are trying to update. 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, save your program to the SD card before you remove power and 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, save your program to the SD card before you remove power and replace the controller.
Flash in Progress	A firmware update that is initiated via ControlFLASH™ or AutoFlash software is in progress. Let the firmware update complete without interruption.
Firmware Installation Required	The controller is using boot firmware, that is, revision 1.*xxx*, and requires a firmware update. The Compact GuardLogix SIL3 controller also shows "Firmware Installation Required", when the controller and the internal safety partner have incompatible firmware. Update the module to correct firmware version.
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 can be due to a user initiated cancel, a download failure, or connection loss.

Compact GuardLogix Status Messages

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The Compact GuardLogix 5380 controller display can show these scrolling messages.

Table 46 - Safety Status Messages

Message	Interpretation
No Safety Signature	Safety Task is in Run mode without a safety signature. Generate a safety signature.
Safety Unlocked	The controller is in Run mode with a safety signature, but is not safety-locked. Safety lock the controller.
Safety Task Inoperable	The safety logic is invalid. For example, a watchdog timeout occurred, or memory is corrupt. For a Compact GuardLogix 5380 SIL3 controllers, a mismatch occurred between the primary controller and the safety partner.
Safety Partner Missing	For Compact GuardLogix 5380 SIL3 controllers, the safety partner is missing or unavailable.

Fault Messages

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

Table 47 - Fault Messages

Message	Interpretation
Major Fault T*XX*:C*XX 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.
I/O Fault Local:*X #XXXX message*	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleName #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module is indicated with the fault code and brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named My_Module is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleParent:X #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The parent name of the module is indicated because no module name is configured in the I/O Configuration tree of Logix Designer application. In addition, the fault code is indicated with a brief description of the fault. Take corrective action specific to the type of fault indicated.
X I/O Faults	I/O faults are present and *X* = the number of I/O faults present. If there are multiple I/O faults, the controller indicates that 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 major recoverable faults and I/O fault codes, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

Major Fault Messages

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The Major Fault T*XX*:C*XX message* on the controller status display indicates major faults.

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

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

I/O Fault Codes

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controller indicates I/O faults on the status display in one of these formats:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent:X #XXXX message*

The first part of the format is used to indicate the location of the module with a fault. How the location is indicated depends on your I/O configuration and the properties of the module that are specified in the Studio 5000 Logix Designer application.

The latter part of the format, #XXXX message, can be used to diagnose the type of I/O fault and potential corrective actions.

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

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

Controller Status Indicators

Table 48 -

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The controller status indicators display the state of the controller.

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 mode switch on the front of the controller or the Controller Status menu in the Logix Designer application.

Table 49 - RUN Indicator

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

FORCE Indicator

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

Table 50 - FORCE Indicator

State	Description
Off	No tags contain I/O force values.
Solid yellow	I/O forces are 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 yellow	I/O forces exist in the application, but are not active because I/O forces are not enabled. **IMPORTANT: Use caution if you enable I/O forces. All existing I/O force values take effect immediately.**

SD Indicator

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

Table 51 - SD Indicator

State	Description
Off	No activity is occurring with the SD card.
Flashing green	The controller is reading from or writing to the SD card. **IMPORTANT**: Do not remove the SD card while the controller is reading or writing. Let the read/write complete without interruption. If you interrupt the read/write, data corruption or loss can occur.
Solid green	
Flashing red	One of the following exists: • The SD card does not have a valid file system. • The SD card drew excessive current and power has been removed from the card.
Solid red	The controller does not recognize the SD card.

OK Indicator

The OK indicator shows the state of the controller.

Table 52 - OK Indicator

State	Description
Off	No power is applied.
Flashing red	One of the following exists: • The controller requires a firmware update. Typically, the controller is in its out-of-box state when a firmware update is required. If a firmware update is required, the 4-character display indicates Firmware Installation Required. For more information on how to update firmware, see Upload from the Controller on page 80. • A firmware update is in progress. If a firmware update is in progress, the 4-character display indicates Flash in Progress. For more information on how to update firmware, see Upload from the Controller on page 80. • The controller has a major fault. The fault can be recoverable or nonrecoverable. If the fault is nonrecoverable, the program has been cleared from the controller memory. If a fault has occurred, the 4-character display shows information about the fault, for example, the Type and Code. For details about major faults, see the following: – The fault descriptions in the General Status Messages that begin on page 253. – Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014. • All user tasks, that is, standard and safety, are stopped.
Solid red	• One of the following: • The controller is completing power-up diagnostics. • The controller is depleting its residual stored energy 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, full power is applied.
Solid green	The controller is operating normally.

EtherNet/IP Status Indicators

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The EtherNet/IP indicators show the state of the controller Ethernet ports and network communication activity.

NET A1 and NET A2 Indicators

The NET A1 and NET A2 indicators show the state of the Ethernet port.

Table 53 - NET A1 and NET A2 Indicators

State	Description
Off	One of the following: • The controller is not configured, or does not have an IP address. • The port is administratively disabled. • The EtherNet/IP mode is Linear/DLR mode. In this case, the NET A2 indicator is off. The NET A1 indicator remains on.
Flashing green	The controller has an IP address, but no active connections are established.
Steady green	The controller has an IP address and at least one established active connection.
Steady red	Duplicate IP address or invalid configuration.

LINK A1 and LINK A2 Indicators

The LINK A1 and LINK A2 indicators show the state of the EtherNet/IP links.

Table 54 - LINK A1 and LINK A2 Indicators

State	Description
Off	The link is down. One or more of these conditions exists: • Ethernet cables are not properly connected at both ends. That is, the cables are not properly connected the controller Ethernet port and to the connected device. • No link exists on the port. For example, the connected device is not powered. • The port is administratively disabled. • LINK A2 only - The controller is the active ring supervisor in a DLR network and has detected a rapid ring fault.
Flashing green	All of these conditions exist: • The port is enabled. • A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device. • There is **activity** on the port.
Steady green	All of these conditions exist: • The port is enabled. • A link exists. That is, the cable is properly connected to an enabled controller Ethernet port on to another device. • LINK A2 only - The controller is the active ring supervisor in a DLR network, and the ring is not broken. This is normal operation. • There is **no activity** on the port.

Power Status Indicators

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

The power status indicators show the status of module power and sensor/actuator power, known as MOD Power and SA Power, respectively.

MOD Power Indicator

Table 55 describes the MOD Power indicator on a CompactLogix 5380 and Compact GuardLogix 5380 controller.

Table 55 - MOD Power Indicator

State	Description
Off	Module Power is not present
Steady green	Module Power is present[1]

[1] Although unlikely, it is possible that there is enough Module Power present for the indicator to turn steady green but the power is not valid. Valid power is 18…32V DC to operate a CompactLogix 5380 system. If the system does not power up and operate successfully, Module Power can be invalid.
If Module Power is invalid, we recommend that you make sure that the external power supply is working correctly, properly sized for your application and that all wiring is correct.

SA Power Indicator

Table 56 describes the SA Power indicator on a CompactLogix 5380 and Compact GuardLogix 5380 controller.

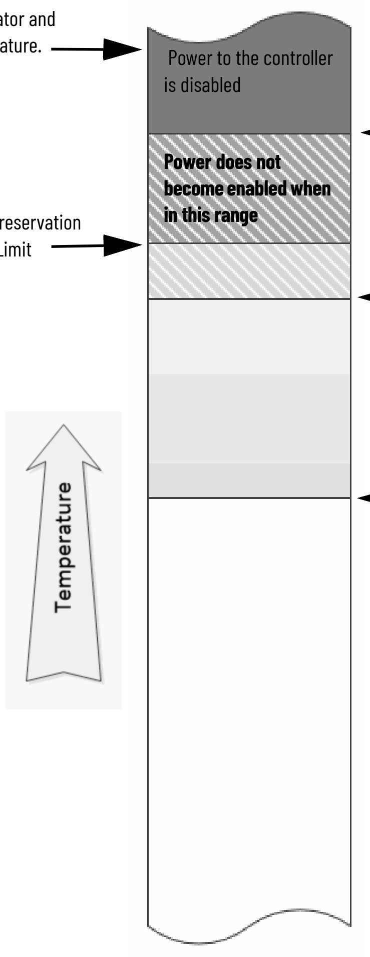
Table 56 - SA Power Indicator

State	Description
Off	One of the following: • Sensor Actuator Power is not present • Status of Sensor Actuator power is unknown
Steady green	Sensor Actuator Power is present[1]

[1] Although unlikely, it is possible that there is enough Sensor/Actuator Power present for the indicator to turn steady green but the power is not valid. Valid power is 18…32V DC in applications that require DC voltage and 18…240V AC in applications that require AC voltage.
If Sensor/Actuator Power is invalid, we recommend that you make sure that the external power supply is working correctly, properly sized for your application and that all wiring is correct.

Thermal Monitoring and Thermal Fault Behavior

The controllers monitor internal module temperatures. As shown below, the controller takes actions as the temperature increases.


Power to the controller is disabled
Power does not become enabled when in this range
Temperature

All power to the controller is disabled except to run the red OK status indicator and monitor the temperature.

Hardware Preservation Hysteresis Limit

Threshold for controller to declare a `Hardware Preservation Fault', resetting the module and disabling power.
In the disabled power condition, only the OK status indicator is illuminated, and it is red. The module does not apply power until it has cooled below the Hardware Preservation Hysteresis limit. The module then enters fault mode, records the fault in the major fault log, and displays `CPU Temperature Fault' on the front panel.

Threshold for controller to declare a `CPU Temperature Fault' major recoverable fault.
If a fault handler does not clear the fault, then the module enters fault mode, records the fault in the major fault log, and displays `T17:C34 CPU Temperature Fault' on the front panel.

Threshold for controller to declare a `T17:C35 Controller internal temperature is approaching operating limit' minor fault and set the Diagnostics minor fault bit.
The fault is recorded in the minor fault log, but is not displayed on the front panel. If the temperature returns to an acceptable range, the Diagnostics minor fault bit clears, but the minor fault record remains.

Applies to these controllers:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

IMPORTANT If you follow the recommended limits for ambient (inlet) temperature and apply the required clearances around the system, the controller is unlikely to reach the initial warning (minor fault) temperature.

For more information on CompactLogix 5380 and Compact GuardLogix 5380 controller specifications, see CompactLogix 5380 and Compact GuardLogix 5380 Controller Specifications Technical Data, publication 5069-TD002.

IMPORTANT The presence of any temperature warning indicates that measures must be taken to reduce the ambient temperature of the module.

Instructions for how to use Ladder Diagram 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.

You can use a GSV instruction to read the MinorFaultBits attribute of the FaultLog class name. If the Diagnostics minor fault bit (Bit 17) is set, a temperature minor fault can be present. Check the Minor Faults tab of the Controller Properties dialog box in Logix Designer to see if the minor fault is a temperature warning.

Change Controller Type

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
- 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:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

You can change from a CompactLogix™ 5380 controller to a Compact GuardLogix® 5380 controller in safety applications.

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

- The safety task is created only if the maximum number of downloadable tasks has not been reached. The safety task is initialized with its default values.

  If your project already contains 32 tasks, and you try to 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).
- A time-based safety network number (SNN) is generated for the local chassis.
- A time-based safety network number (SNN) is also generated for each 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:
CompactLogix 5380
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

Upon confirmation of a change from a safety controller project to a standard controller, some components are changed and others are deleted:

- 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 (SNNs) are deleted.
- Safety-lock and -unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, those new features are visible in the Controller Properties dialog box.

  Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

If the safety controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

Change Safety Controller Types

Applies to these controllers:
Compact GuardLogix 5380 SIL 2
Compact GuardLogix 5380 SIL 3

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

If you change from a safety controller with a SIL 3/PLe application to a Compact GuardLogix 5380 SIL 2 controller, the application changes to SIL 2/PLd.

If you change from a safety controller with a SIL 3/PLe application to a Compact GuardLogix 5380 SIL 3 controller, the application remains SIL 3/PLe.

If you change from a safety controller with a SIL 2/PLe application to a Compact GuardLogix 5380 SIL 3 controller, the representation of the safety partner is updated to appear appropriately for the target controller.

Safety Network Numbers are also preserved when you change to a Compact GuardLogix 5380 controller.

History of Changes

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

5069-UM001J-EN-P, November 2022

Change
Moved information about connection reaction time limit to publication 1756-RM012
Added Real-time Clock section to Chapter 1: CompactLogix 5380 and Compact GuardLogix 5380 Systems and Controllers
Revised information about the safety signature
Added information about secure socket objects
Added Monitor Safety I/O Device Status section in Chapter 12: Safety I/O Devices
Added introduction and Program Safety Applications section to Chapter 14: Develop Safety Applications and moved other safety topics from Chapter 14 to publication 1756-RM012

5069-UM001I-EN-P, March 2022

Change
Updated Appearance Change section
Added CIP Security™ to controller features table
Added new section about CIP Security
Updated general status messages for the controller

5069-UM001H-EN-P, October 2021

Change
Updated graphics throughout
Added MOD Power note
Updated the Use ControlFLASH Plus Software to Update Firmware section
Updated general status messages
Updated major fault messages
Updated I/O fault codes

5069-UM001G-EN-P, August 2020

Change
Added CompactLogix™ 5380 Process controllers
Updated safety signature definition
Added Simple Network Management Protocol (SNMP)
Added Automatic Diagnostics
Added Considerations for Communication Loss Diagnostics
Updated the Disable Controller Web Pages procedure

5069-UM001F-EN-P, May 2020

Change
Added Compact GuardLogix® 5380 SIL 3 controller information
Added links to access Controller and I/O fault code information from the Knowledgebase Support Center
Added Firmware Upgrade Guidelines for Safety Controllers

5069-UM001E-EN-P, January 2020

Change
Updated the description of Ethernet ports A1 and A2
Updated the Connect an Ethernet Cable section
Added the 1784-SDHC8 and 1784-SDHC32 SD cards

5069-UM001D-EN-P, April 2018

Change
Added Compact GuardLogix® 5380 and Safety information throughout
Chapter 3, How to Power Compact GuardLogix 5380 Controllers
Chapter 4, Safety Concept of Compact GuardLogix 5380 Controllers
Chapter 12, Safety I/O Devices
Chapter 14, Develop Safety Applications

5069-UM001C-EN-P, December 2016

Change
Added CompactLogix 5380 controllers 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM

Notes:

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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

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

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, 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
UNITED KINGDOM: Rockwell Automation Ltd. Pitfield, Kiln Farm Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication 5069-UM001K-EN-P - November 2023
Supersedes Publication 5069-UM001J-EN-P - November 2022