User Manual

Original Instructions

Allen-Bradley

CompactLogix 5380 and Compact GuardLogix 5380 Controllers

Catalog Numbers 5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ERM, 5069-L310ER-NSE, 5069-L310ERS2, 5069-L320ER, 5069-L320ERM, 5069-L330ER, 5069-L330ERM, 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM, 5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERMS2, 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

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

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

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

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

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

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

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

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

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

	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

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

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

Chapter 4

Safety Concept of Compact GuardLogix 5380 Controllers

Chapter 5

Connect to the Controller

Chapter 6

Start to Use the Controller

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 Motion Applications

Chapter 16

Troubleshoot the Controller

Appendix A

Status Indicators

Appendix B

Security Options

Appendix C

Change Controller Type

Summary of Changes

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

Topic	Page
Added Compact GuardLogix® 5380 and Safety information	Throughout
Chapter 3, How to Power Compact GuardLogix 5380 Controllers	37
Chapter 4, Safety Concept of Compact GuardLogix 5380 Controllers	49
Chapter 12, Safety I/O Devices	199
Chapter 14, Develop Safety Applications	241

Overview

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.

Additional Resources

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

Table 1 - Additional Resources

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 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 Communication Modules in Logix 5000™ Control Systems User Manual, publication ENET-UM004	Provides information on how to use Compact 5000 I/O EtherNet/IP adapters.
	Guidance for Selecting Cables for EtherNet/IP Networks, publication ENET-WP007-EN-P	Provides information on how to select cabling based on the application, environmental conditions, and mechanical requirements.
CIP Sync (time synchronization)	Integrated Architecture and CIP Sync Configuration Application Technique, publication IA-AT003	Describes how to configure CIP Sync with Integrated Architecture® products and applications.
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 requirements with the GuardLogix 5570 controller system using the Studio 5000 Logix Designer® application.
Motion	Motion Coordinate System User Manual, publication MOTION-UM002	Provides information on how to create and configure a coordinated motion application system.
	Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003	Provides information on how to configure an Integrated Motion on EtherNet/IP networks application system.
	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.
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
	CompactLogix System Selection Guide, publication 1769-SG001	Provides information on how to design and select components for your CompactLogix or Compact GuardLogix system.
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.

Table 1 - Additional Resources

Resource		Description
Compact 5000 Digital and Safety modules	Compact 5000 Digital and Safety I/O Modules User Manual, publication 5000-UM004	Provides information on how to use Compact 5000 I/O digital and safety modules.
	5000 Series Analog I/O Module User Manual, publication 5000-UM005	Provides information on how to use Compact 5000 I/O analog modules.
	5000 Series High-speed Counter Module User Manual, publication 5000-UM006	Provides information on how to use the Compact 5000 I/O high-speed counter module.
Guard I/O Modules	Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Provides information on how to use Guard I/O™ DeviceNet Safety modules, including 1732DS and 1791DS I/O modules.
	Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001	Provides information on how to use Guard I/O EtherNet/IP Safety modules, including 1732ES and 1791ES I/O modules.
	POINT Guard I/O™ Safety Modules User Manual, publication 1734-UM013	Provides information on how to use POINT Guard I/O™ modules.
Drives	Kinetix 5500 Servo Drives User Manual, publication 2198-UM001	Provides information on how to use a Kinetix 5500 servo drive system. Also includes requirements for how to use Kinetix 5500 drives in safety applications.
	Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Provides information on how to use a Kinetix® 5700 servo drive system. Also includes requirements for how to use Kinetix 5700 drives in safety applications.
	PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002	Provides information on how to use a PowerFlex® 520-series adjustable frequency AC drive.
Product Certifications	Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

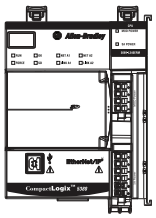
Notes:

CompactLogix 5380 and Compact GuardLogix 5380 Systems and Controllers

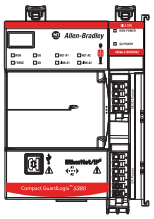
This chapter describes features and functions that are associated with the CompactLogix® 5380 and Compact GuardLogix® 5380 controllers.

Minimum Requirements

CompactLogix



Compact GuardLogix



The controllers have minimum requirements.

- CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers have minimum hardware requirements. For more information on the hardware requirements, see Table 2 on page 20.
- The controller firmware revision must be compatible with the software version that you use. For more information, see page 16.
- Programming software

System	Cat. No.	Studio 5000 Logix Designer® Application[1]
CompactLogix	5069-L320ER, 5069-L340ERM	Version 28.00.00 or later
CompactLogix	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM, 5069-L320ERM, 5069-L330ER, 5069-L330ERM, 5069-L340ER	Version 29.00.00 or later
CompactLogix	5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	Version 30.00.00 or later
Compact GuardLogix	5069-L306ERS2, 5069-L306ERMS2, 5069-L310ERS2, 5069-L310ERMS2, 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 31.00.00 or later

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

IMPORTANT If safety connections or safety logic are 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 prevent personal injury resulting from accessibility to live parts.

The enclosure must have suitable flame-retardant properties to 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 regarding specific enclosure type ratings that are required to comply with certain product safety certifications, see the Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014.

Waste Electrical and Electronic Equipment (WEEE)

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

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 Rockwell Automation® Product Compatibility and Download Center (PCDC) available at: http://compatibility.rockwellautomation.com/Pages/home.aspx

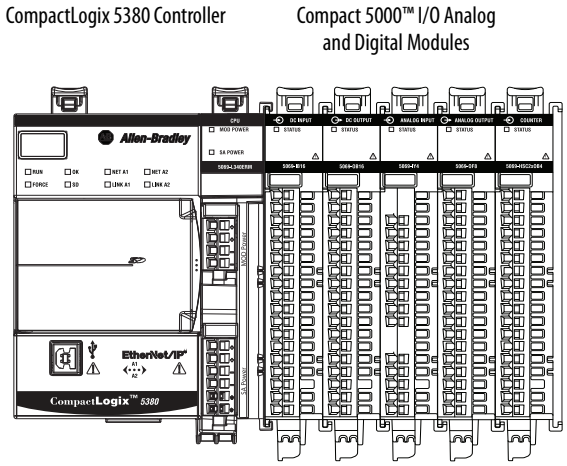
In the PCDC:

- 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.

CompactLogix 5380 System

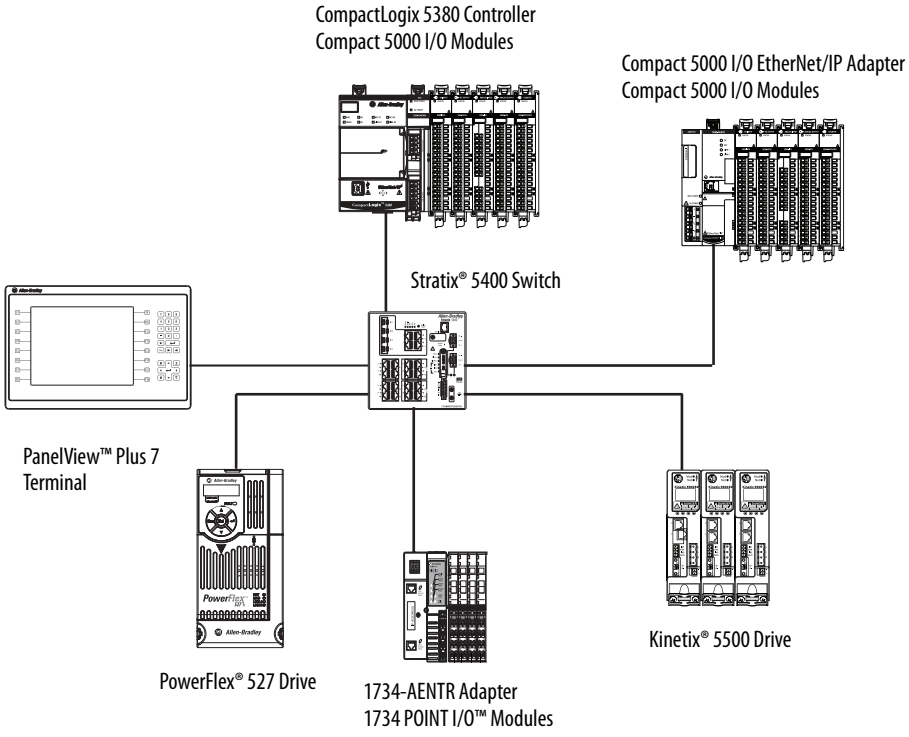
CompactLogix 5380 control systems are DIN rail-mounted systems that can operate in various applications, including standalone systems that contain local standard I/O modules, as shown in Figure 1.

Figure 1 - CompactLogix 5380 Controller in a Standalone System



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



Compact GuardLogix 5380 System

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:

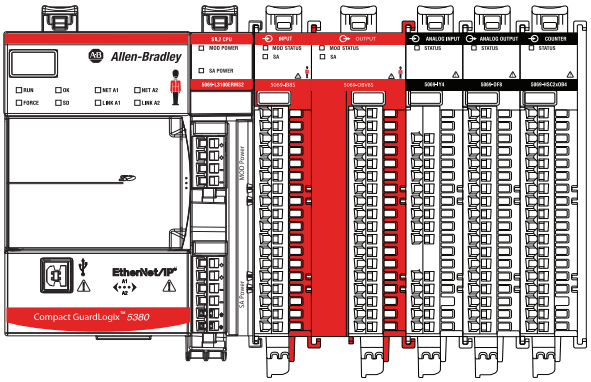
- Ladder Diagram (LD)
- Structured Text (ST)
- Function Block Diagram (FBD)
- Sequential Function Chart (SFC)

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

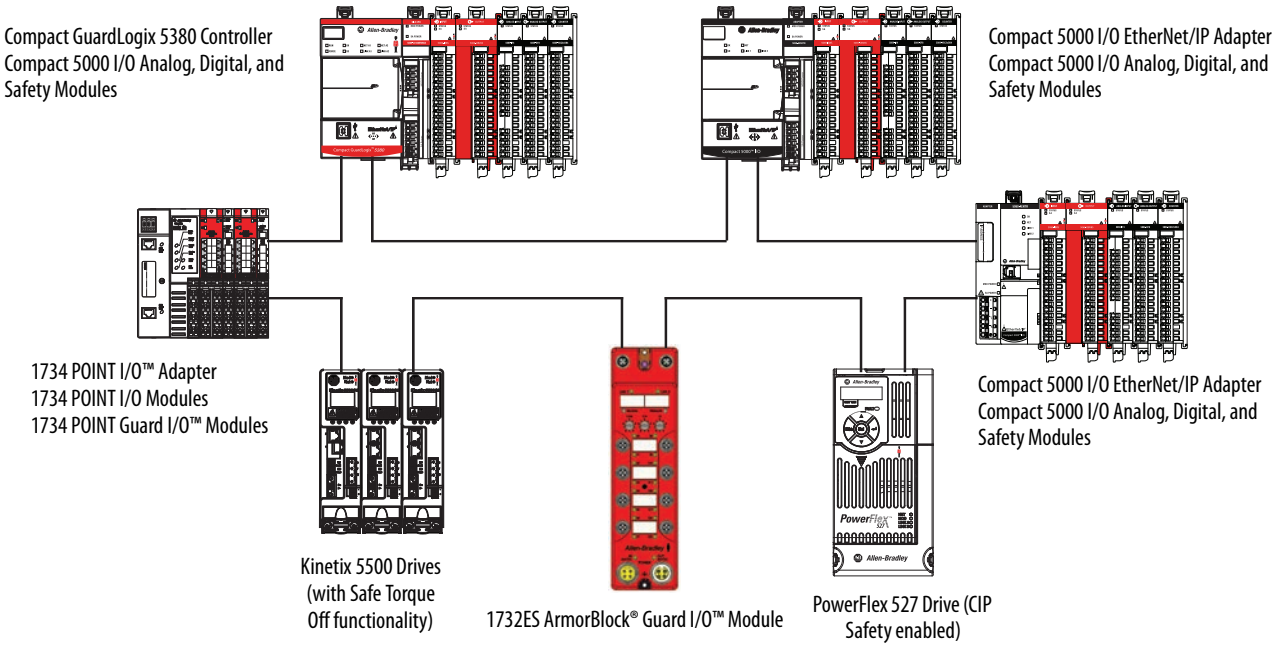
Compact GuardLogix 5380 Controller

Compact 5000 I/O standard analog, standard digital, and safety digital modules



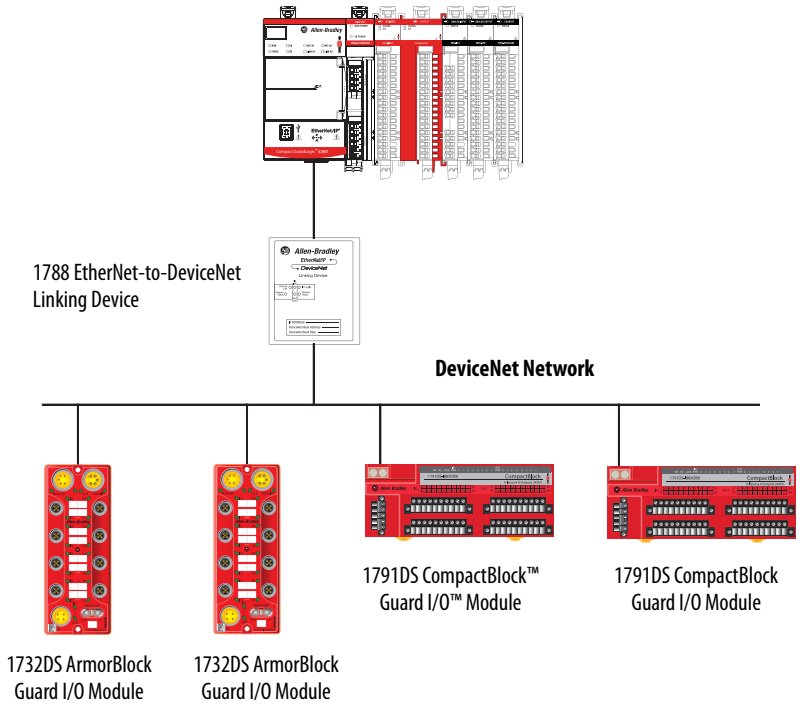
The controllers can also operate in more complex systems with devices that are connected to the controller via an EtherNet/IP network, as shown in Figure 4.

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



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

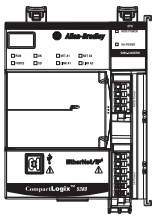
Figure 5 - Compact GuardLogix 5380 Controller Connected to Devices on a DeviceNet Network



Design the System

When you design a system, you must decide what system components your application needs. Table 2 describes components that are commonly used in CompactLogix 5380 and Compact GuardLogix 5380 control systems.

CompactLogix



Compact GuardLogix

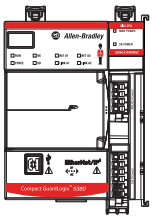


Table 2 - System Components

Component	Purpose	Required	For More Information
DIN rail	Mounting system	Yes	• CompactLogix 5380 Controllers Installation Instructions, publication 5069-IN013 • Compact GuardLogix 5380 Controllers Installation Instructions, publication 5069-IN014
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	
External power supply(1)	Provides Module (MOD) Power to the system	Yes	Power the System on page 25
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 15 • Create a Logix Designer Application Project on page 85
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 55
ControlFLASH™ software	Update controller firmware	Yes	• For compatible ControlFLASH™ software, see the Product Compatibility and Download Center (PCDC). • Update Controller Firmware on page 75
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 64
Ethernet port A1	Connect to device-level networks	—	Chapter 9, Use EtherNet/IP Modes on page 141
Ethernet port A2	Connects to these network types: • Enterprise-level network • Device-level network	—	

Table 2 - System Components

Component	Purpose	Required	For More Information
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 117
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 63
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 64
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 199
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 177 • Safety I/O Devices on page 199
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 177 • Safety I/O Devices on page 199 • Develop Motion Applications on page 277

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

Controller Features

Table 3 lists features available on the controllers. The features are described in detail in the rest of this manual.

Table 3 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Features

Feature	CompactLogix 5380 Controllers	Compact GuardLogix 5380 Controllers	Value
User memory	5069-L306ER, 5069-L306ERM	5069-L306ERS2, 5069-L306ERMS2	0.6 MB
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L310ERS, 5069-L310ERMS2	1 MB
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	2 MB
	5069-L330ER, 5069-L330ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	3 MB
	5069-L340ER, 5069-L340ERM	5069-L340ERS2, 5069-L340ERMS2	4 MB
	5069-L350ERM	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	5 MB
	5069-L380ERM	5069-L380ERS2, 5069-L380ERMS2	8 MB
	5069-L3100ERM	5069-L3100ERS2, 5069-L3100ERMS2	10 MB
Safety memory	—	5069-L306ERS2, 5069-L306ERMS2	0.3 MB
	—	5069-L310ERS2, 5069-L310ERMS2	0.5 MB
	—	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	1 MB
	—	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	1.5 MB
	—	5069-L340ERS2, 5069-L340ERMS2	2 MB
	—	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	2.5 MB
	—	5069-L380ERS2, 5069-L380ERMS2	4 MB
	—	5069-L3100ERS2, 5069-L3100ERMS2	5 MB
Controller tasks	• 32 tasks **IMPORTANT**: The Compact GuardLogix 5380 controllers support a Safety Task. The Safety Task is included in the 32 total tasks available with the Compact GuardLogix 5380 controllers. As a result, the Compact GuardLogix 5380 controllers support 31 standard tasks. • 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		
EtherNet/IP network topologies supported	• Device Level Ring (DLR) • Star • Linear		
EtherNet/IP nodes supported, max(1)	5069-L306ER, 5069-L306ERM	5069-L306ERS2, 5069-L306ERMS2	16
	5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L310ERS2, 5069-L310ERMS2	24
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	40
	5069-L330ER, 5069-L330ERM	5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	60
	5069-L340ER, 5069-L340ERM	5069-L340ERS2, 5069-L340ERMS2	90
	5069-L350ERM	5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	120
	5069-L380ERM	5069-L380ERS2, 5069-L380ERMS2	150
	5069-L3100ERM	5069-L3100ERS2, 5069-L3100ERMS2	180

Table 3 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Features (continued)

Feature	CompactLogix 5380 Controllers	Compact GuardLogix 5380 Controllers	Value
EtherNet/IP modes	• Linear/DLR mode • Dual-IP mode - Available with the Logix Designer application, version 29.00.00 or later.		
Integrated motion axes supported **IMPORTANT**: Not all CompactLogix 5380 or Compact GuardLogix 5380 controllers support Integrated Motion on an EtherNet/IP network. Only controllers with an 'M' in the catalog number support motion.	5069-L306ERM	5069-L306ERMS2	2
	5069-L310ERM	5069-L310ERMS2	4
	5069-L320ERM	5069-L320ERMS2, 5069-L320ERMS2K	8
	5069-L330ERM	5069-L330ERMS2, 5069-L330ERMS2K	16
	5069-L340ERM	5069-L340ERMS2	20
	5069-L350ERM	5069-L350ERMS2, 5069-L350ERMS2K	24
	5069-L380ERM	5069-L380ERMS2	28
	5069-L3100ERM	5069-L3100ERMS2	32
Local I/O modules, max	5069-L306ER, 5069-L306ERM, 5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERS2, 5069-L310ERMS2	8
	5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	16
	5069-L330ER(2), 5069-L330ERM(2), 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	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	31
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 131.

(2) When you use this controller with the 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 Rockwell Automation® Knowledgebase article #942580, '5380 CompactLogix controllers limited to 16 local Compact 5000 I/O modules in V29 of Studio 5000.' The document is available at http://www.rockwellautomation.com/knowledgebase.
With the Logix Designer application, version 30.00.00 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 SIL 2/PLd safety applications via the Safety task in the Logix Designer application.

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

Feature	Studio 5000 Logix Designer Application, Version 31 or Later	
	Safety Task	Standard Task
Add-On Instructions	X	X
Instruction-based alarms and events	—	X
Tag-based alarms	—	X
Controller logging	X	X
Event tasks(1)	—	X
Function Block Diagrams (FBD)	—	X
Integrated motion	X(2)	X
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) While the safety task cannot be an Event task, standard Event tasks can be triggered with the use of the Event instruction in the safety task.

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

IMPORTANT **Safety Consideration**

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.

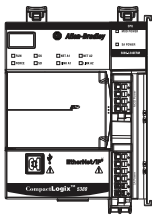
When you configure a produced safety tag, you are only allowed to configure unicast connection options. Logix Designer does not allow you to configure multicast connection options.

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

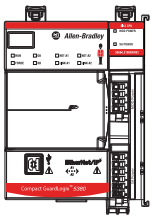
- If the producer in the I/O tree of this controller is a GuardLogix 5580 or Compact GuardLogix 5380 controller, and you are consuming a safety tag, you must configure the consumed tag to use unicast.
- If the producer in the I/O tree of this controller is a GuardLogix 5570 or GuardLogix 5560 controller, 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 19.00.00 or later for unicast produce/consume safety tags.

Power the System

CompactLogix



Compact GuardLogix



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 27
- How to Power Compact GuardLogix 5380 Controllers - Chapter 3 on page 37

Notes:

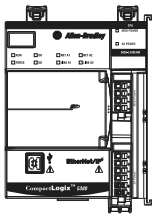
How to Power CompactLogix 5380 Controllers

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 37.

Two Types of Power

CompactLogix



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.

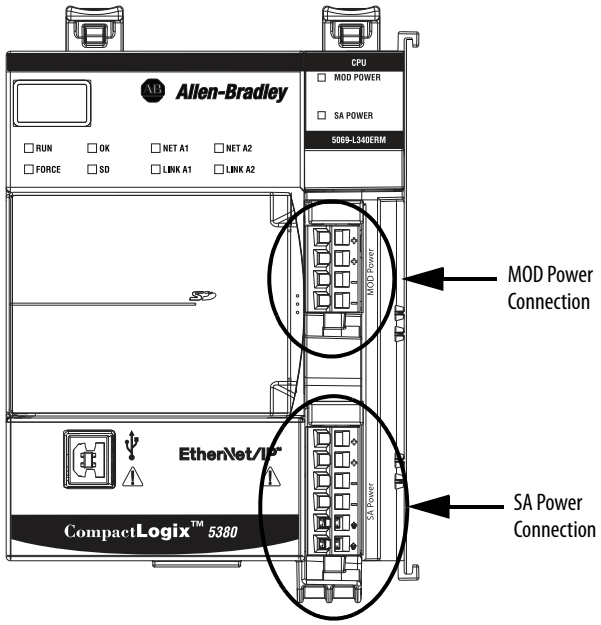
  System-side power is provided through the MOD Power RTB.

- 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.

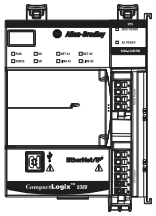
IMPORTANT We **recommend** that you use separate external power supplies for MOD power and SA power, respectively. This practice can help prevent unintended consequences that can result if you use one supply.

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

CompactLogix



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

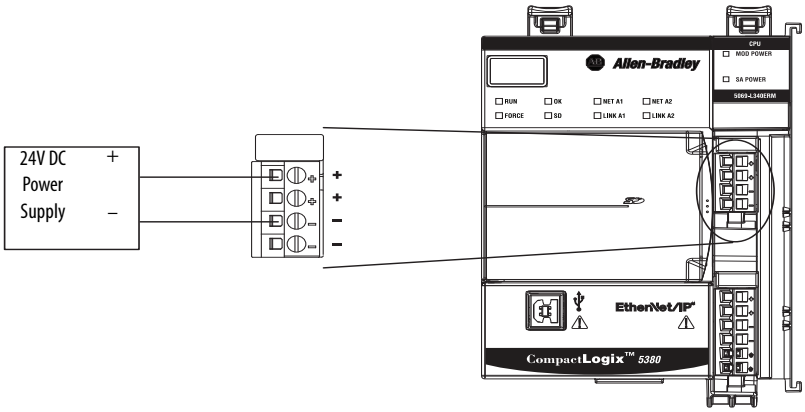
IMPORTANT You can only use DC power on the MOD power bus. Do not connect AC power to the MOD power bus.

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

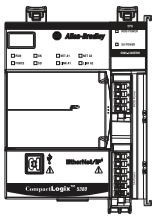
When the MOD power source is turned on, the following occurs.

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

CompactLogix



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.

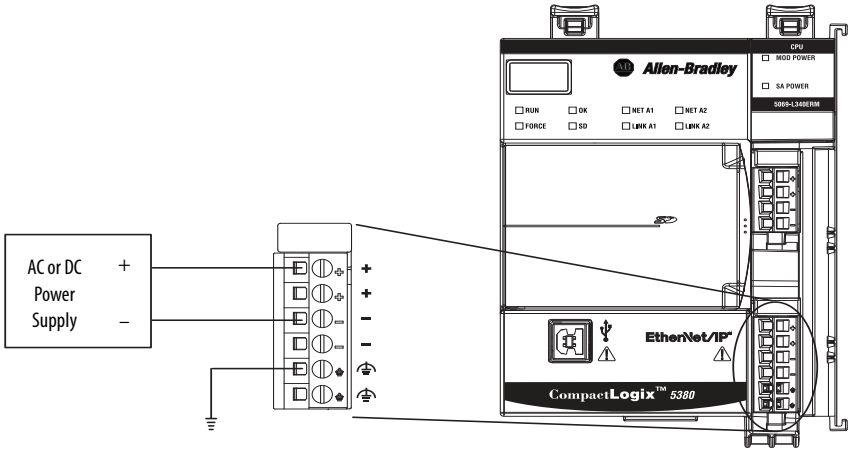
  For more information on how to use a 5069-FPD field potential distributor in a CompactLogix 5380 system, see page 34.
- If the SA power source uses DC voltage, the total continuous current draw across the SA power bus must not be more than to 10 A, max at 18...32V DC.
- We recommend that you use an external 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. That is, 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.

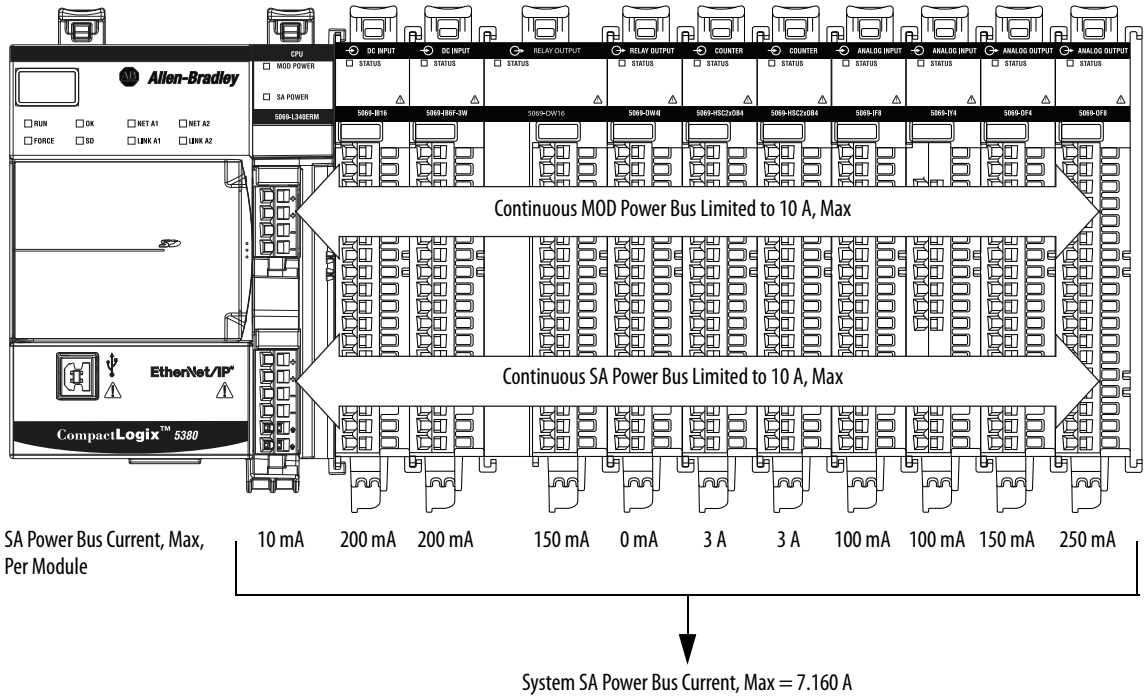
  Other modules that do not use SA power bus current, but are not shown in the graphic, include the 5069-OB16, 5069-OB16F, 5069-OX4I, and 5069-SERIAL modules.

- 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

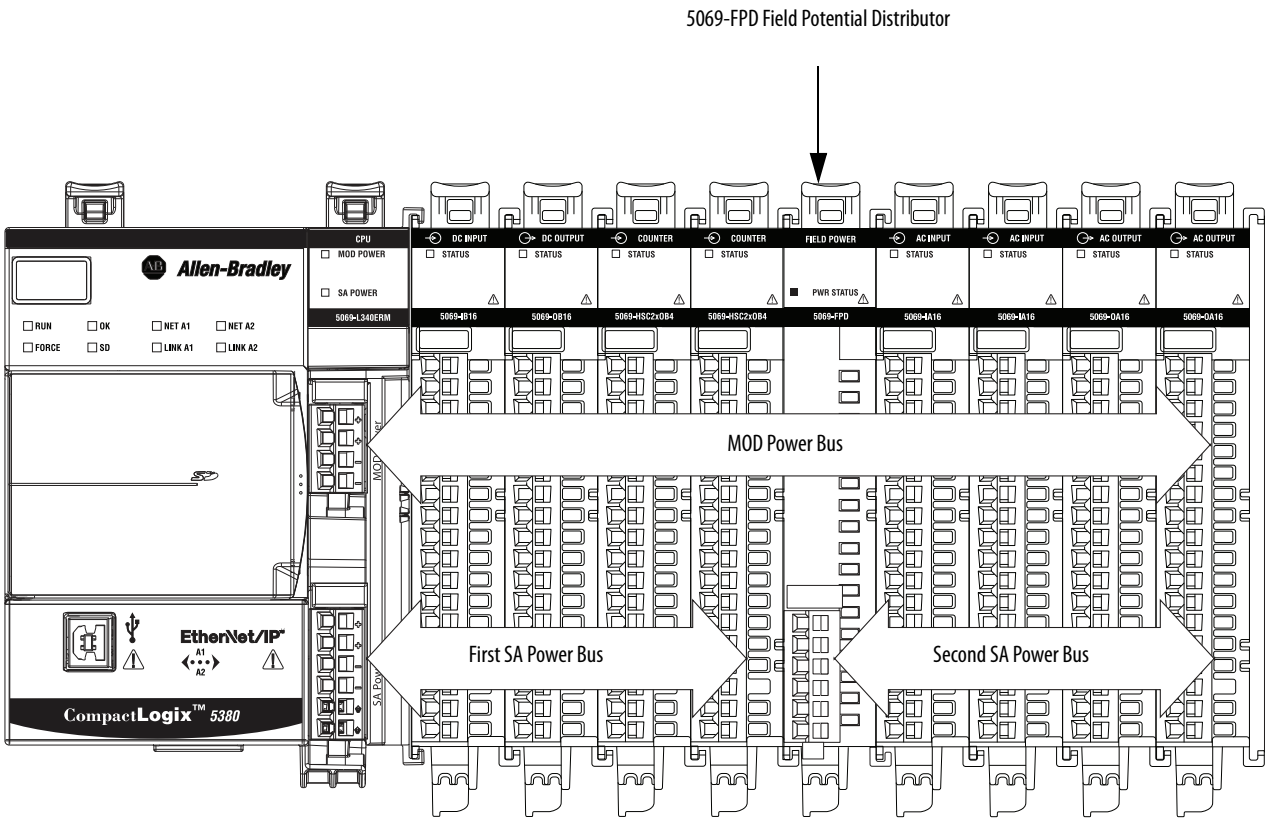
You can use a 5069-FPD field potential distributor to establish a new SA power bus in a CompactLogix 5380 system.

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.

Notes:

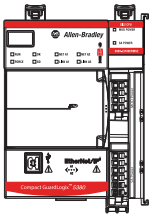
How to Power Compact GuardLogix 5380 Controllers

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 27.

Two Types of Power

Compact GuardLogix



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.

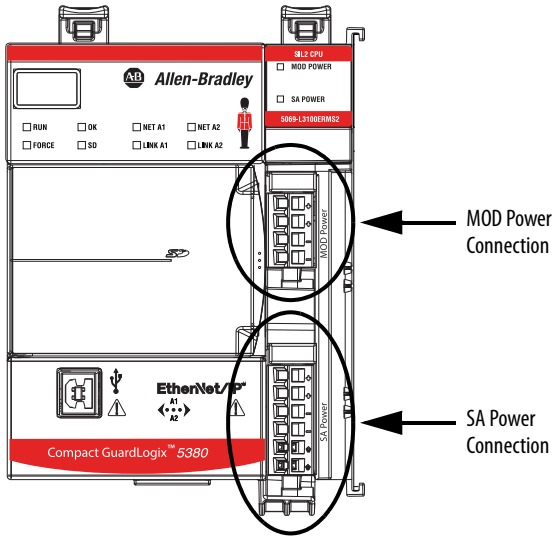
  Field-side power is provided through the SA Power RTB.

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 Power and SA Power RTBs on a Compact GuardLogix 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.

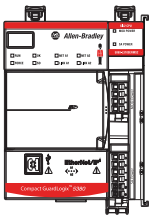
IMPORTANT We **recommend** that you use separate external power supplies for MOD power and SA power, respectively. This practice can help prevent unintended consequences that can result if you use one supply.

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 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 the Compact GuardLogix 5380 Controllers Installation Instructions, publication 5069-IN014.

MOD Power

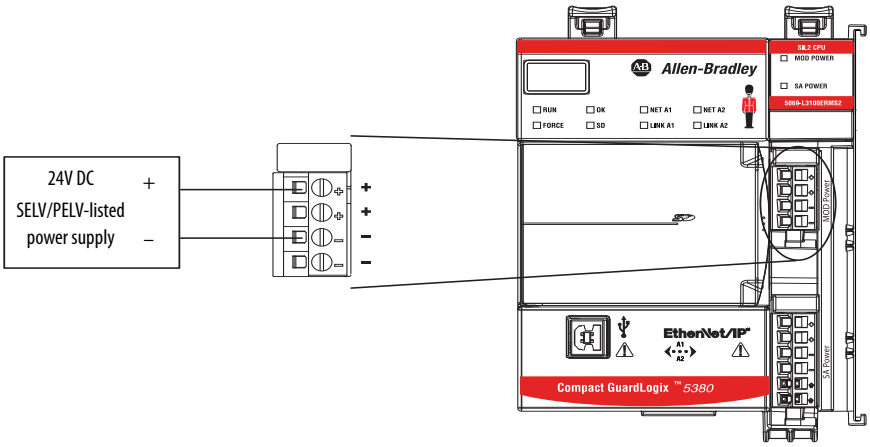
Compact GuardLogix



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

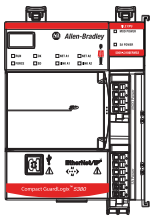
When the MOD power source is turned on, the following occurs.

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

Compact GuardLogix



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 45.

- 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 44.

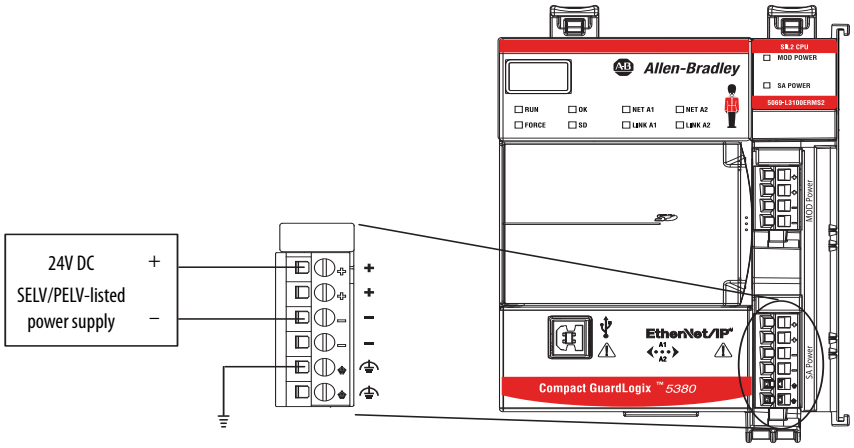
- We recommend that you use an external power supply that is adequately sized for the total SA power bus current draw on an individual bus. You must consider **current inrush requirements** when you calculate the total SA power bus current draw on a specific bus.

- 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.

That is, 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:

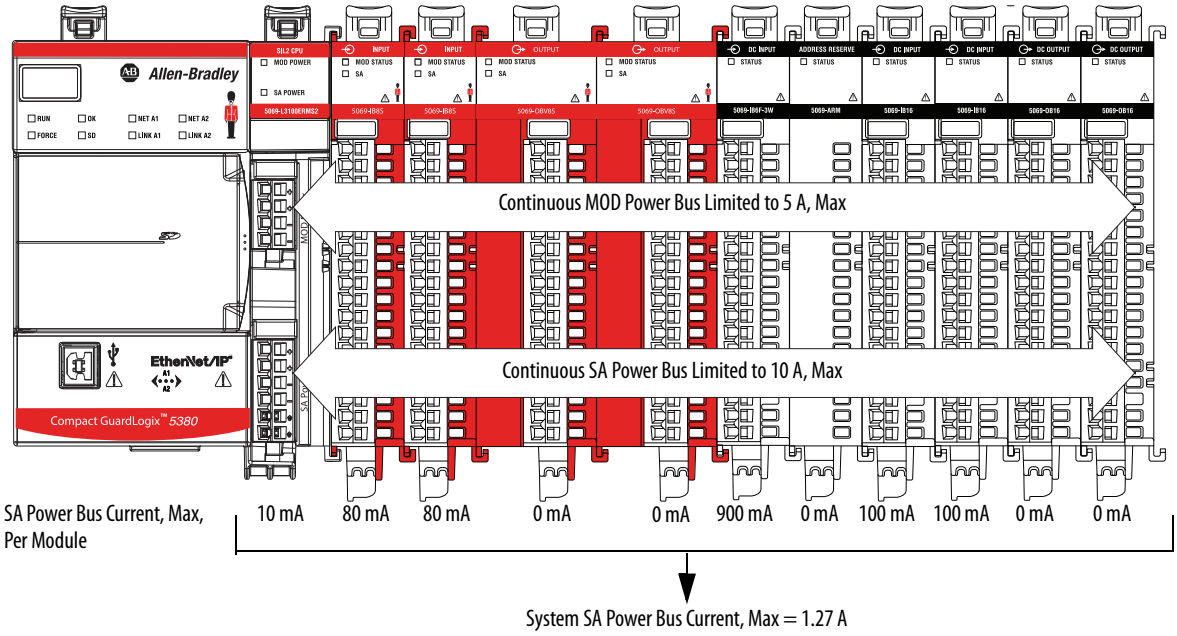
- The values in this example represent a worst-case calculation. That is, all modules that draw SA power bus current, draw the maximum available on the module.
- Not all modules that are shown in Figure 14 on page 43 use SA power bus current. For example, the 5069-OBV8S, 5069-ARM and 5069-OB16 modules 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



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 local 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.

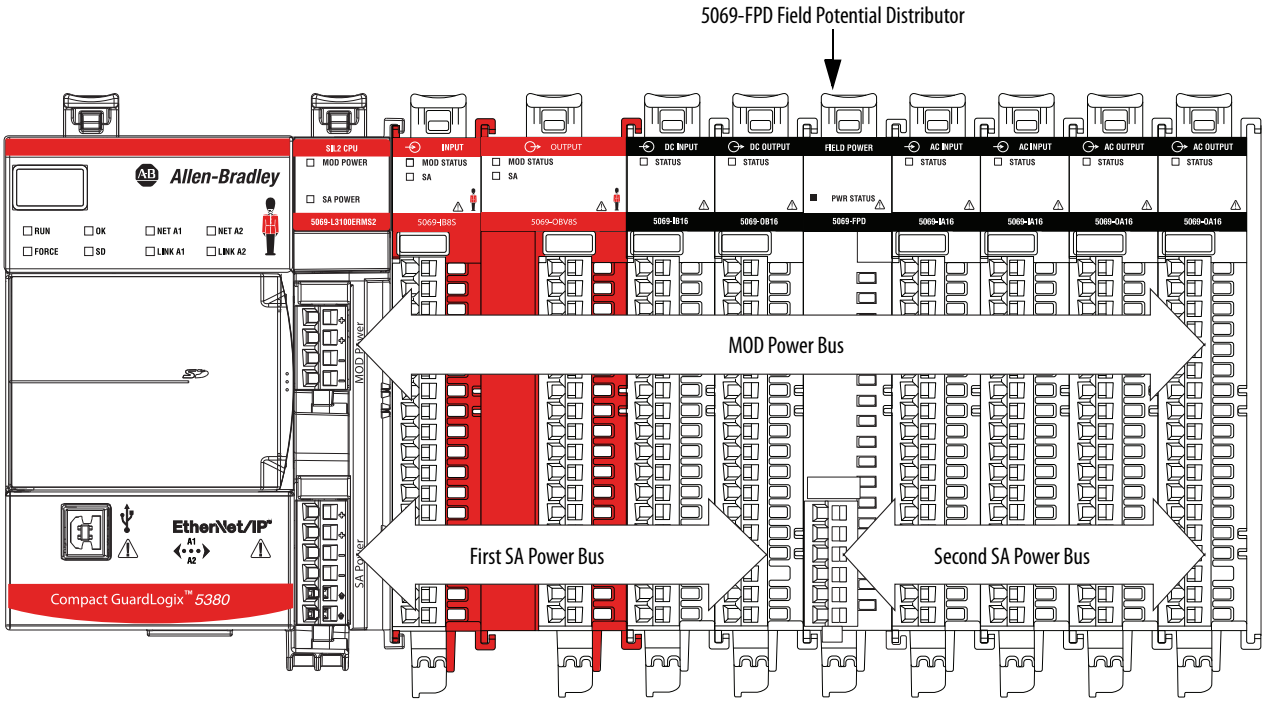
You can connect either a 24V DC or 120/240V AC external power supply to a 5069-FPD field potential distributor in a Compact GuardLogix 5380 system.

IMPORTANT Some restrictions apply when you connect SA power to a 5069-FPD field potential distributor.

For more information, see page 45.

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

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



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

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

Remember these restrictions in Table 4 when 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 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

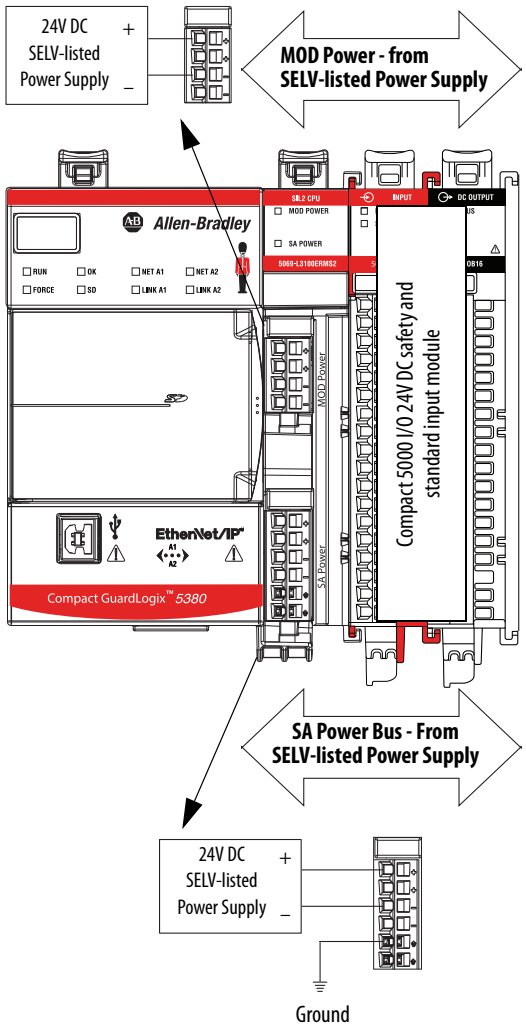


Table 4 - SA Power Restrictions - Compact GuardLogix 5380 System

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 45, 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

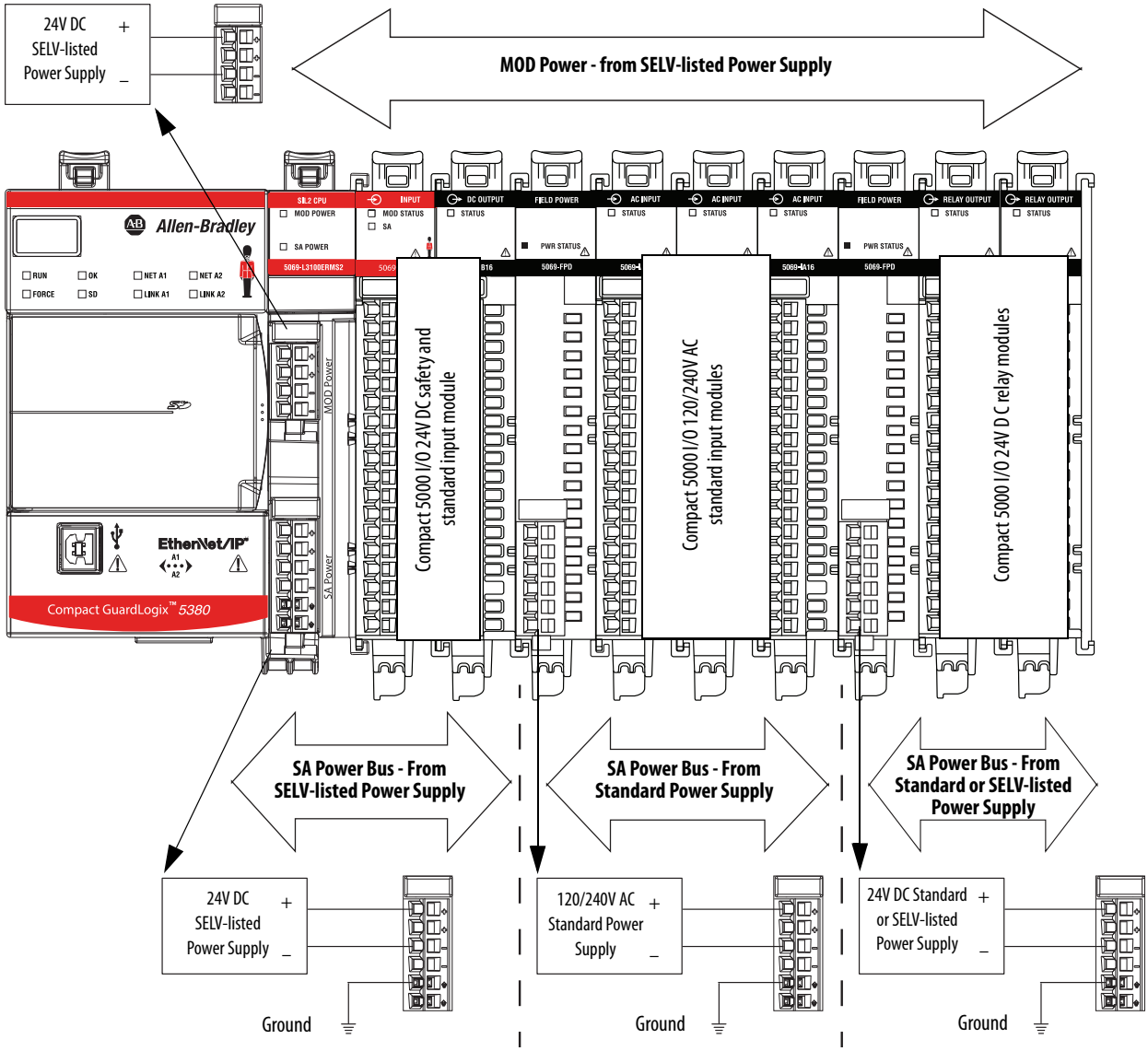
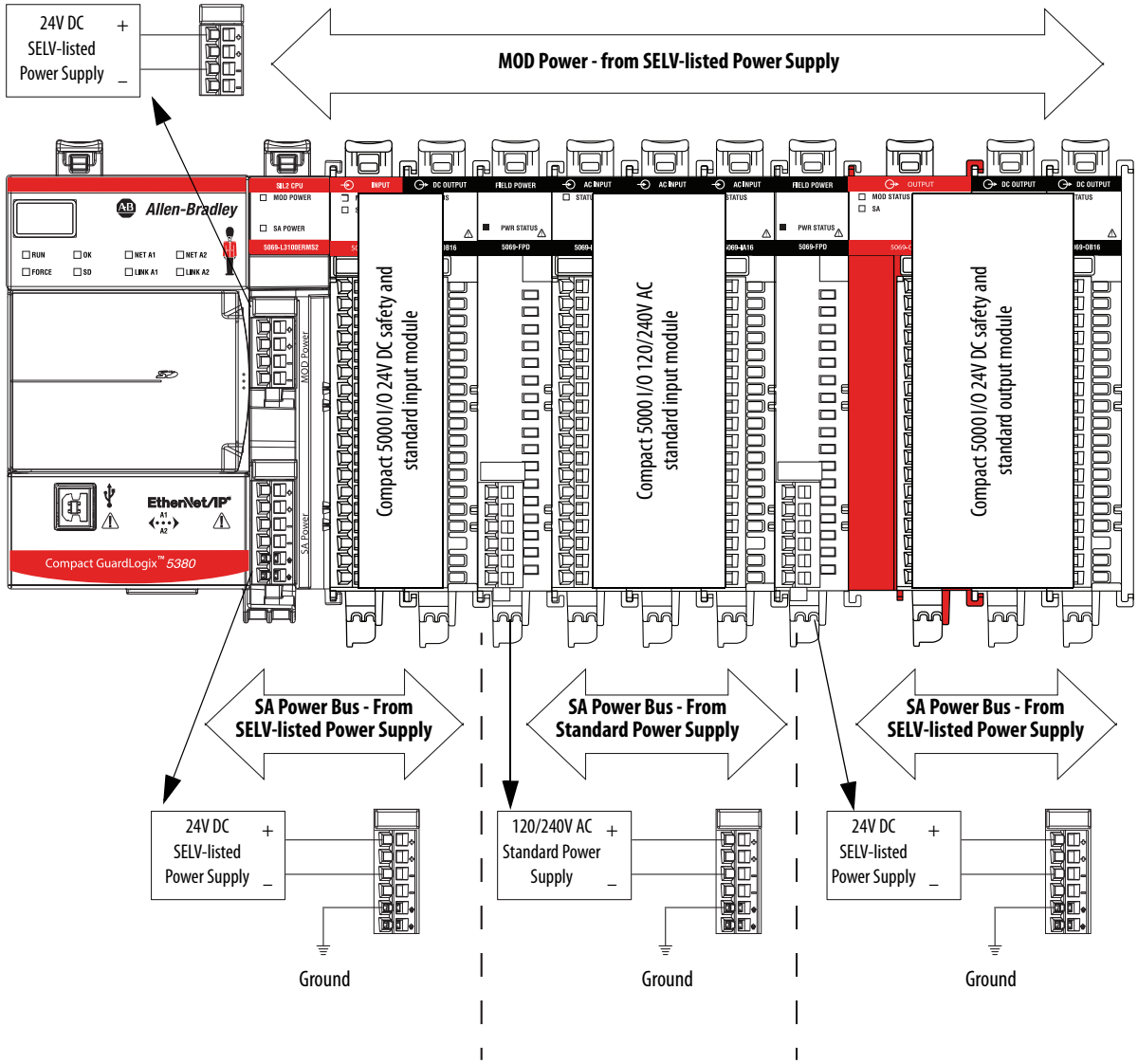


Table 4 - SA Power Restrictions - Compact GuardLogix 5380 System

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 45 and page 46, 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 System



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.

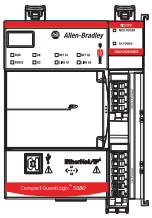
  In this case, you can use the same external power supply that is connected to the SA power RTB on the controller to the LA+ and LA– terminals.

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.

Safety Concept of Compact GuardLogix 5380 Controllers

Functional Safety Capability

Compact GuardLogix



The Compact GuardLogix® 5380 controller system is certified for use in safety applications up to and including SIL 2/PLd where the de-energized state is the safe state.

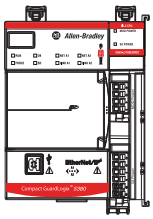
Compact GuardLogix 5380 controller-based SIL 2/PLd safety applications require a safety signature be used.

For SIL 2/PLd safety system requirements, including functional validation test intervals, system reaction time, and PFD/PFH calculations, refer 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 SIL 2/PLd safety system.

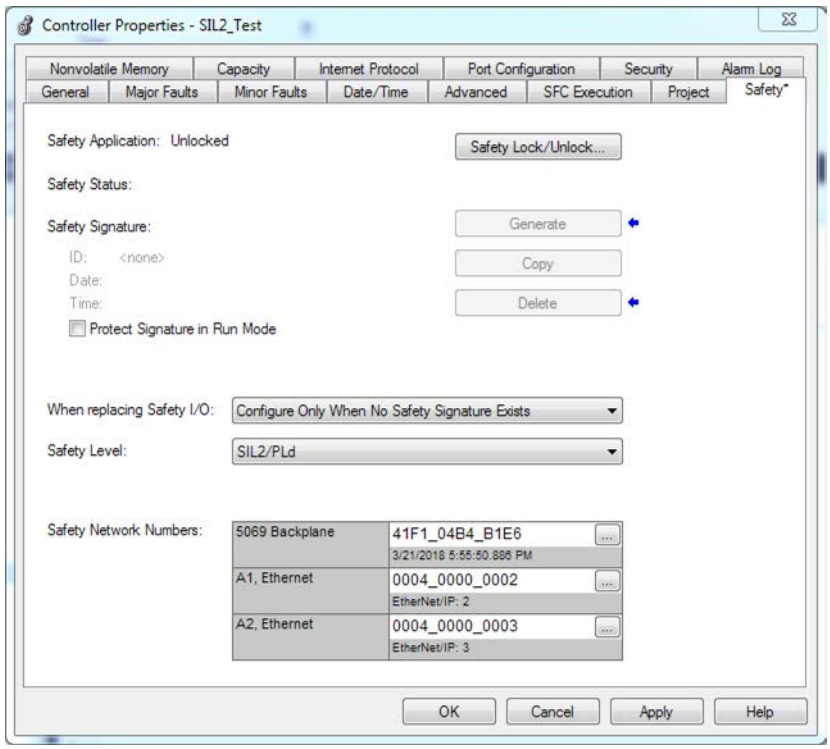
Safety Network Number

Compact GuardLogix



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.

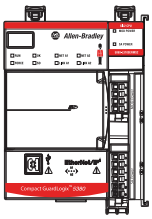


For an explanation of the Safety Network Number, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

For information on how to assign the SNN, see Assign the Safety Network Number (SNN) on page 88.

Safety Signature

Compact GuardLogix



The safety signature consists of an ID number, date, and time that uniquely identifies the safety portion of a project. This signature encompasses safety logic, data, and configuration.

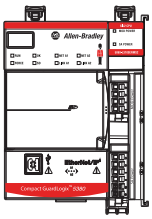
The Compact GuardLogix 5380 system uses the safety signature to determine project integrity and to let you verify that the correct project is downloaded to the target controller. The ability to create, record, and verify that the safety signature is a mandatory part of the safety-application development process.

The safety signature must be present to operate as a SIL 2/PLd safety controller.

See Generate the Safety Signature on page 262 for more information.

Distinguish between Standard and Safety Components

Compact GuardLogix



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

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

Compact GuardLogix

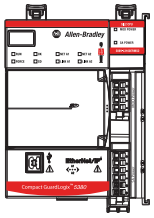
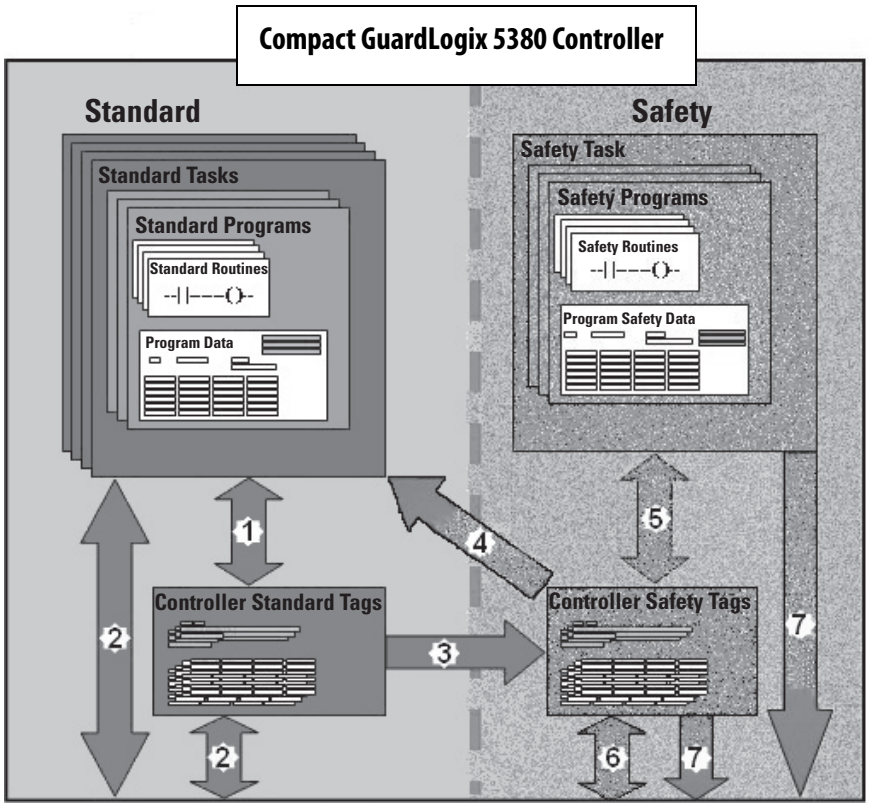


Figure 16 - Data-flow Capabilities



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 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 SIL 2/PLd data.

Safety Terminology

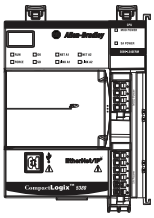
The following table defines terms that are used in this manual.

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 2/PLd-rated version of CIP.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
SIL	Safety Integrity Level	A relative level of risk-reduction 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.

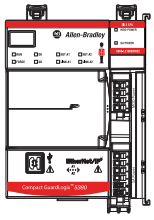
Notes:

Connect to the Controller

CompactLogix



Compact GuardLogix



You connect to a controller through Linx-based software. To use Linx-based software, you must use a communication driver that corresponds to the cable connections.

For example, before you can connect to the controller via an Ethernet cable, you must create an EtherNet/IP driver through Linx-based software.

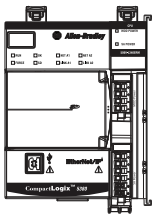
TIP The example procedures in this chapter use RSLinx® Classic. For other Linx-based communication software, the procedure can slightly differ. See the online help for your Linx-based software.

A communication driver is required to complete these tasks:

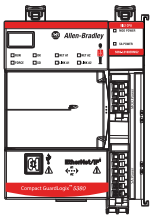
- Upload and download Studio 5000 Logix Designer® application projects
- Update controller firmware
- Set or change the controller IP address
- Collect controller data for electronic operator interfaces over an Ethernet network
- Connect RSNetWorx™ for EtherNet/IP to the Ethernet network for online monitoring of network resource utilization.

Configure EtherNet/IP and USB Drivers on Your Workstation

CompactLogix



Compact GuardLogix



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.

A workstation running the Studio 5000 Logix Designer application can use these communication drivers:

- 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
- Ethernet devices driver:
  - Lets you download a Logix Designer application project to a controller that is on an Ethernet network when your controller is not directly connected to that network
  - Requires that you configure the IP addresses to which the software browses and, therefore, the devices with which the controller communicates
- 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

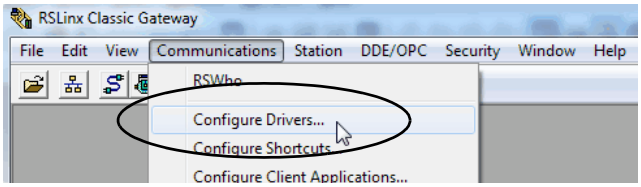
Configure the EtherNet/IP Communication Driver in RSLinx Classic Software

Before you add an Ethernet driver, confirm that these conditions exist:

- The workstation is properly connected to the EtherNet/IP network.
- The IP address and other network parameters are correctly configured for the workstation.

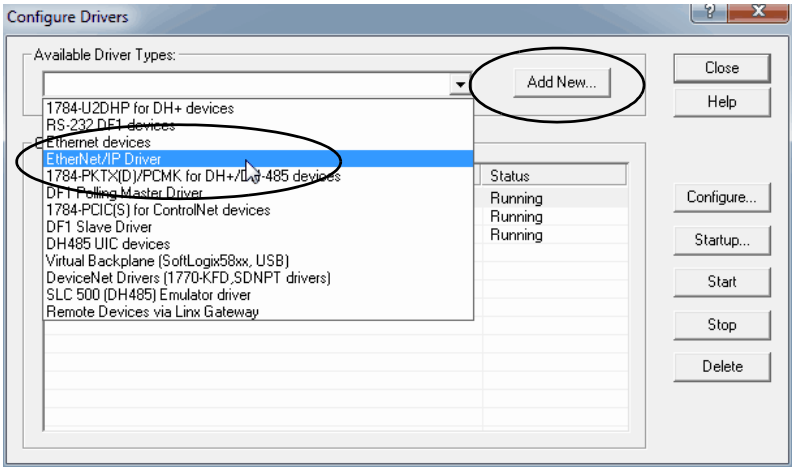
To configure the EtherNet/IP driver, complete these steps.

1. From the Communications pull-down menu, choose Configure Drivers.



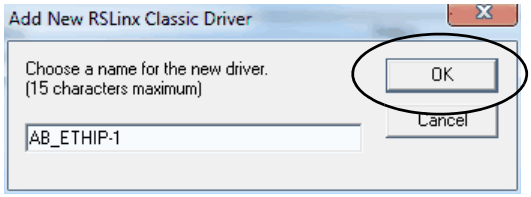
   The Configure Drivers dialog box appears.

2. From the Available Driver Types pull-down menu, choose EtherNet/IP Driver.
3. Click Add New.



The Add New RSLinx Driver dialog box appears.

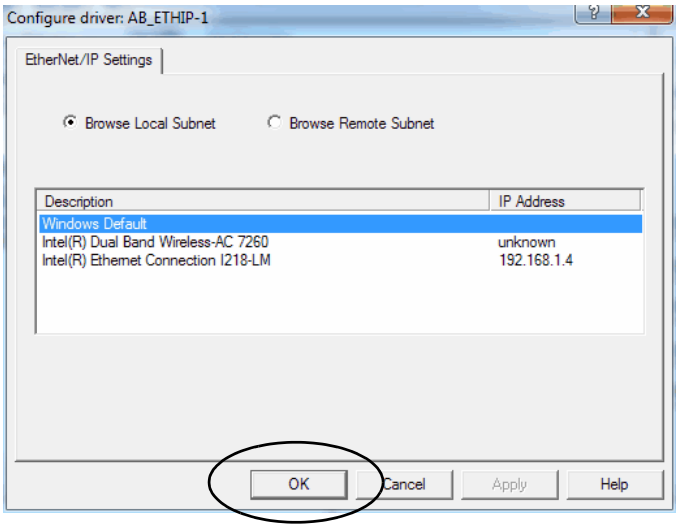
4. Type a new name or use the default name, and click OK.



The Configure driver dialog box appears.

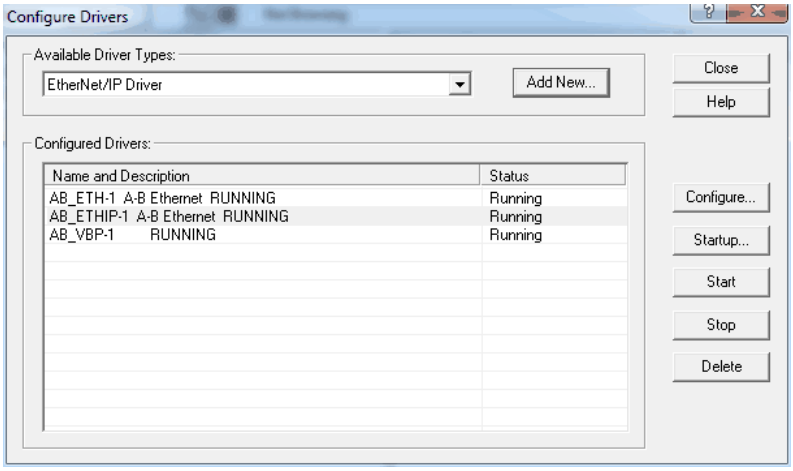
5. Click Browse Local Subnet.

TIP To view devices on another subnet or VLAN from the workstation running Linx-based communication software, click Browse Remote Subnet.



6. Select the Driver that you want to use.
7. Click OK to close the dialog box.

The new driver is available on the Configure Drivers dialog box.



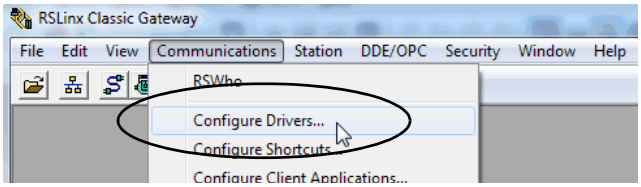
Configure the Ethernet Devices Drivers in RSLinx Classic Software

The following conditions must exist to configure an Ethernet devices driver:

- The workstation is connected to another Ethernet network than the target controller.
- The IP address and other network parameters are correctly configured on the workstation.

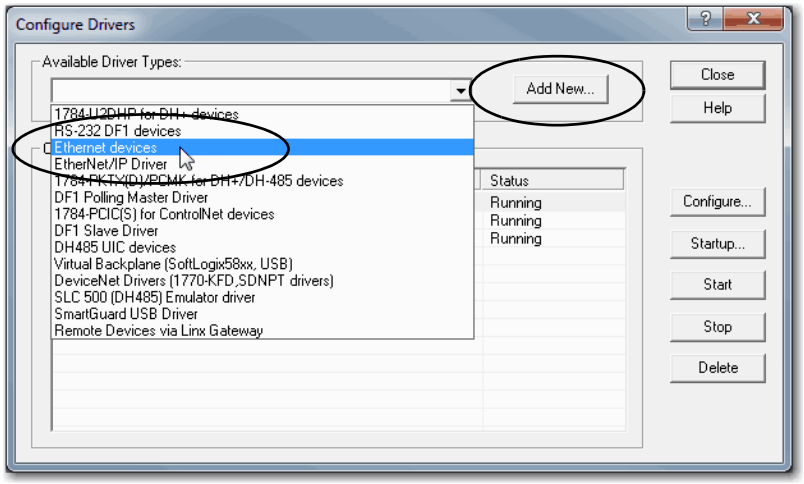
To configure the Ethernet devices driver, complete these steps.

1. From the Communications pull-down menu, choose Configure Drivers.



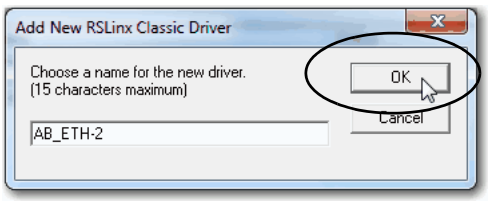
   The Configure Drivers dialog box appears.

2. From the Available Driver Types pull-down menu, choose Ethernet devices.
3. Click Add New.



   The Add New RSLinx Driver dialog box appears.

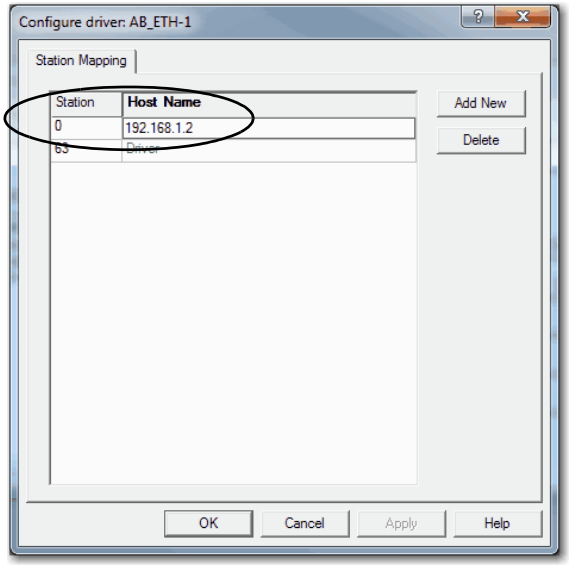
4. You can use the default name for the new drive or type a new name, and click OK.



The Configure driver dialog box appears.

5. On the Configure driver dialog box, enter a host name for each station to which RSLinx Classic software browses.

   The host name is the IP address for the device.



6. Click Add New to add stations and give each a host name.
7. When you are finished adding stations, click OK.
8. On the Configure Drivers dialog box, click Close.

Configure the USB Communication Driver in RSLinx Classic Software

In RSLinx Classic software, version 3.80.00 or later, a USB driver automatically appears in the software when you connect the USB cable from your workstation to the controller.

The USB driver can take a moment to appear in RSLinx Classic software.

IMPORTANT A USB driver appears in RSLinx Classic software only when a USB cable is connected between the workstation and the controller.

Once the cable is disconnected, the driver disappears from RSLinx Classic software.

If you use the RSLinx Classic software, version 3.80.00 or later, and a USB driver does not appear automatically, complete these steps.

1. Confirm that the USB cable is connected to the controller.

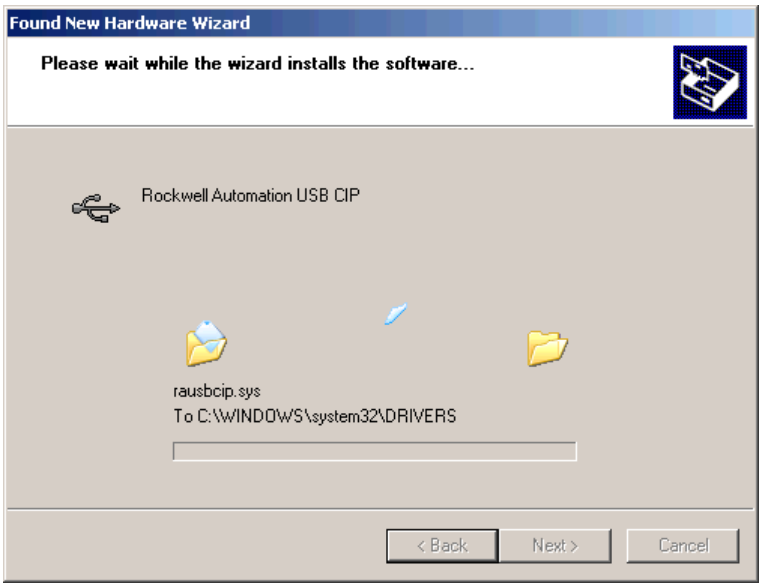
   The Found New Hardware Wizard dialog box appears.

2. Click any of the Windows Update connection options and click Next.

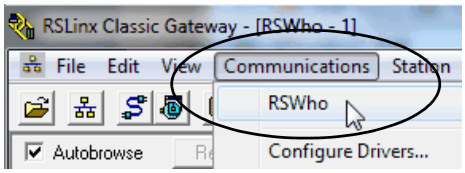
TIP If the software for the USB driver is not found and the installation is canceled, verify that you have installed RSLinx Classic software, version 3.80 or later.

3. Click Install the software automatically (Recommended) and click Next.

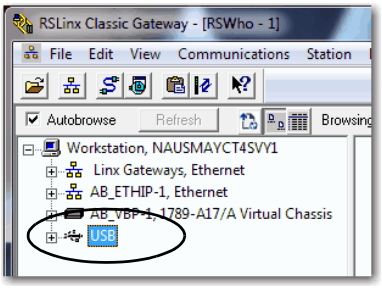
   The software is installed.



4. Click Finish to configure your USB driver.
5. From the Communications pull-down menu, choose RSWho.

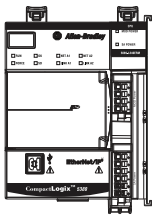


   The USB Port Driver appears in the RSLinx Classic Workstation organizer.

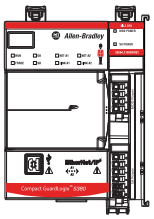


Connection Options

CompactLogix



Compact GuardLogix



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 Configure EtherNet/IP and USB Drivers on Your Workstation on page 56).

Connection options with the controller include:

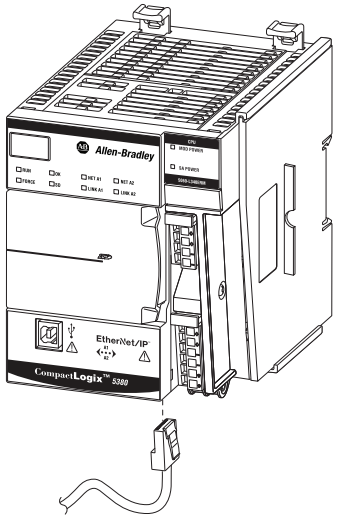
- Ethernet cable to an Ethernet port - The controller Ethernet ports support communication rates of 10 Mbps, 100 Mbps, and 1 Gbps. See Connect an Ethernet Cable on page 63.
- USB cable to the USB port - The controller USB port uses a Type B receptacle and is USB 2.0 compatible. The port runs at 12 Mbps. See Connect a USB Cable on page 64.

Connect an Ethernet Cable

The example graphic shows a CompactLogix™ 5380 controller. You perform the same task to connect an Ethernet cable to a Compact GuardLogix® 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 the controller directly to an EtherNet/IP network, connect a CAT 5e or CAT 6 Ethernet cable with an RJ45 connector to a controller Ethernet port.



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

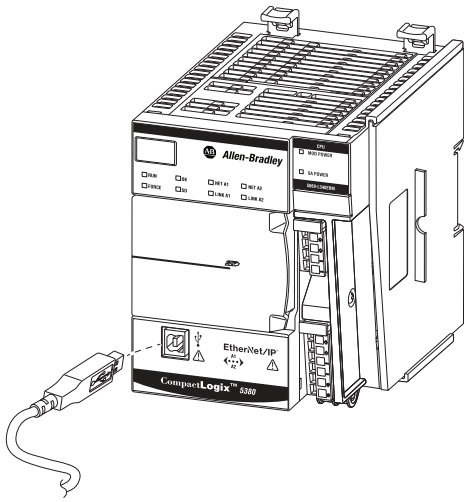
Use the USB connection to update firmware and download programs.

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.

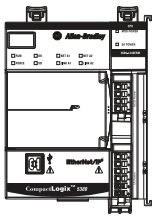
WARNING: Do not use the USB port in hazardous locations.

Figure 17 - USB Connection

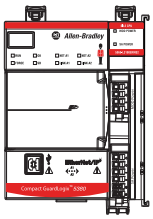


Set the Controller IP Address

CompactLogix



Compact GuardLogix



You must set the IP address on a CompactLogix 5380 or Compact GuardLogix 5380 controller for the controller to operate on an EtherNet/IP network. The controllers ship without an IP address.

IMPORTANT This section provides a general description of how to set an IP address.

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 Chapter 9, Use EtherNet/IP Modes on page 141.

Additionally, the tasks that are described in this section show a CompactLogix 5380 controller. You complete the same set of tasks to set the IP address on a Compact GuardLogix 5380 controller.

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.

You can use these tools to set the IP address:

- BOOTP-DHCP tool
- DHCP server
- RSLinx® Classic software
- SD card

Each tool has connection requirements to set the IP address via that tool. For example, your computer must be connected to the controller via a USB cable to set the initial IP address of the controller with RSLinx Classic software or the application.

To operate on an EtherNet/IP network, you must define these parameters.

EtherNet/IP Network Parameter	Description
IP address	The IP address uniquely identifies the module. The IP address is in the form *xxx.xxx.xxx.xxx* where each *xxx* is a number from 000…255. There are some reserved values that you **cannot use as the first octet** in the address. These numbers are **examples** of values **you cannot use**: 001.*xxx.xxx.xxx* 127.*xxx.xxx.xxx* 223 to 255.*xxx.xxx.xxx* The specific reserved values that cannot be used vary according to the conditions of each application. The previous values are only examples of reserved values.
Subnet mask	The subnet mask divides IP addresses into a network address and a host address. It defines whether the controller exchanges Ethernet packets directly with another device, or whether it routes packets through the Gateway. This field is set to 0.0.0.0 by default.
Gateway	A gateway connects individual physical networks into a system of networks. When a node communicates with a node on another network, a gateway transfers the data between the two networks. This field is set to 0.0.0.0 by default.

If you use Domain Name System (DNS) addressing, or reference the controller via host name in MSG instructions, define these parameters.

Table 5 - EtherNet/IP Network Parameters for DNS Addressing

EtherNet/IP Network Parameter	Description
Host name	A host name is part of a text address that identifies the host for a module. The full text address of a module is *host_name.domain_name*. **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.
Domain name	A domain name is part of a text address that identifies the domain in which the module resides. The full text address of a module is *host_name.domain_name*. The domain name has a 48-character limit. If you specify a DNS server, you must type a domain name. Also, if you send email from the module, some mail relay servers require a domain name during the initial handshake of the SMTP session.
Primary DNS server address	An address that identifies any DNS servers that are used in the network. You must have a DNS server if you specified a domain name or a host name in the module configuration. The DNS server converts the domain name or host name to an IP address that is used by the network. For more information on DNS addressing, see page 73.
Secondary DNS server address	

Set the IP Address with the BOOTP DHCP EtherNet/IP Commissioning Tool

The controllers are DHCP-enabled by default.

The BOOTP-DHCP tool is a standalone tool that you can use to set an IP address. When used, the BOOTP-DHCP tool sets an IP address and other Transport Control Protocol (TCP) parameters.

The BOOTP-DHCP tool is installed automatically when you install RSLinx Classic software or the Logix Designer application on your computer.

Access the BOOTP-DHCP tool from one of these locations:

- Programs > Rockwell Software® > BOOTP-DHCP Tool

  If you have not installed the server, you can download and install it from http://www.ab.com/networks/ethernet/bootp.html.

- Tools directory on the Studio 5000® environment installation CD

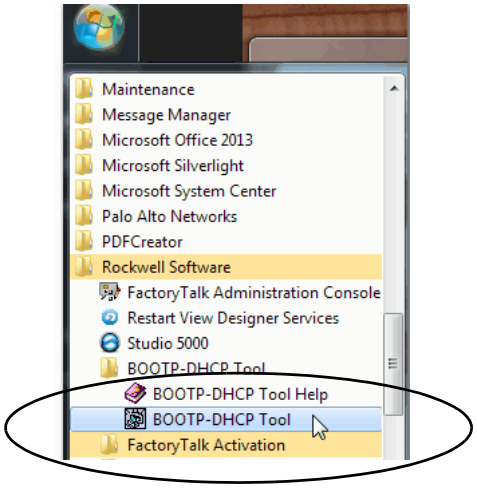
IMPORTANT Before you start the BOOTP-DHCP tool, make sure that you have the module hardware (MAC) address.

The MAC address scrolls across the controller status on the front of the controller. The address uses a format similar to the following:

00-00-BC-14-55-35

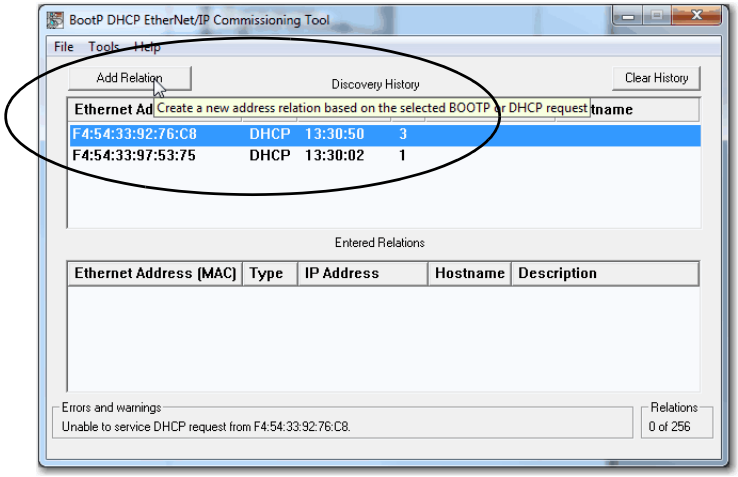
To set the IP address with a BOOTP-DHCP tool, complete these steps.

1. Connect your workstation to the Ethernet network where the controller resides.
2. Start the BOOTP-DHCP tool.



The MAC address of the controller appears in the Request History window.

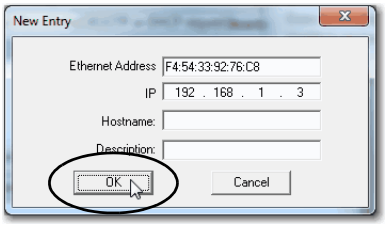
3. Select the appropriate controller and click Add to Relation List.



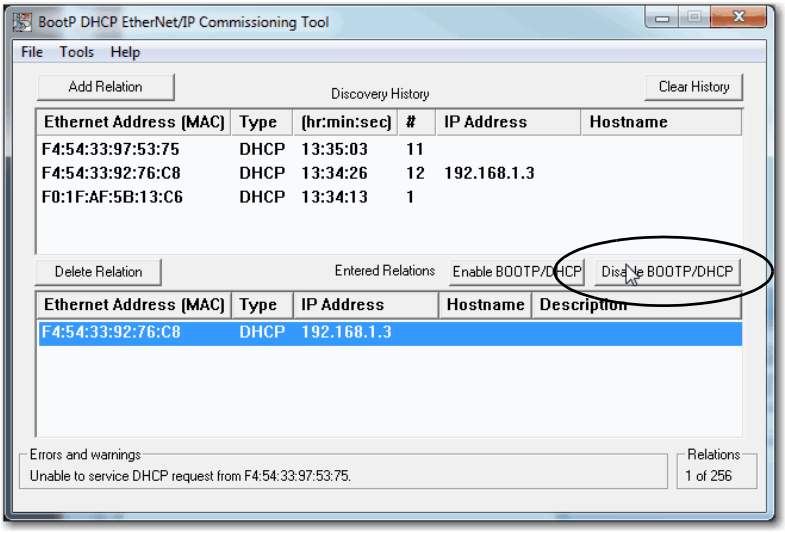
The New Entry dialog box appears.

4. Type an IP address, Hostname, and Description for the module.

   Hostname and Description are optional.



5. Click OK.
6. To assign this configuration to the module, wait for the module to appear in the Relation List panel and select it.
7. Click Disable BOOTP/DHCP.



The module now uses the assigned configuration and does not issue BOOTP or DHCP requests after power is cycled on the controller.

IMPORTANT Remember the following:

- If you do not click Disable BOOTP/DHCP, on future power cycles, the current IP configuration is cleared and the controller sends DHCP requests again.
- If you click Disable BOOTP/DHCP and it does not disable BOOTP/DHCP, you can use RSLinx Classic software to disable BOOTP/DHCP.

For more information on how to use RSLinx Classic software to disable BOOTP/DHCP, see page 69.

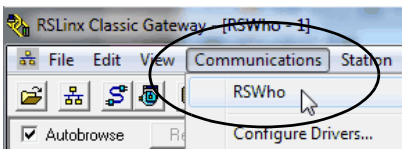
Disable BOOTP/DHCP with RSLinx Classic Software

To disable BOOTP/DHCP from RSLinx Classic software, complete these steps.

1. Start RSLinx Classic software.

   After several seconds, an RSWho dialog box appears.

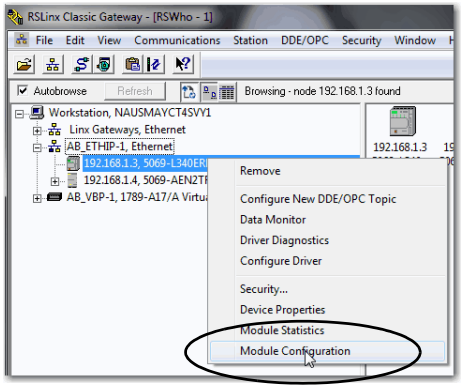
2. If no RSWho dialog box appears, from the Communications pull-down menu, choose RSWho.



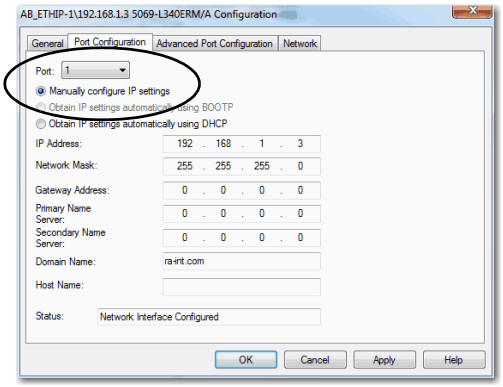
3. Navigate to the controller.

You can access the controller via the USB or an EtherNet/IP driver.

4. Right-click on the controller and choose Module Configuration.



5. Click the Port Configuration tab.
6. From the Network Configuration Type, click Static to disable BOOTP/DHCP.



7. Click OK.

Use a DHCP Server to Set the Controller IP Address

Because the controllers are DHCP-enabled when they are in the out-of-box condition, you can use a DHCP server to set the IP address.

The DHCP server automatically assigns IP addresses to client stations logging on to a TCP/IP network. DHCP is based on BOOTP and maintains some backward compatibility.

ATTENTION: You can use a DHCP server that is configured to always assign the same IP address to specific devices when they appear on the EtherNet/IP network and request an IP address.

If your system **does not** use a DHCP server that assigns the same IP address for specific devices, we strongly recommend that you assign the controller a fixed IP address. Do not set the IP address dynamically. That is, do not use the Obtain IP settings automatically by using DHCP option in RSLinx Classic software or the Logix Designer application.

When a controller uses Obtain IP settings automatically by using DHCP, the IP address for that controller is cleared with each power cycle. If the same IP address is not automatically assigned to the controller via a DHCP server, when it requests a new IP address, it can be assigned a new IP address.

The use of a new IP address can have unintended consequences. For example, a Duplicate IP Address condition can exist or the controller can experience configuration faults because the IP address differs from what is stored in the Logix Designer application project.

Failure to observe this precaution can result in unintended machine motion or loss of process control.

Duplicate IP Address Detection

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

- Connect the 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. To assign a new IP address to the controller and leave Conflict mode, see Set the IP Address with the BOOTP DHCP EtherNet/IP Commissioning Tool on page 67.
• 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: a. Assign a new IP address to the controller. For more information, see Set the IP Address with the BOOTP DHCP EtherNet/IP Commissioning Tool on page 67. b. Cycle power to the other device.
One device supports duplicate IP address detection and a second device does not.	1. Regardless of which device obtained the IP address first, the device that does not support IP address detection uses the IP address and continues to operate without interruption. 2. The device that supports duplicate IP address detection detects the duplication and enters Conflict mode. To assign a new IP address to the controller and leave Conflict mode, see Set the IP Address with the BOOTP DHCP EtherNet/IP Commissioning Tool on page 67.

DNS Addressing

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

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

To use DNS addressing, follow these steps.

1. Assign a host name to the controller.

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

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

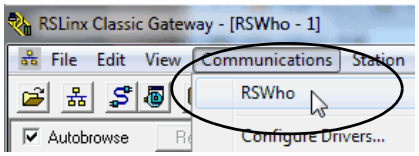
IMPORTANT Remember the following:

- 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.

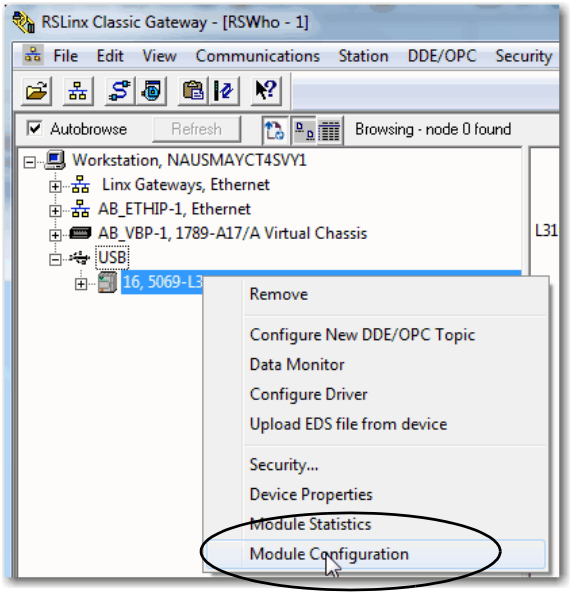
Use RSLinx Classic Software to Set the Controller IP Address

Complete these steps to set the IP address of the controller with RSLinx Classic software.

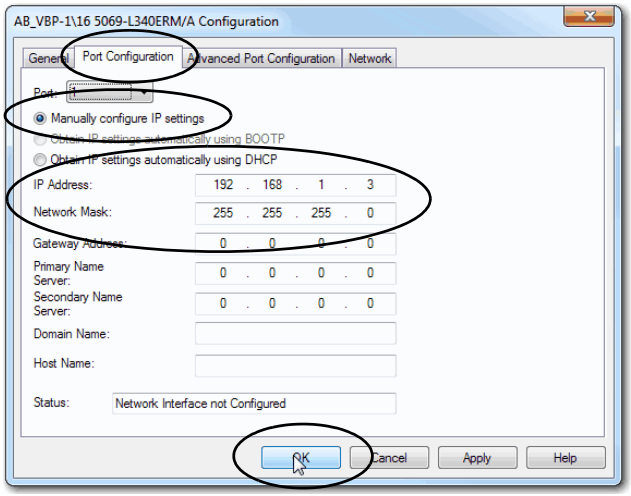
1. Confirm that your computer is connected to the controller via a USB cable.
2. Start the RSLinx Classic software. After several seconds, an RSWho dialog box appears.
3. If the RSWho dialog box does not appear, from the Communications pull-down menu, choose RSWho.



4. Navigate to the controller via the USB driver.
5. Right-click the controller and choose Module Configuration.



6. On the Port Configuration tab, click Manually configure IP settings for the port.
7. Assign the port configuration parameters and click OK.



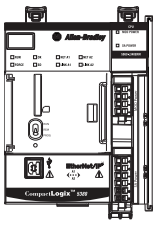
Use a Secure Digital Card to Set the Controller IP Address

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.

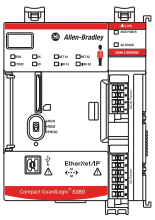
For more information on how to use an SD card, see Chapter 7, Use the Secure Digital Card on page 117.

Update Controller Firmware

CompactLogix



Compact GuardLogix



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

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

IMPORTANT **Safety Consideration**

You cannot update a controller that is safety locked.

You can use these tools to update the controller firmware:

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

To update the controller firmware, complete these tasks:

- Determine Required Controller Firmware
- Obtain Controller Firmware
- Use ControlFLASH Software to Update Firmware
- Use AutoFlash to Update Firmware

IMPORTANT This section provides a general description of how to update controller firmware.

Firmware changes can have different effects on some controllers based on system conditions when the change is made, particularly regarding the EtherNet/IP mode that is used.

For more information on how controller firmware revision changes can affect your controller configuration regarding EtherNet/IP mode use, see Chapter 9, Use EtherNet/IP Modes on page 141.

Determine Required Controller Firmware

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

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

Not all controllers support the same minimum firmware revisions.

Make sure that you are aware of the appropriate firmware revision, and compatible software version, for your controller before obtaining and updating firmware.

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center (PCDC) at http://compatibility.rockwellautomation.com/Pages/home.aspx.

Obtain Controller Firmware

You can obtain controller firmware in these ways:

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

  IMPORTANT The firmware that is packaged with the software installation is the initial release of the controller firmware. Subsequent firmware revisions can be released.

  We recommend that you check the PCDC to determine if later revisions of the controller firmware are available. For more information, see the next bullet.

- Download firmware, associated files, and access product release notes from the PCDC:

  http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page

Use ControlFLASH Software to Update Firmware

IMPORTANT Based on the catalog number, Logix Designer application version, and firmware revision that are used, CompactLogix 5380 and Compact GuardLogix 5380 controllers have different minimum ControlFLASH™ software version requirements.

To determine the minimum software version for your application, see the PCDC at: http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page.

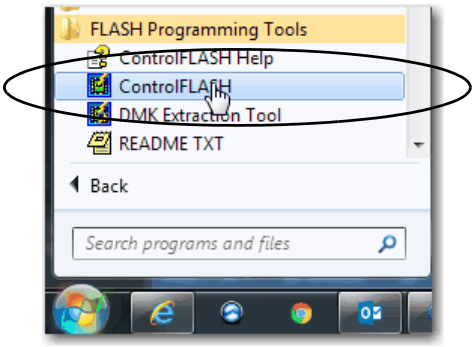
The ControlFLASH software is available as follows:

- Part of Studio 5000 Logix Designer application installation process
- Standalone download from the PCDC.

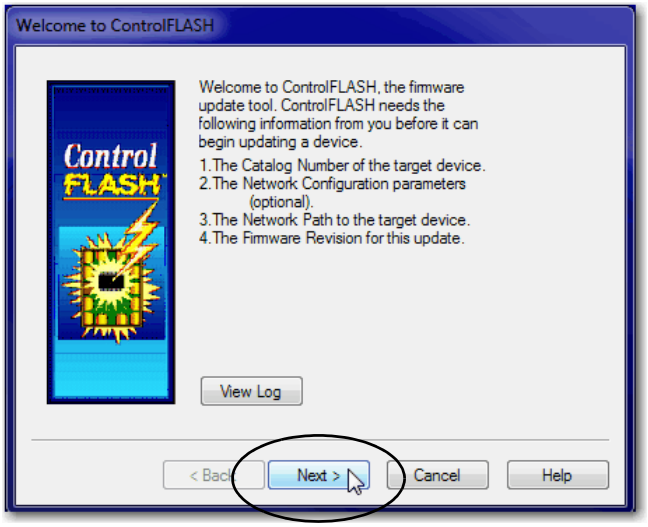
ATTENTION: If the Secure Digital (SD) card is locked and set to load on power-up, this update can be overwritten by firmware on the SD card.

For more information on how to use SD cards, see Chapter 7, Use the Secure Digital Card on page 117.

1. Verify the following:
   - The network connection is made.
   - The network driver has been configured in Linx-based communication software.
   - The controller is in Remote Program or Program mode and all major recoverable faults are cleared.
2. From the Windows Start Menu, click FLASH Programming Tools > ControlFLASH.

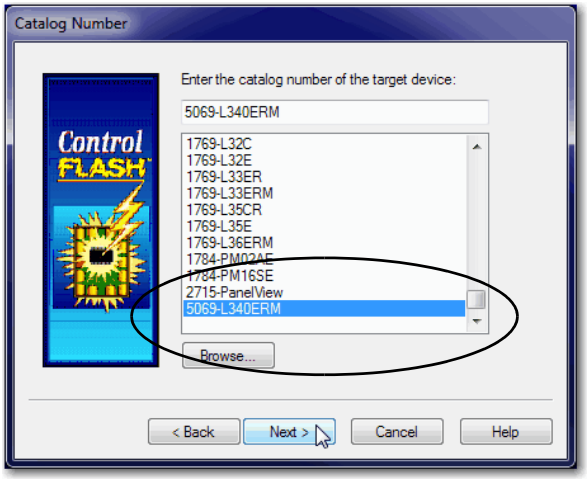


3. Click Next.

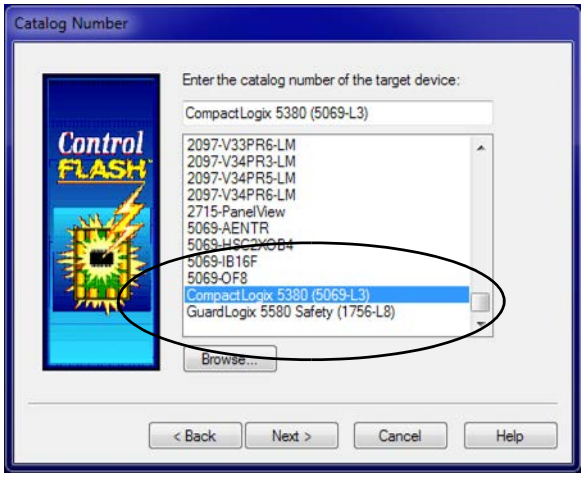


4. Select the controller, and click Next.

   ControlFLASH version 15.01.00 or later has a family name that applies to all controllers in that family, instead of individual controller catalog numbers.

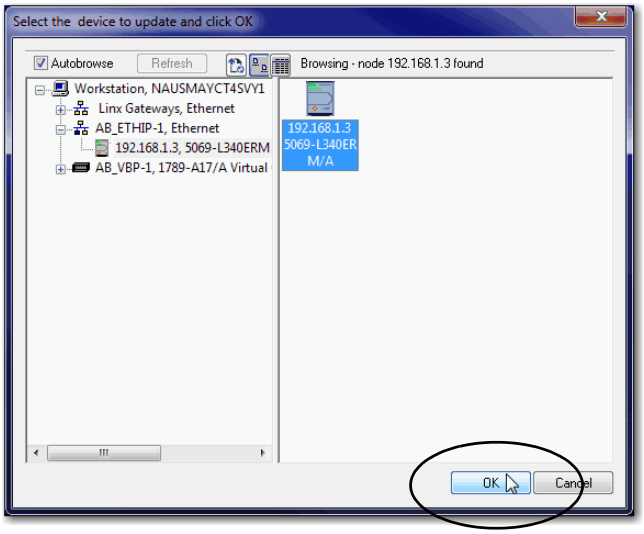


ControlFLASH version 14.01.00 or earlier



ControlFLASH version 15.01.00 or later

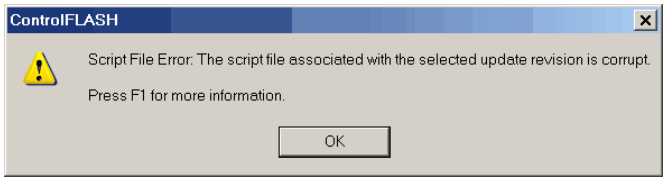
5. Expand the communication path and select the controller.
6. Click OK.



7. Select the firmware revision and click Next.

   If the firmware revision you need is not on the list, choose Show all revisions.

   TIP If you experience a Script File Error after you select the firmware revision number, as shown, there can be an issue with your firmware files.

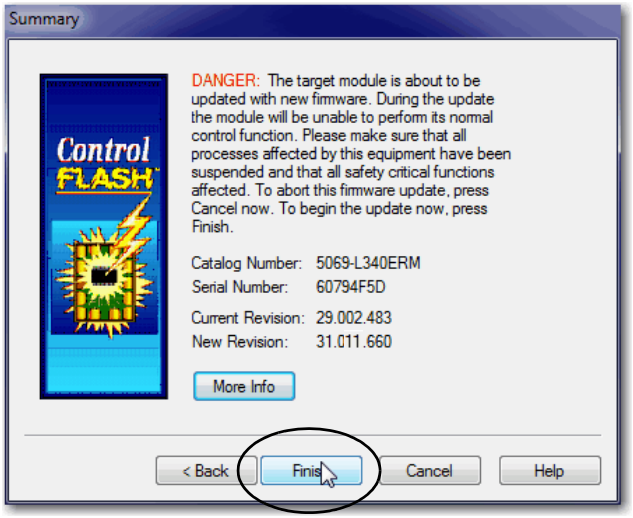
   

   We recommend that you use the latest version of the ControlFLASH software. If you are not, first upgrade to the latest version.

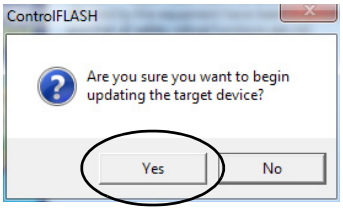
   To resolve the issue, perform the following:

   - Go to http://www.rockwellautomation.com/support/ and download the firmware revision you are trying to update. Replace the firmware revision that you have previously installed with that posted on the Technical Support website.
   - If the replacement firmware revision does not resolve the anomaly, contact Rockwell Automation Technical Support.

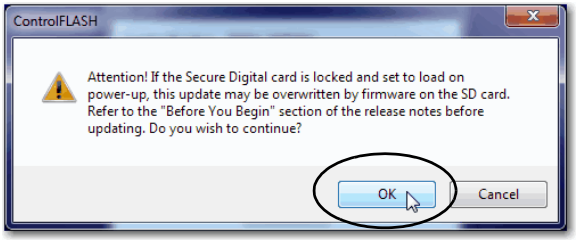
8. On the Summary Screen, click Finish.

9. When a confirmation dialog box appears, click Yes.

Before the firmware update begins, this dialog box appears. Take the required action for your application. In this example, the upgrade continues when OK is clicked.



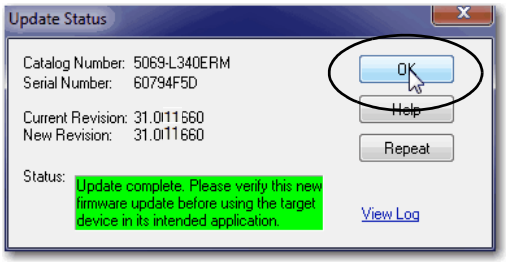
The progress dialog box indicates the progress of the firmware update. The controllers indicate progress in updates and blocks.

IMPORTANT Let the firmware update complete before you cycle power or otherwise interrupt the update.

If the firmware update is interrupted, the controller reverts to boot firmware, that is, revision 1.*xxx*.

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

10. Click OK.



11. Close the ControlFLASH software.

Use AutoFlash to Update Firmware

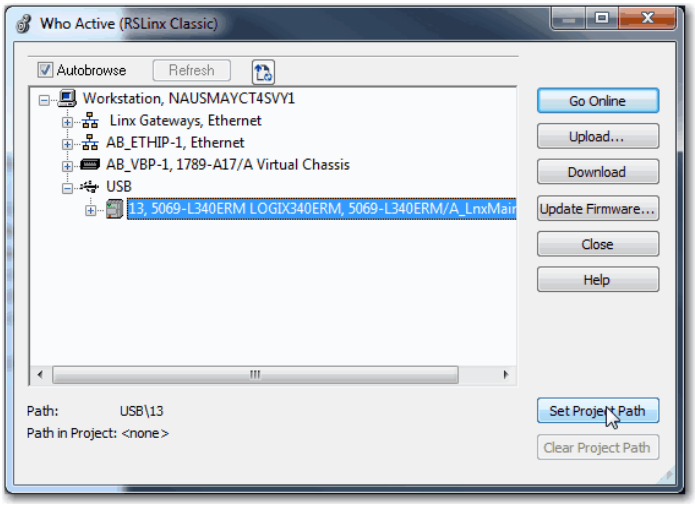
To update the controller firmware with the AutoFlash feature, complete these steps.

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.

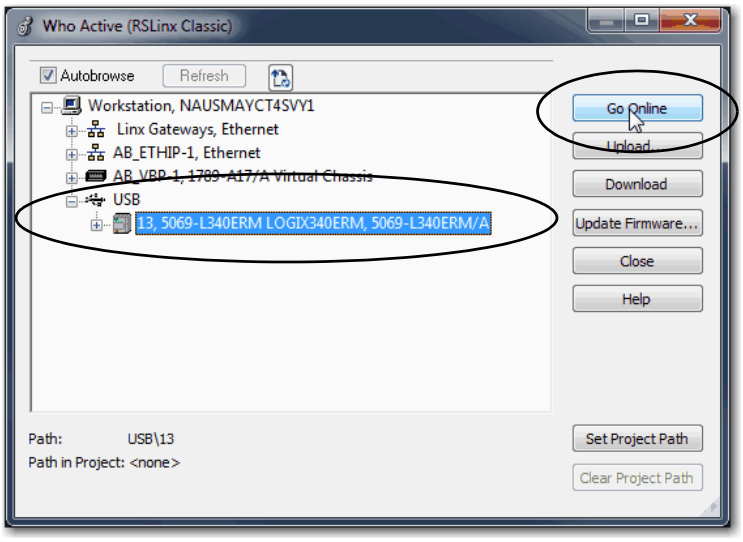
1. Verify the following:
   - The network connection is made.
   - The network driver has been configured in Linx-based communication software.
   - The controller is in Remote Program or Program mode and all major recoverable faults are cleared.
2. Start the Logix Designer application, and create a project.

   For more information, see Create a Logix Designer Application Project on page 85.
3. In the project, click RSWho.

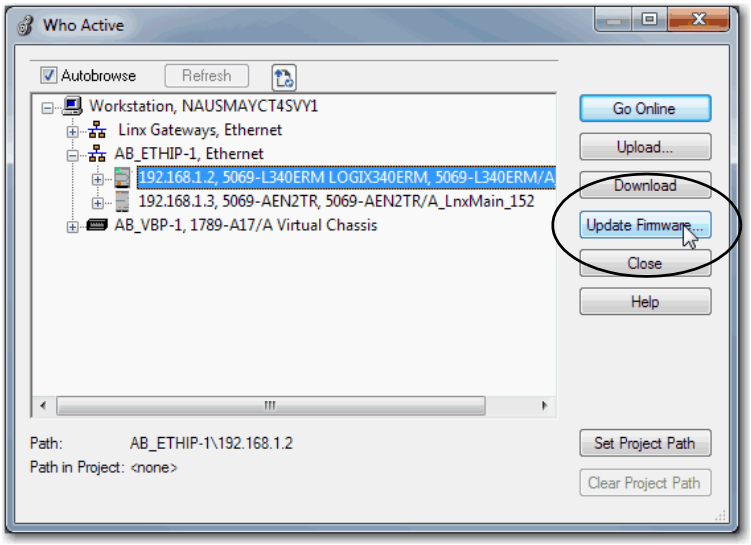
4. Expand the communication path and select the controller.



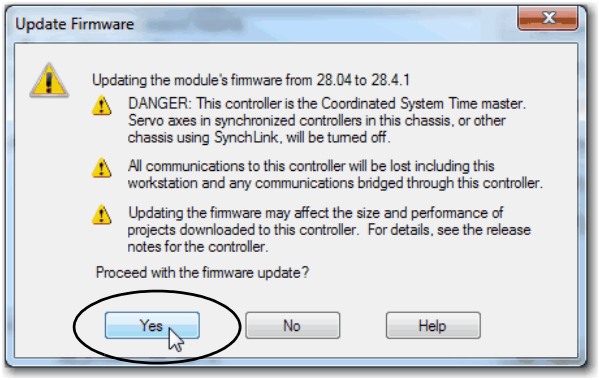
5. Select the controller and click Go Online.



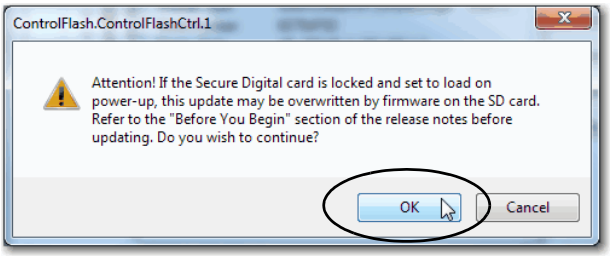
6. On the Who Active dialog box, select the controller under the communication driver you want to use, and click Update Firmware.



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.



10. On the ControlFlash Attention dialog, click OK.



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.

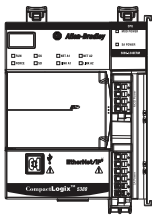
11. Click OK on the Who Active dialog box.

Start to Use the Controller

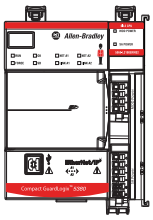
Create a Logix Designer Application Project

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.

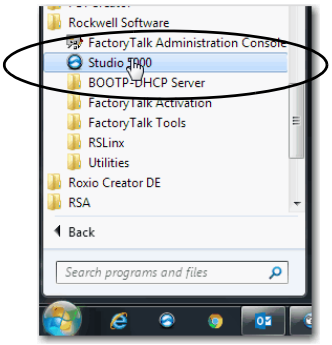
CompactLogix



Compact GuardLogix

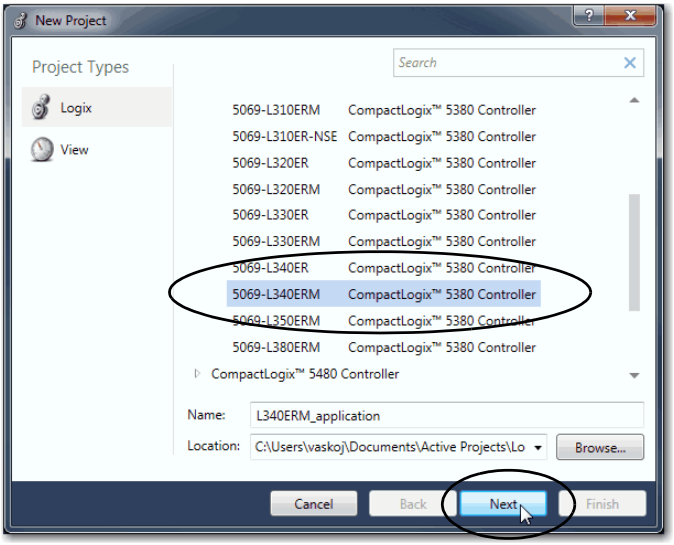


1. Start the application. The Logix Designer application is part of the Studio 5000® environment.



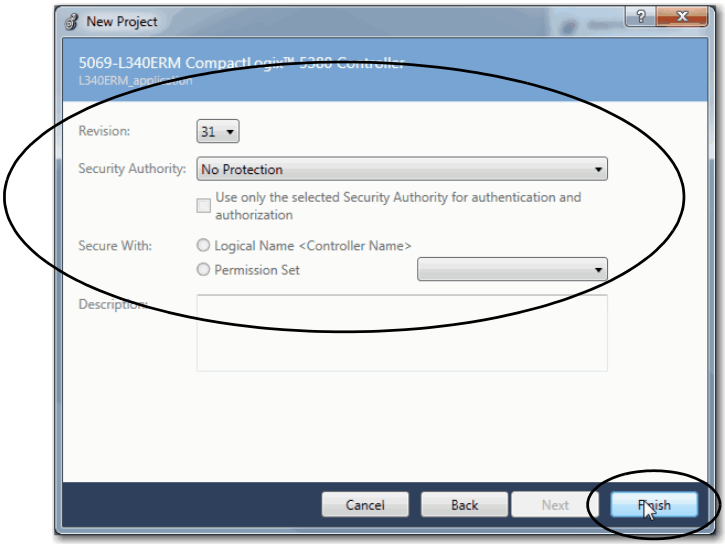
2. Click New Project.

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.



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

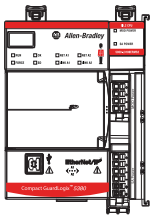
   For information on security, refer to the Logix 5000 Controllers Security Programming Manual, publication 1756-PM016.



5. Click Finish.
6. Based on your controller:
   - For a Compact GuardLogix® 5380 controller, continue with Additional Configuration for a Compact GuardLogix Controller on page 88.
   - For a CompactLogix™ 5380 controller, continue with Go Online with the Controller on page 95.

Additional Configuration for a Compact GuardLogix Controller

Compact GuardLogix

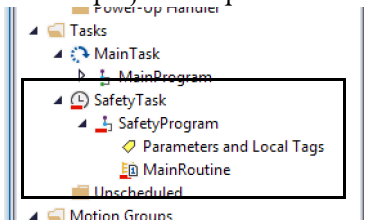


Compact GuardLogix 5380 controllers require additional configuration after you create the project. These topics describe how to configure the additional parameters.

Topic	Page
Assign the Safety Network Number (SNN)	88
Go Online with the Controller	95

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.

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

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

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

- Automatic Assignment of Time-based SSN on page 90
- Manual Assignment of SSN on page 91

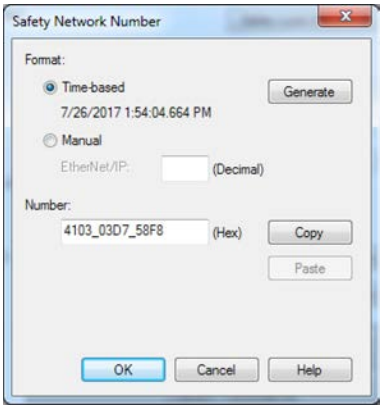
Automatic Assignment of Time-based SSN

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 18 - Time-based Format



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.

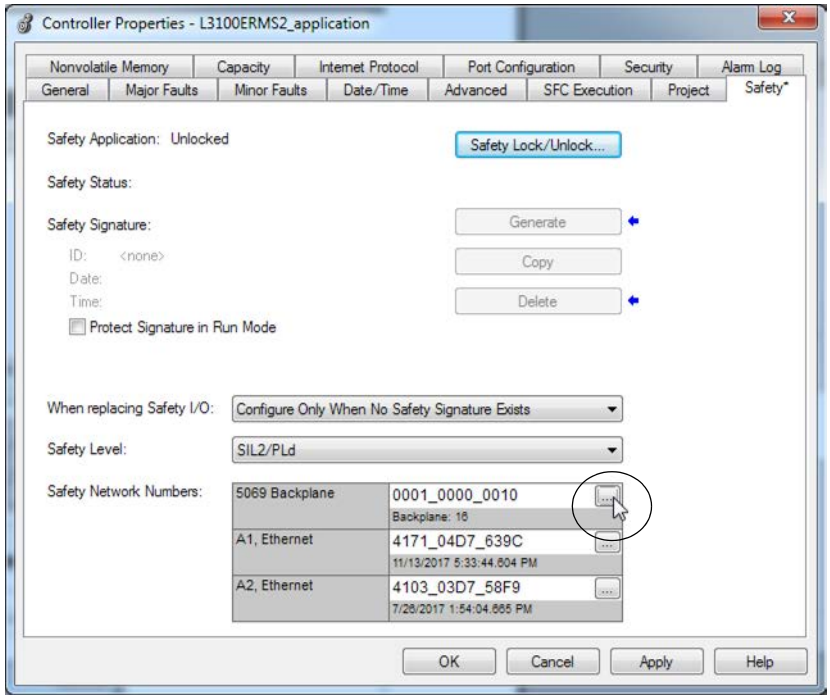
However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Logix Designer application, and you will not see a warning.

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.

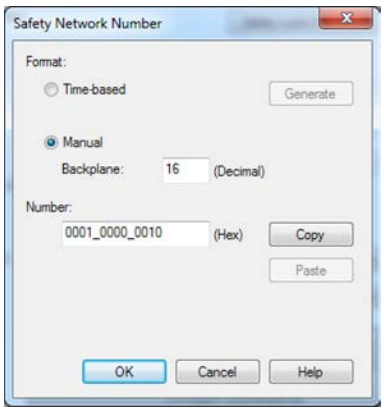
If there are duplicate unique node references, as the system user, you are responsible for proving that an unsafe condition cannot result.

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, click the Safety tab.
3. On the Safety tab, click [...] to the right of the safety network number for the port that you want to change.



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



6. Click OK.

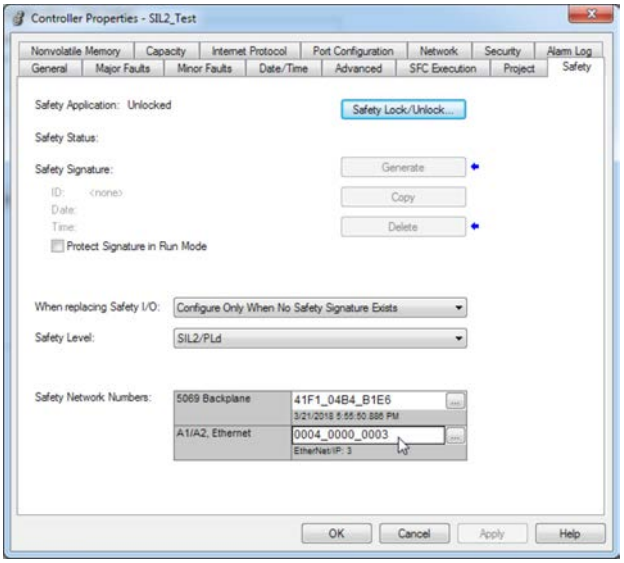
Copy and Paste a Safety Controller Safety Network Number (SNN)

If you must apply an SNN to other safety controllers, you can copy and paste the SNN. There are multiple ways to copy and paste safety controller SNNs.

Copy a Safety Controller SNN

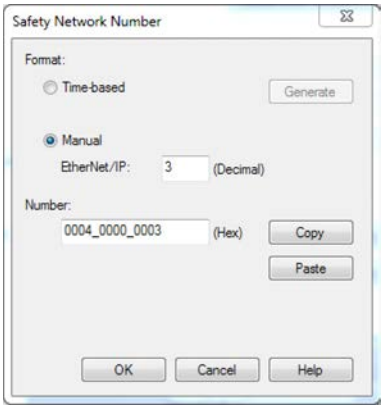
From the Controller Properties Safety Tab:

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



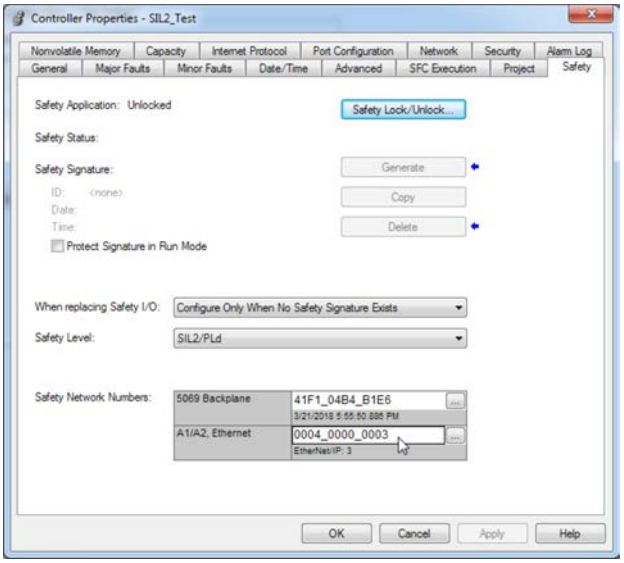
From the Safety Network Number dialog:

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

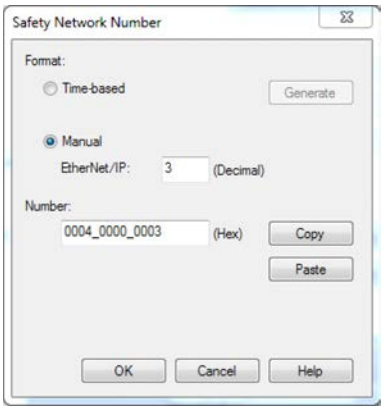


Paste a Safety Controller SNN

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



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

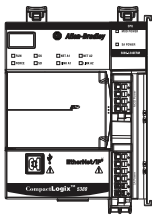


4. Click OK.
5. On the Controller Properties Safety tab, click OK.

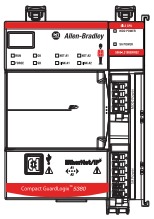
Go Online with the Controller

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

CompactLogix



Compact GuardLogix

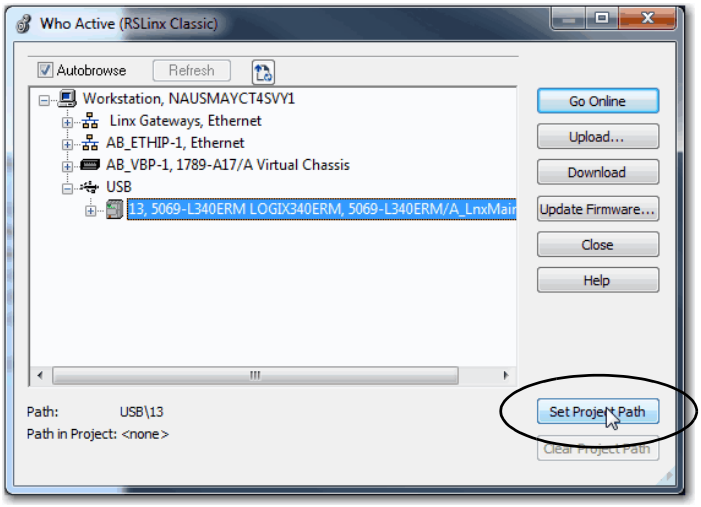


TIP For this section, the USB port was chosen as the communication path. Another path through the embedded Ethernet ports is also possible.

Use RSWho

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

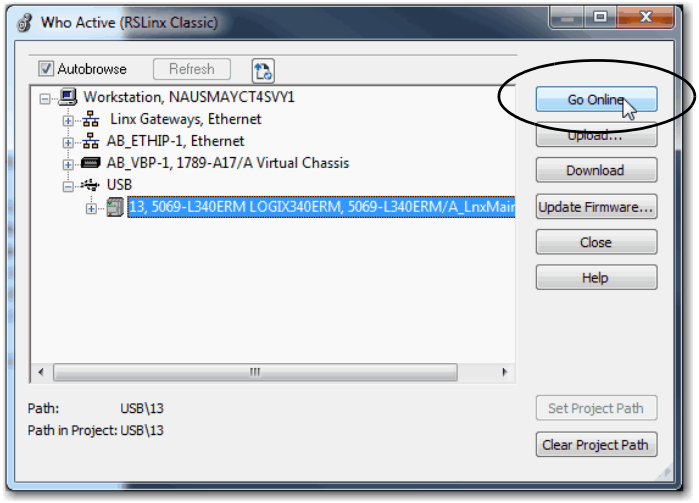
3. Expand the communication path and select the controller.



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

   If you store the project path in the project, 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.



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.

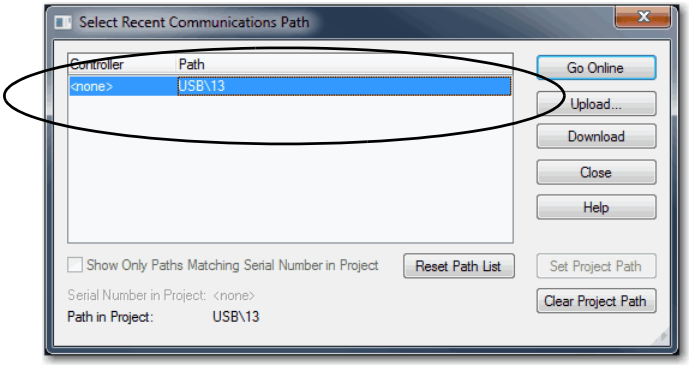
See Additional Considerations for Going Online with a Controller on page 98.

Use a Recent Communications Path

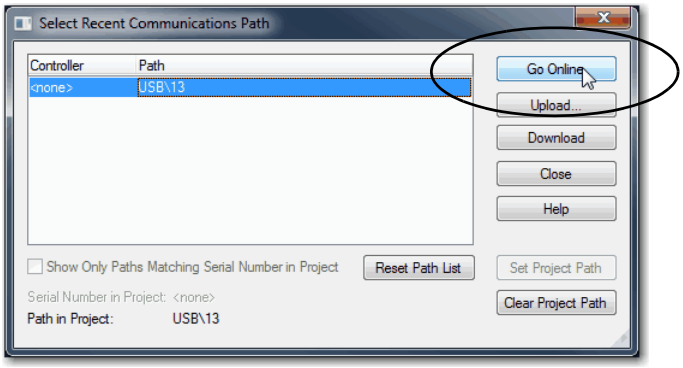
You can also select a recent communications path and go online or apply it to your project.

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

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

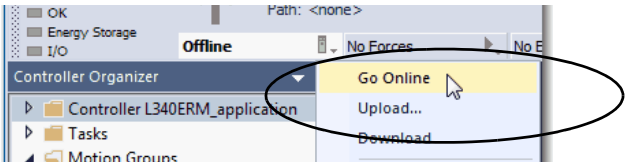


3. To store the path in your project, click Set Project Path.
4. Click Go Online.



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

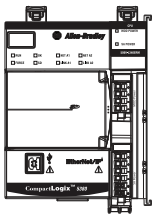
Once you have established a communication path, then you can choose Go Online from the Controller Status menu when you are working in the project.



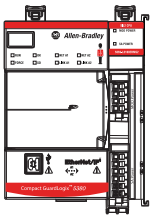
See Additional Considerations for Going Online with a Controller on page 98.

Additional Considerations for Going Online with a Controller

CompactLogix



Compact GuardLogix



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.

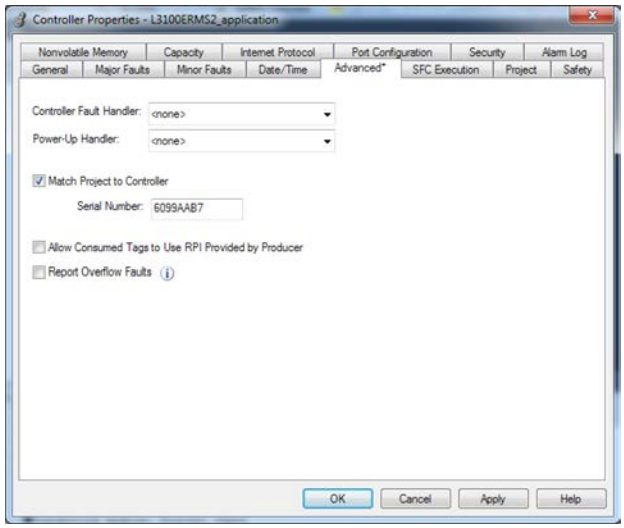
TIP For information on uploading a project, downloading a project, and the upload and download dialog boxes, see the Logix Designer Online Help.

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 100.

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 Controller Properties Advanced tab.



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

Firmware Revision Matching

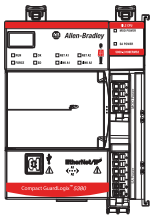
Firmware revision matching affects the download process. If the revision of the controller does not match the revision of the project, you are prompted to update the firmware of the controller. The Logix Designer application lets you update the firmware as part of the download sequence.

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

TIP 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

Compact GuardLogix



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 6 - 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 tags are reinitialized to the values they had when the safety signature was created. 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 and safety tags are reinitialized to the values they had when the safety signature was created. If the offline project is not safety-locked, but the controller is, the download is blocked and you must first unlock the controller to allow the download to proceed.
	Safety signatures do not match.	You must first safety-unlock the controller to allow the download to proceed. If the controller had a safety signature, it is automatically deleted, and the entire project is downloaded. Safety lock status matches the status in the offline project.

Checks for Going Online with a GuardLogix Controller

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

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

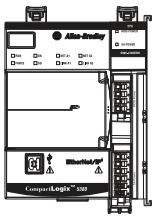
Table 7 - Connect to the Controller with a Safety Project

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.

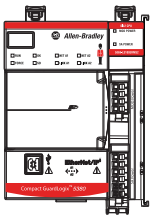
When the controller and the Logix Designer application are online, the safety-locked status and safety signature of the controller match the controller project. The safety-lock status and safety signature of the offline project are overwritten by the controller. If you do not want the changes to the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

Download to the Controller

CompactLogix



Compact GuardLogix



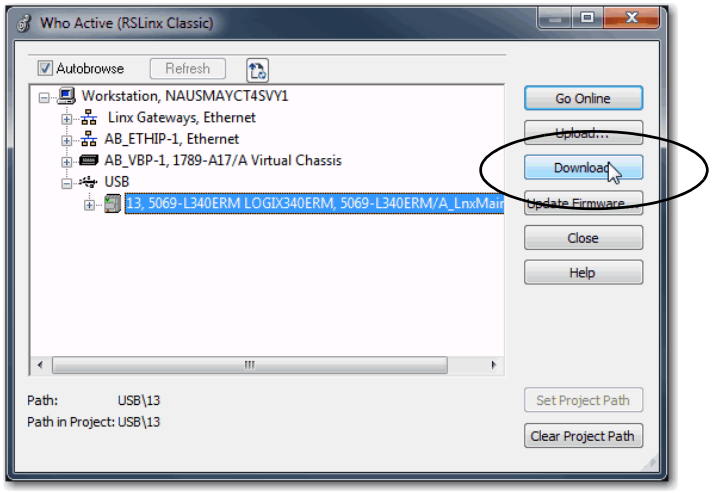
When you download a project to the controller, it copies the project from the Logix Designer application onto the controller. You can download a project in two ways:

- Use Who Active on page 102
- Use the Controller Status Menu on page 103

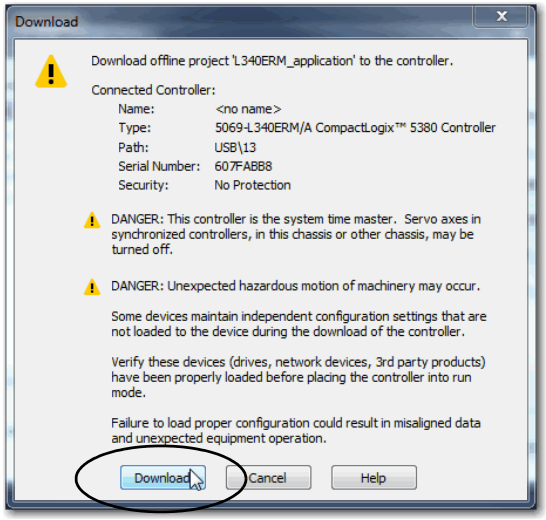
Use Who Active

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.



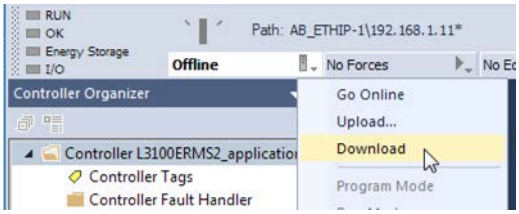
2. After reading the warnings in the Download dialog box, click Download.



Use the Controller Status Menu

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

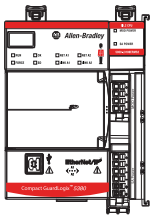
Figure 19 - Download Via the Controller Status Menu



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

Additional Considerations for Download to a Compact GuardLogix Controller

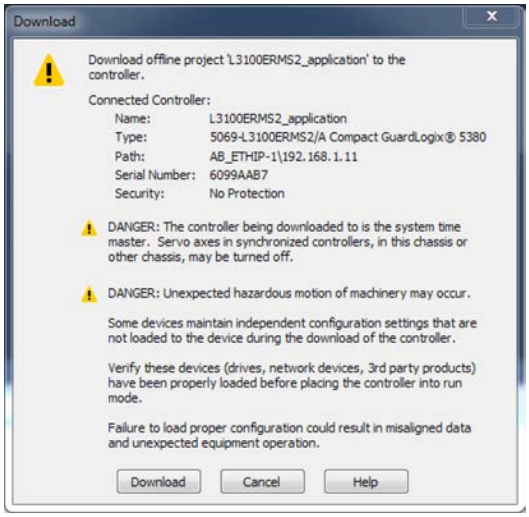
Compact GuardLogix



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.



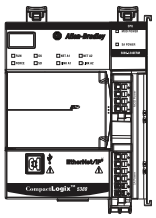
The Logix Designer application displays status messages in the download dialog, progress screen, and the Errors window.

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. 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.

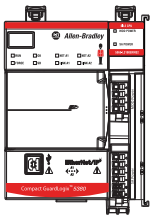
Following a successful download, the safety-locked status and safety signature of the controller match the project that was downloaded. Safety data is initialized to the values that existed when the safety signature was created.

Upload from the Controller

CompactLogix



Compact GuardLogix



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:

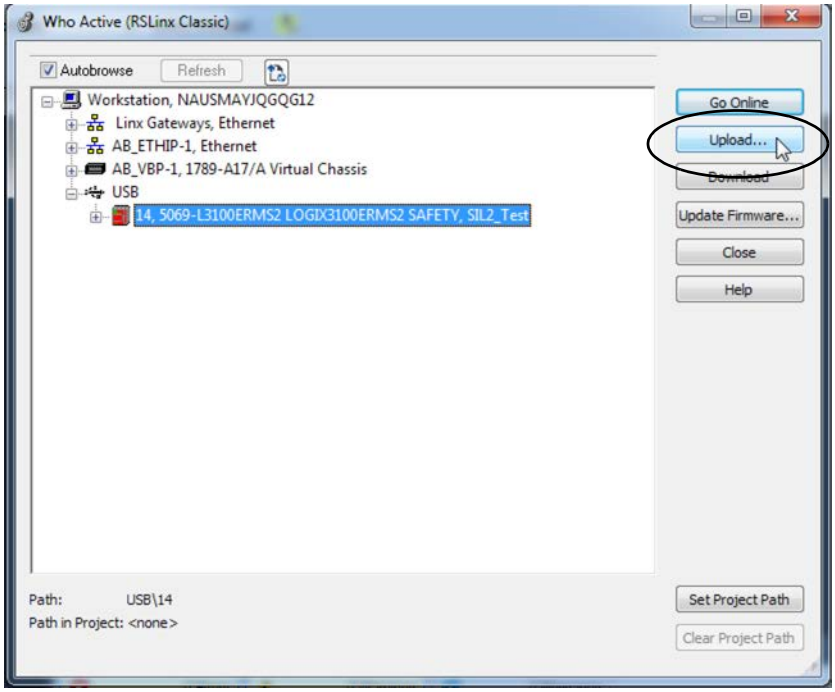
- Use Who Active on page 105
- Use the Controller Status Menu on page 106

Use Who Active

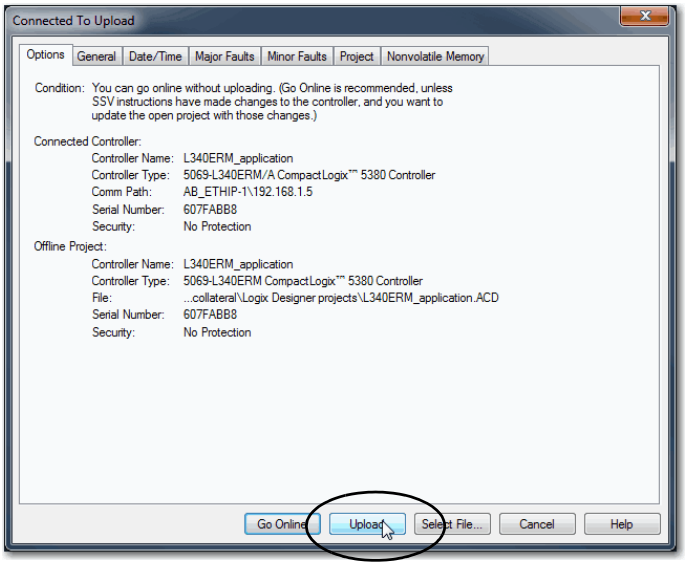
You can use the features of the Who Active dialog box to upload from your controller after you have set the communication path. Complete these steps to upload from the controller.

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.



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

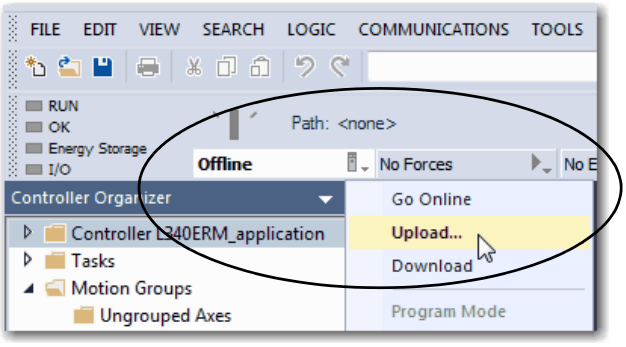


For more information on the Connected To upload dialog box, see the Logix Designer Online Help.

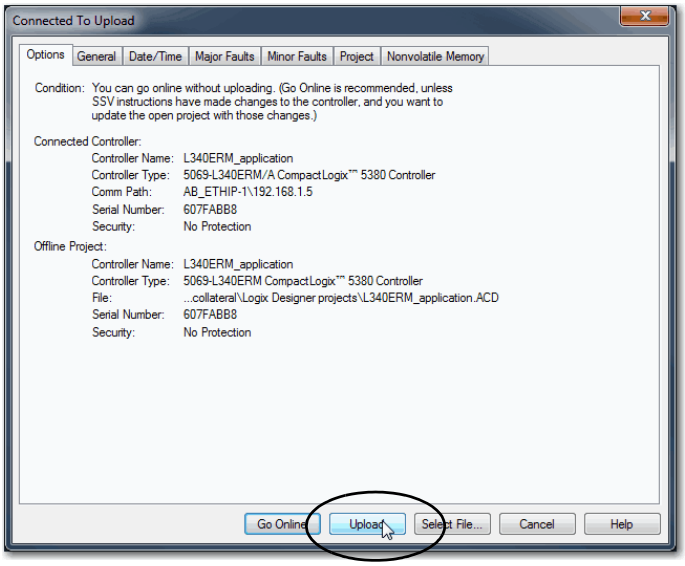
Use the Controller Status Menu

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

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

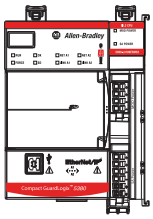


2. On the Connected to Upload dialog box, verify that the project is the one you want to upload.
3. Click Upload.



Additional Considerations for Upload to a Compact GuardLogix Controller

Compact GuardLogix



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 8 - 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.

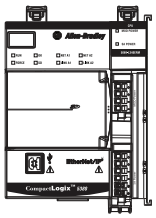
If you choose Upload, the standard and safety applications are uploaded. If a safety signature exists, it is also uploaded. The safety-lock status of the project reflects the original status of the online (controller) project.

TIP 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.

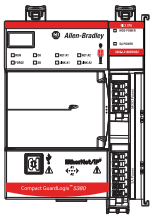
Choose the Controller Operation Mode

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

CompactLogix



Compact GuardLogix



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 109 for a list of prohibited features.

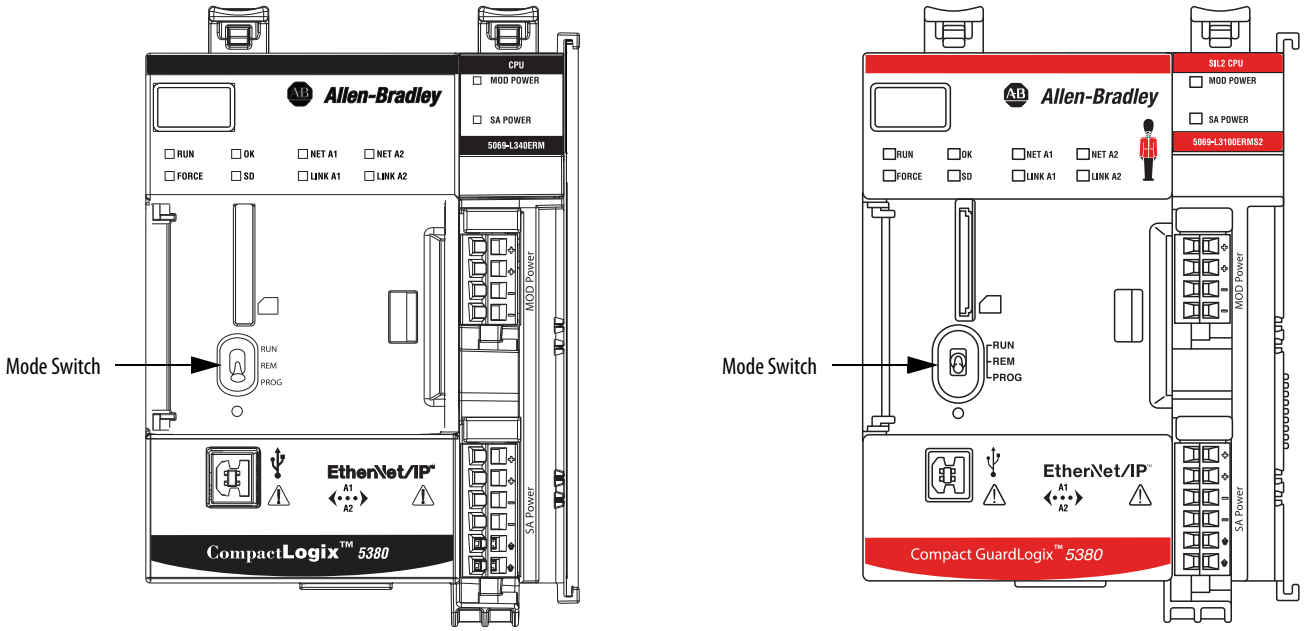
The mode switch can complement other authorization and authentication methods that similarly control user-access to the controller, such as the FactoryTalk® Security service.

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)



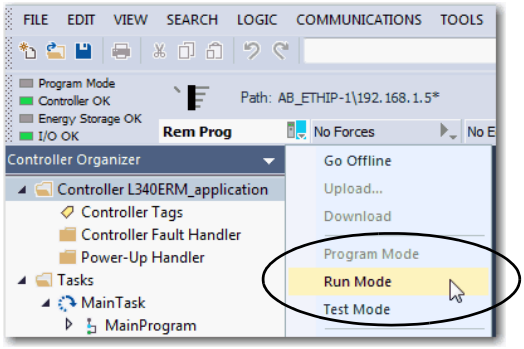
Use the Logix Designer Application to Change the Operation Mode

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

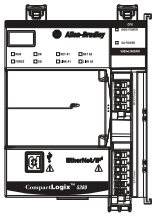
1. From the Controller Status pull-down menu, choose the operation mode.



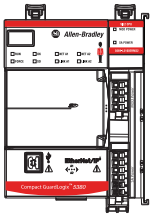
TIP For this example, the controller mode switch is set to Remote mode. If the controller mode switch is set to Run or Program modes, the menu options change.

Change Controller Configuration

CompactLogix



Compact GuardLogix



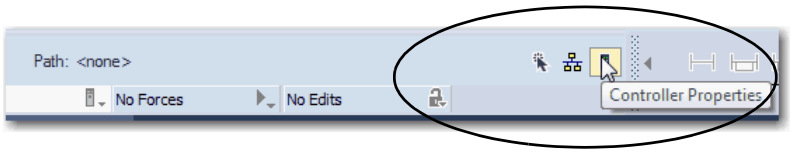
After the project is created, you can change some configuration parameters on the Controller Properties dialog box while the **controller is offline**.

Examples of configurable parameter that you can change offline include the following:

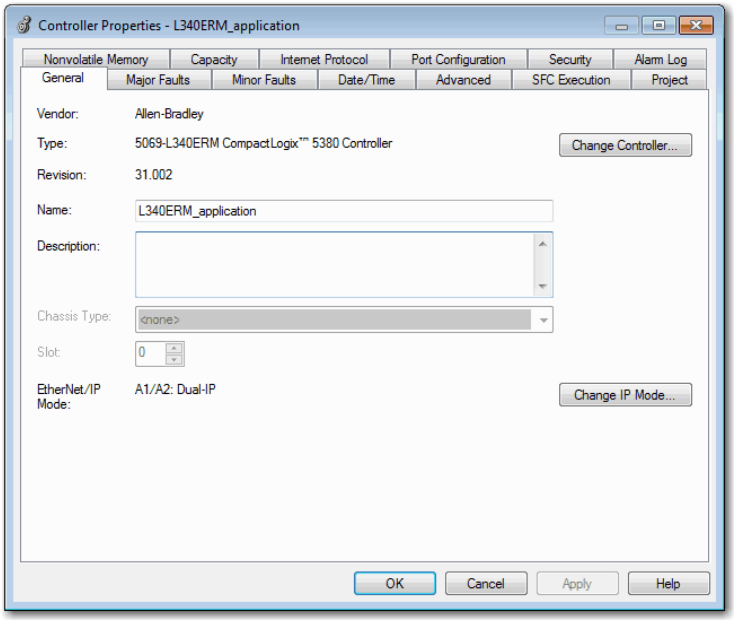
- EtherNet/IP Mode on the General tab
- Enable Time Synchronization on the Date/Time tab
- Execution Control on the SFC Execution tab

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.



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.

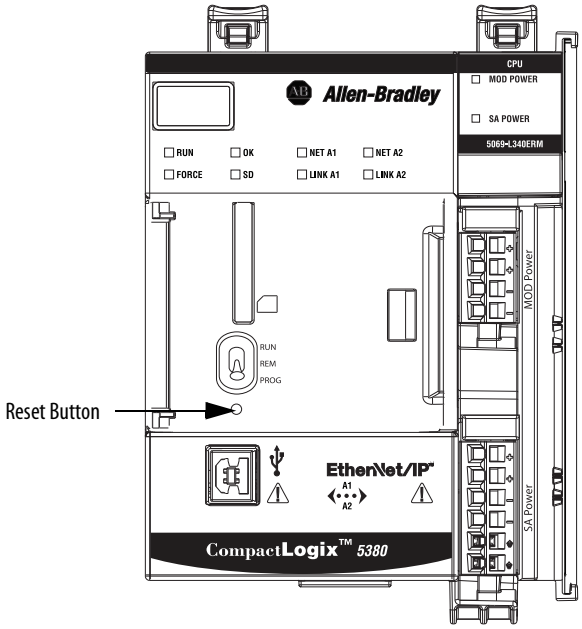
For a Compact GuardLogix controller, the Safety Locked status or safety signature does not prevent you from performing a controller reset. Because the application is cleared from the controller during a reset, the safety level of the controller is cleared also. When you download a safety project to the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

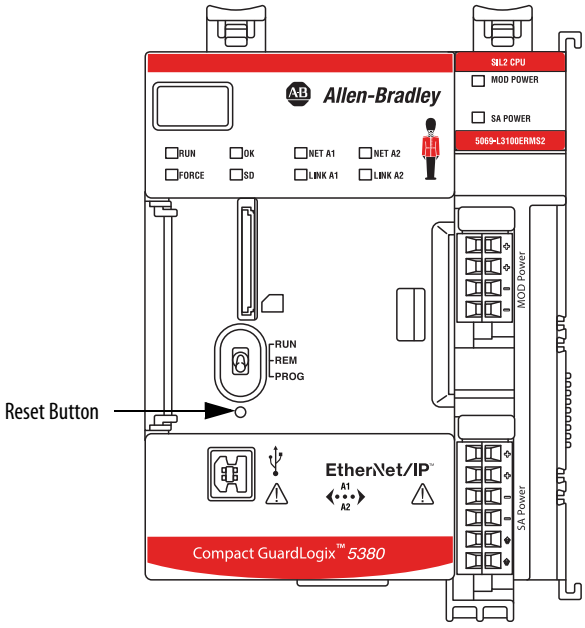
A controller has two stages of reset:

- 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 114.
- 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 115.

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.





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 102
- 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 Controller IP Address on page 65.

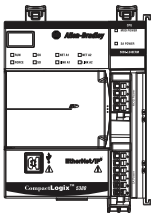
- Update the firmware revision - For more information, see Update Controller Firmware on page 75.

- 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 102.
  - Cycle power on the controller to load a project from the SD card.

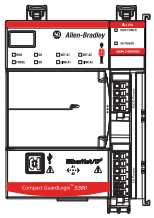
    This option works only if the project stored on the SD card is configured to load the project on powerup.

Use the Secure Digital Card

CompactLogix



Compact GuardLogix



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
- 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.

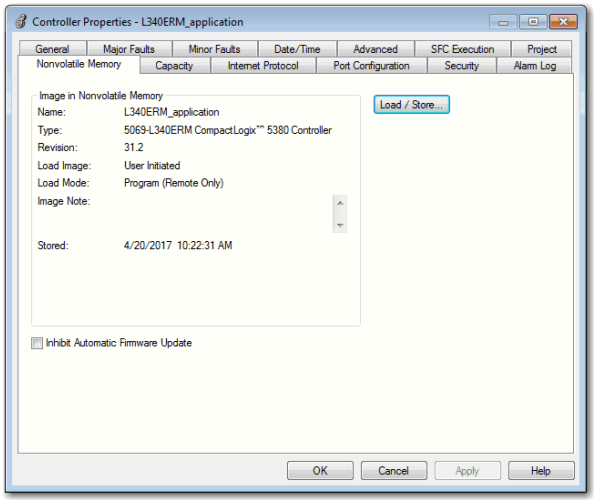
If you make changes to the project in the controller memory but do not store those changes, the next time that you load the project from the SD card to the controller, you overwrite the changes.

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

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

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

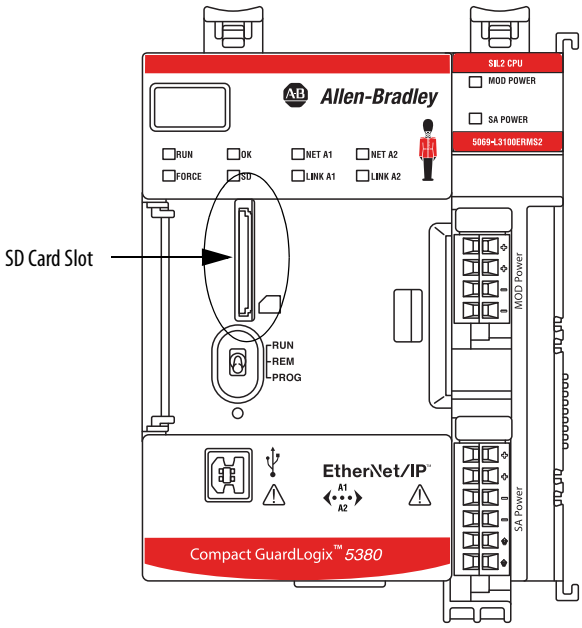
Figure 20 - Nonvolatile Memory Tab

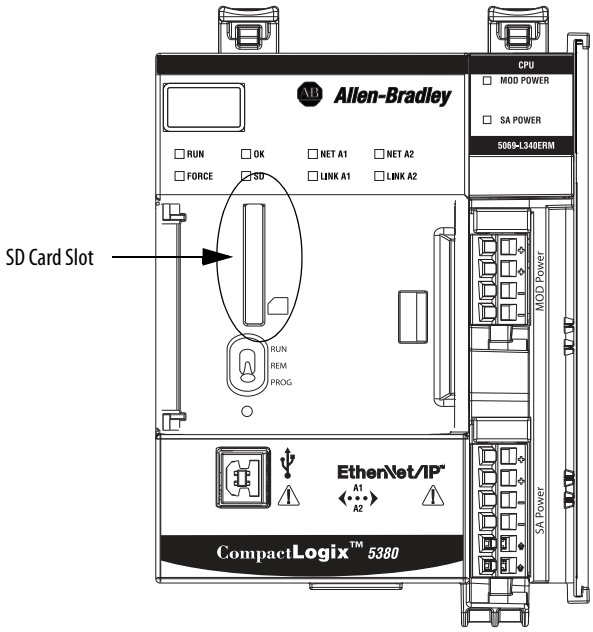


The project must be online to see the contents of the SD card.

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.

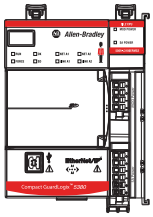
IMPORTANT Rockwell Automation recommends that you back up your Studio 5000 Logix Designer® program to an SD card regularly.

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

Compact GuardLogix



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.

If no application project exists in the controller, you can save only the firmware of the safety controller.

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

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

When you store a safety application project on an SD card, Rockwell Automation recommends 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.

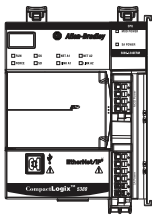
IMPORTANT To help prevent the firmware that is stored on the SD card from overwriting newly updated firmware:

- 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.

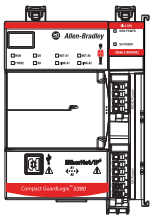
If the SD card is locked, the load option does not change, and the firmware that is stored on the SD card can overwrite the newly updated firmware.

Store to the SD Card

CompactLogix



Compact GuardLogix

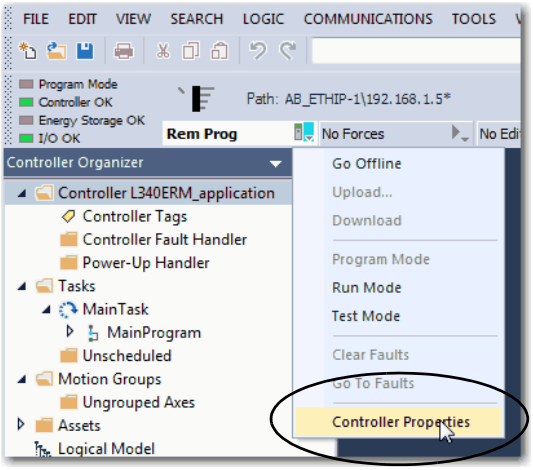


We recommend that you back up your Studio 5000 Logix Designer application to an SD card regularly.

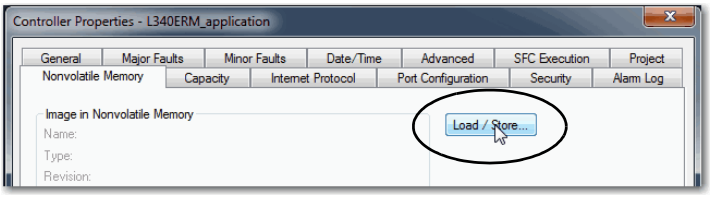
If a major non-recoverable fault occurs that removes the program from the controller memory, the backup copy on the SD card can be automatically restored to the controller to quickly resume normal controller operation.

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.

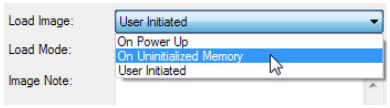


TIP If Load/Store is dimmed (unavailable), verify the following:

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

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

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



This table describes the Load Image options.

Table 9 - Load Image Options

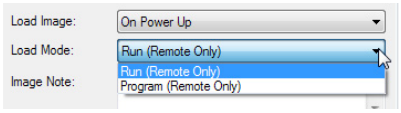
If You Want to Load the Project	Then Select This Load Image Option	Notes	Safety Considerations
Whenever you turn on or cycle power	On Power Up	• During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory. • The controller loads 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)	
Run	Run (remote only)	

IMPORTANT Safety Consideration

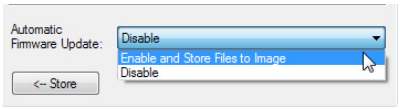
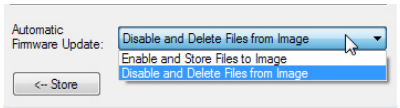
Rockwell Automation recommends that you use Program (Remote Only), when you set the Load Mode for a safety application project.

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

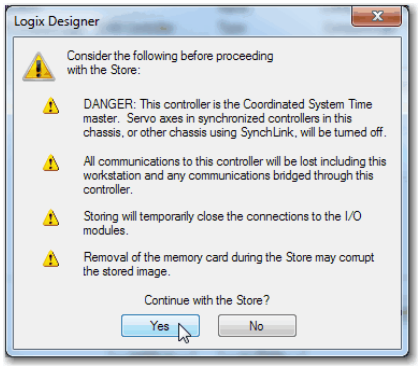
Some Safety I/O devices do not support the Firmware Supervisor feature. For example, Safety I/O devices on DeviceNet networks and POINT Guard I/O™ modules do not support the Firmware Supervisor feature.

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

Setting	Description	Menu Items
Disable	Disables any automatic firmware updates. This item only appears in the menu when you initially save the image.	
Enable and Store Files to Image	Enables automatic firmware updates for I/O devices in the configuration tree of the controller. Saves I/O device firmware and controller firmware to the image. Only I/O devices that are configured for Exact Match Keying participate in the Automatic Firmware Update process.(1)	
Disable and Delete Files from Image	Disables automatic firmware updates for I/O devices in the configuration tree of the controller. Removes I/O device firmware from the image, but does not remove controller firmware from image.This item only appears in the menu on subsequent saves of the image.	

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

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



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.

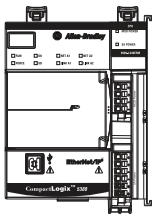
   The project is saved to the SD card as indicated by the controller status indicators.

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.

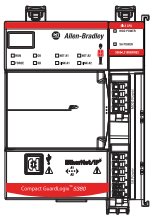
IMPORTANT Allow the store to complete without interruption. If you interrupt the store, data corruption or loss can occur.

Load from the SD Card

CompactLogix



Compact GuardLogix



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

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

Controller Power-up

This table shows what happens at power-up when 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(2)	Firmware > 1.*xxx* and Internal Nonvolatile Memory Is Valid(2)
User Initiated	Loads Firmware Only(1)	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(2)	• Loads Firmware if there is a revision mismatch • Loads Application	Does Nothing

(1) Indicates change in behavior from CompactLogix 5370 and older controllers.

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

User-initiated Action

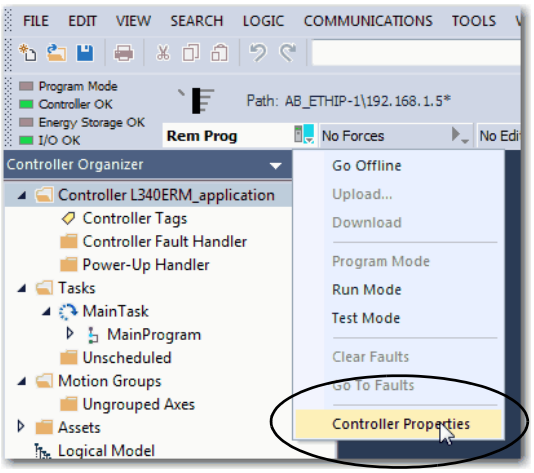
IMPORTANT For an out-of-box controller that uses firmware revision 1.xx, you must manually update the controller to the required firmware revision before you can load a project on the controller.

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

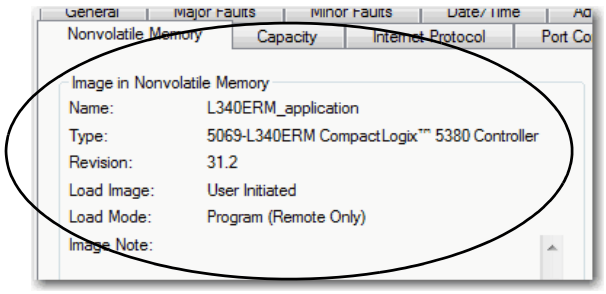
- Make sure that the controller has a working firmware revision.
- Establish the communication path.
- Go online with the controller.
- Make sure that the controller is in Program mode.

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

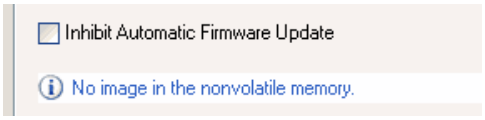
1. From the Controller Status pull-down menu, click Controller Properties.



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

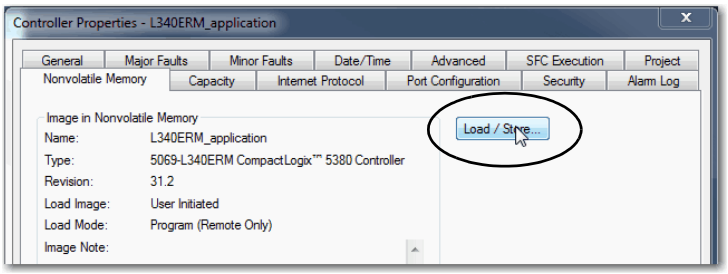


TIP If no project is stored on the SD card, a message on the Nonvolatile Memory tab indicates that an image (or project) is not available.



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

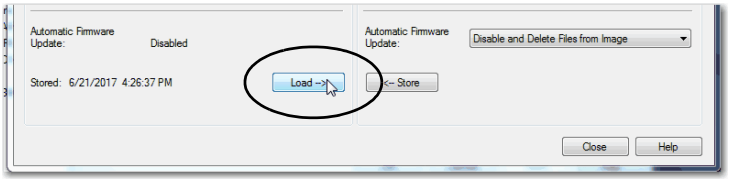
3. Click Load/Store.



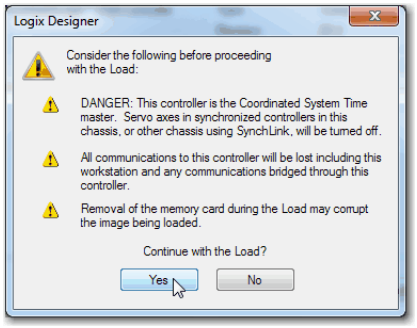
TIP If Load/Store is dimmed (unavailable), verify the following:

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

4. Click Load.



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



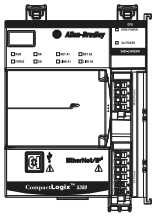
After you click Yes, the project is loaded to the controller as indicated by the controller status indicators.

These Indications Show the Load Status
While the **load is in progress**, the following occurs: • OK indicator is solid red • SD indicator is flashing green • Loading…Do Not Remove SD Card is shown on the status display • Updating Firmware…Do Not Remove SD Card can be shown on the status display if the firmware is also updating with the load • A dialog box in the Logix Designer application indicates that the store is in progress When the **load is complete**, the following occurs: • Controller reboots.

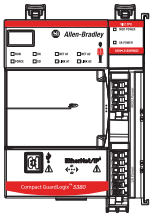
IMPORTANT Let the load to complete without interruption. If you interrupt the load, data corruption or loss can occur.

Other Secure Digital Card Tasks

CompactLogix



Compact GuardLogix



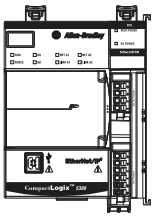
You can perform these tasks with the SD card:

- 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.

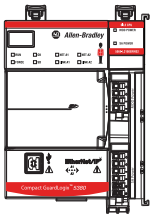
For more information to complete any of these tasks, see the Logix 5000 Controllers Memory Card Programming Manual, publication 1756-PM017.

EtherNet/IP Network

CompactLogix



Compact GuardLogix



CompactLogix™ 5380 and Compact GuardLogix® 5380 controllers operate on EtherNet/IP networks.

Remember, before your controller can operate on EtherNet/IP network, you must configure driver in RSLinx® Classic software. For more information on how to configure a driver, see page 57 and page 59.

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 135 use Compact GuardLogix 5380 controllers. You can use CompactLogix 5380 controllers in the same examples.

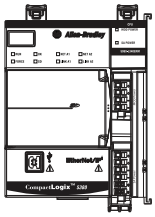
The EtherNet/IP network offers a full suite of control, configuration, and data collection services by layering the Common Industrial Protocol (CIP) over the standard Internet protocols, such as TCP/IP and UDP. This combination of well-accepted standards provides the capability that is required to support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

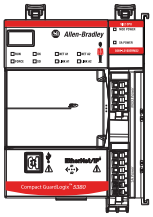
For more information on socket interface transactions, see Socket Interface on page 139.

EtherNet/IP Network Functionality

CompactLogix



Compact GuardLogix



The CompactLogix 5380 and Compact GuardLogix 5380 controllers support the following EtherNet/IP network functionality:

- Dual built-in EtherNet/IP network ports - Port A1 and port A2
- Support for these EtherNet/IP modes:
  - Dual-IP mode - Available with the Studio 5000 Logix Designer® application, version 29.00.00 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.

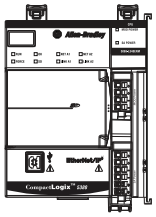
- Support for CIP Sync technology that is based on Time Synchronization using the IEEE-1588 Precision Time Protocol
- Duplicate IP address detection
- Socket interface to communicate with Ethernet devices that do not support the EtherNet/IP application protocol
- Compatible with industry-standard Ethernet switches - Managed switches are recommended, and CIP-protocol-aware switches can provide more predictable performance.
- CIP Safety over an EtherNet/IP network - Compact GuardLogix 5380 controllers only
- Support for messaging, produced/consumed tags, HMI, and distributed I/O modules
- Support for Integrated Motion Over an EtherNet/IP network - Not available on all CompactLogix 5380 or Compact GuardLogix 5380 controllers

  For more information on using Integrated Motion over an EtherNet/IP network, see Chapter 15, Develop Motion Applications on page 277.

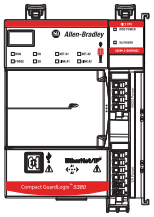
For more information about network design, see the Ethernet Design Considerations Reference Manual, publication ENET-RM002.

Software for EtherNet/IP Networks

CompactLogix



Compact GuardLogix



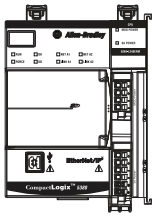
[Table 10](#) lists software that is used with the EtherNet/IP networks and modules.

Table 10 - Software for Use with EtherNet/IP Networks

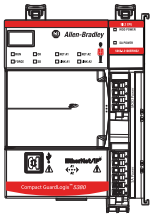
Software	Use	Required or Optional
Logix Designer application	• Configure CompactLogix projects. • Define EtherNet/IP communication.	Required
RSLinx® Classic or RSLinx Enterprise	• Configure communication devices. • Provide diagnostics. • Establish communication between devices.	Required
BOOTP DHCP EtherNet/IP Commissioning tool	Assign IP addresses to the controller and devices on an EtherNet/IP network.	Optional

Nodes on an EtherNet/IP Network

CompactLogix



Compact GuardLogix



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 11](#) shows the maximum number of EtherNet/IP nodes that the controllers support.

Table 11 - CompactLogix 5380 and Compact GuardLogix 5380 Controller EtherNet/IP Nodes

CompactLogix 5380 Controllers	Nodes Supported, Max
5069-L306ER, 5069-L306ERM	16
5069-L310ER, 5069-L310ER-NSE, 5069-L310ERM	24
5069-L320ER, 5069-L320ERM	40
5069-L330ER, 5069-L330ERM	50, 60(1)
5069-L340ER, 5069-L340ERM	55, 90(1)
5069-L350ERM	60, 120(1)
5069-L380ERM	70,150(1)
5069-L3100ERM	80, 180(1)
Compact GuardLogix 5380 Controllers	**Nodes Supported, Max**
5069-L306ERMS2, 5069-L306ERS2	16
5069-L310ERS2, 5069-L310ERMS2	24
L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	40
5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2, 5069-L330ERMS2K	60
5069-L340ERS2, 5069-L340ERMS2	90
5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2, 5069-L350ERMS2K	120
5069-L380ERS2, 5069-L380ERMS2	150
5069-L3100ERS2, 5069-L3100ERMS2	180

(1) With Studio 5000 Logix Designer Application Version 31 or later.

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

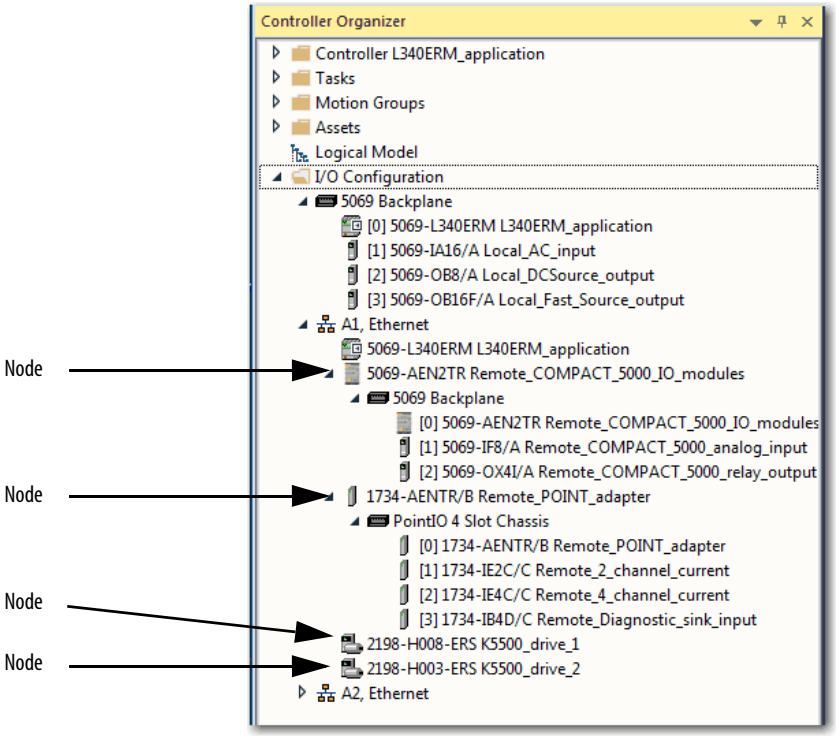
When you calculate the EtherNet/IP node limitation of a controller, do not count devices that exist on the EtherNet/IP network but are not added to the I/O configuration section.

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

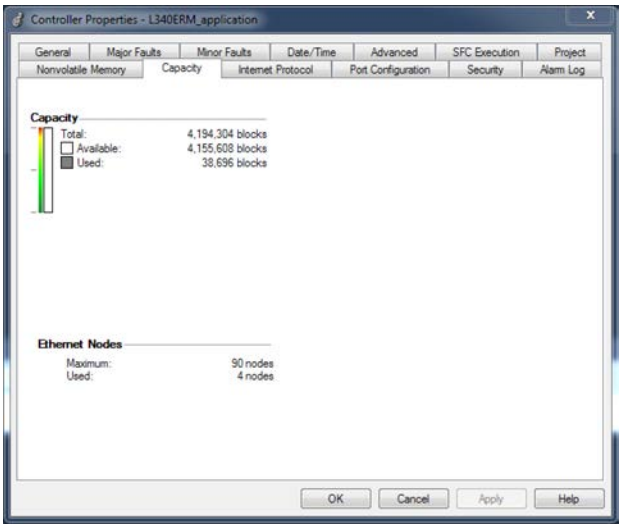
- Computer
- HMIs that are not added to the I/O configuration section
- Devices that are the target of MSG Instructions but were not added to the I/O configuration section
- Standard Ethernet devices with which the controller communicates via a socket interface

Figure 21 shows nodes in the I/O tree.

Figure 21 - Example EtherNet/IP Nodes

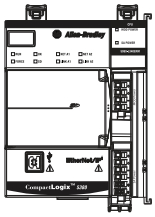


The Capacity tab in the Controller Properties dialog box displays the number of Ethernet nodes that are used in a project. The following graphic is representative of the project shown in Figure 21.

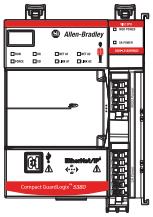


EtherNet/IP Network Topologies

CompactLogix



Compact GuardLogix



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

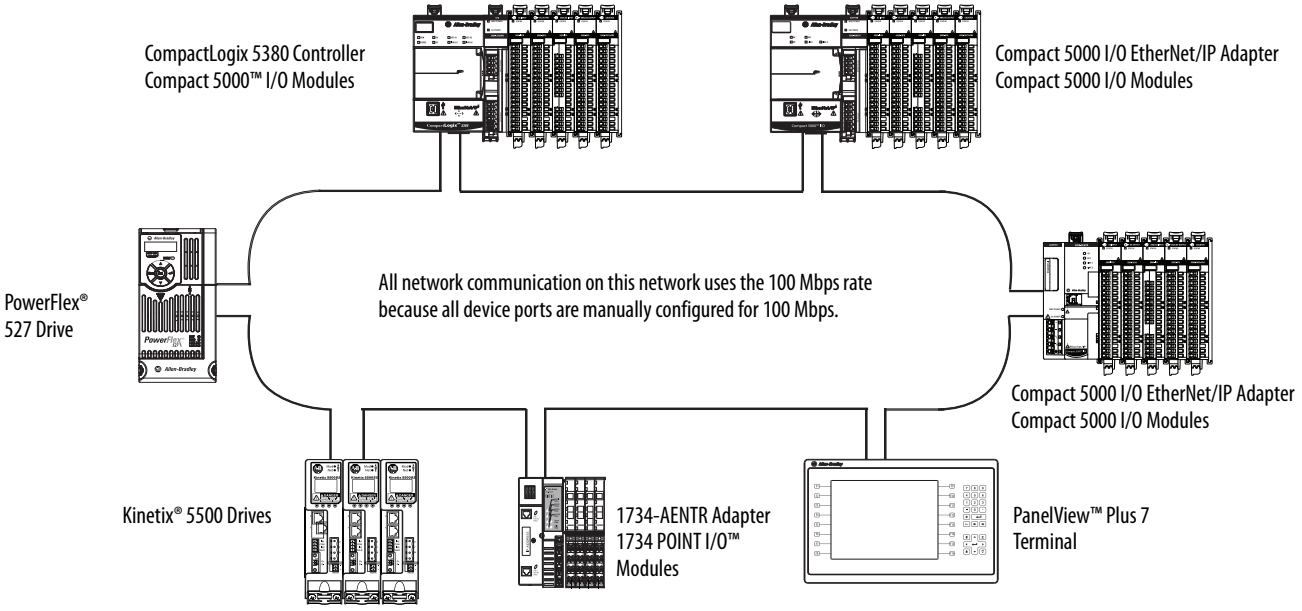
A DLR network topology is a single-fault tolerant ring network that is intended for the interconnection of automation devices. A DLR network uses Supervisor (Active and Backup) nodes and Ring nodes.

DLR network topologies automatically convert to linear network topologies when a fault is detected. The conversion to the new network topology maintains communication of data on the network. The fault condition is typically easily detected and corrected.

The 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.

IMPORTANT If you use a controller in a DLR network with at least one device that has a maximum network communication rate of 100 Mbps, set the controller ports to 100 Mbps. If there are other devices in the ring that support 1 Gbps, you should still set all devices in the ring to 100 Mbps to help provide more reliable communication.

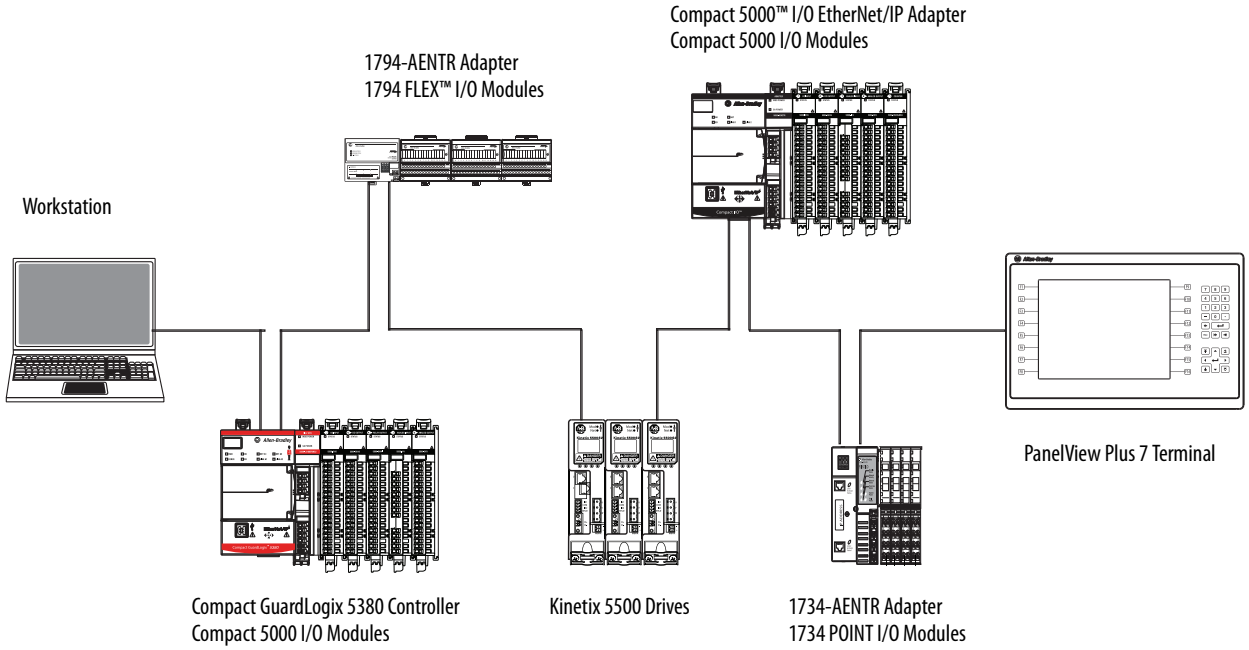
Figure 22 - CompactLogix 5380 Controller in a DLR Network Topology



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 23 - Compact GuardLogix 5380 Controller in a Linear Network Topology



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

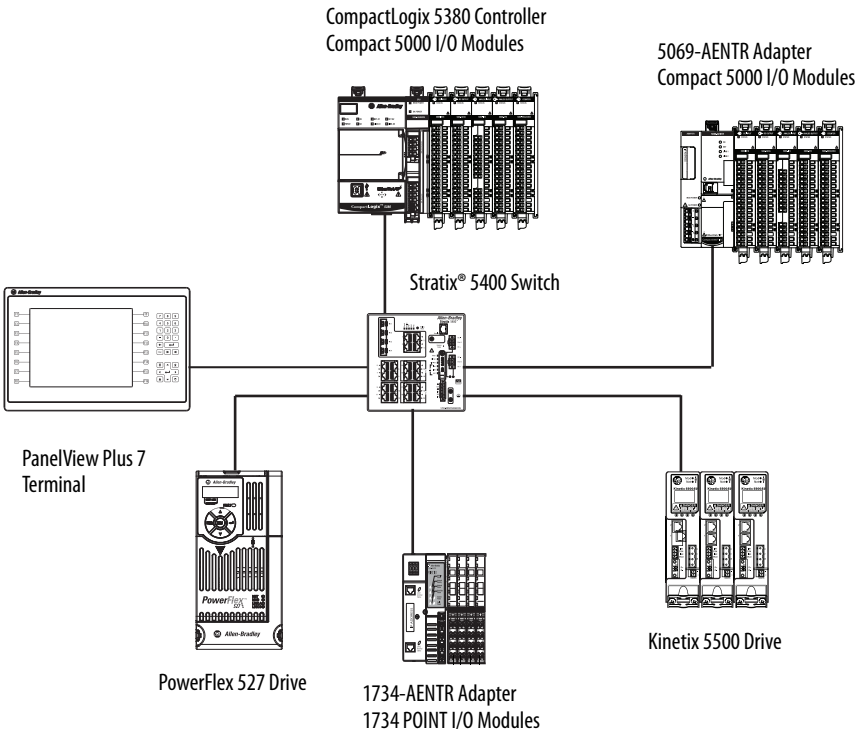
Star Network Topology

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 Chapter 9, Use EtherNet/IP Modes on page 141.

Figure 24 - CompactLogix 5380 Controllers in a Star Network Topology



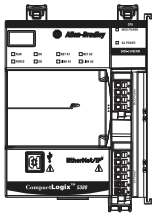
Integrated Architecture Tools

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.

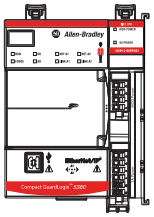
The tool and resources are available at: http://www.rockwellautomation.com/global/products-technologies/integrated-architecture/tools/overview.page

EtherNet/IP Network Communication Rates

CompactLogix



Compact GuardLogix



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

- 10 Mbps
- 100 Mbps
- 1 Gbps

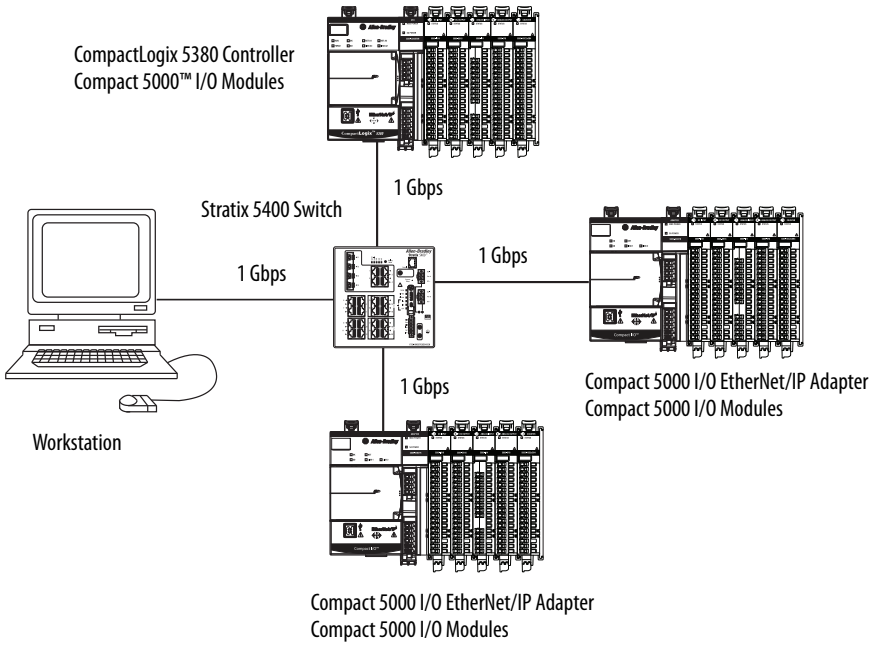
Network performance in a CompactLogix 5380 system is optimal if the 1 Gbps network communication rate is used. However, many Ethernet devices do not support the 1 Gbps network communication rate. Instead, they support a maximum rate of 100 Mbps.

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:

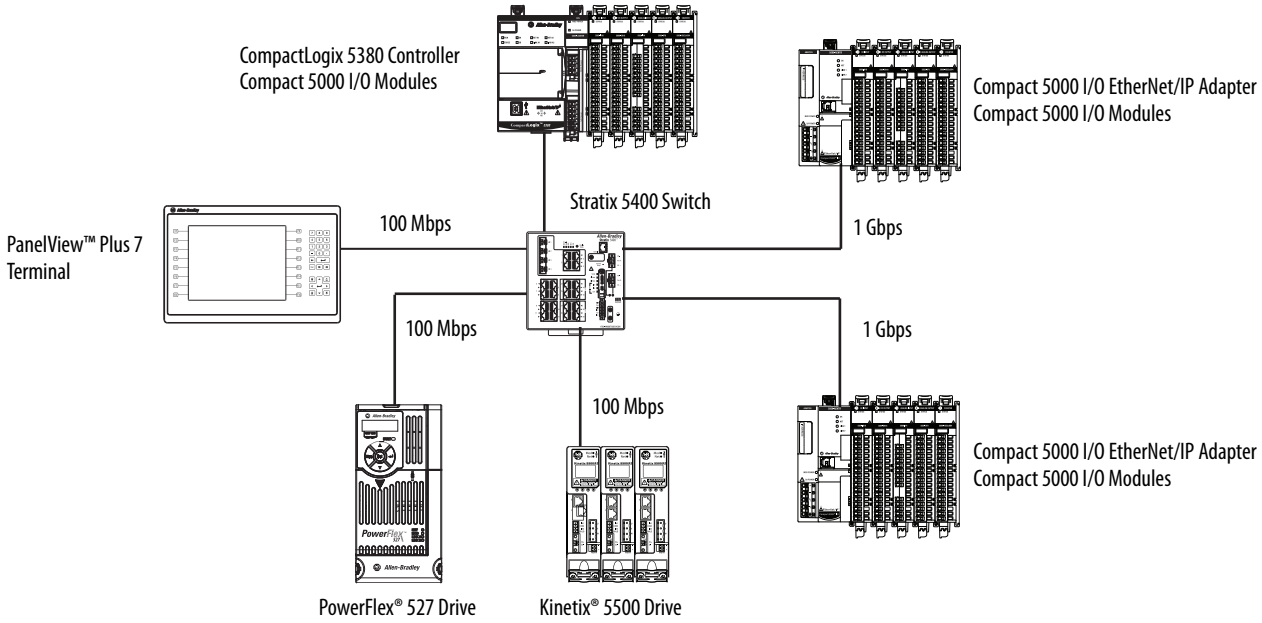
- You can use the 1 Gbps network communication rate on the controller ports when all network devices support the 1 Gbps, for example, 5069-AEN2TR adapters with Compact 5000 I/O modules and a gigabit-capable switch.

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



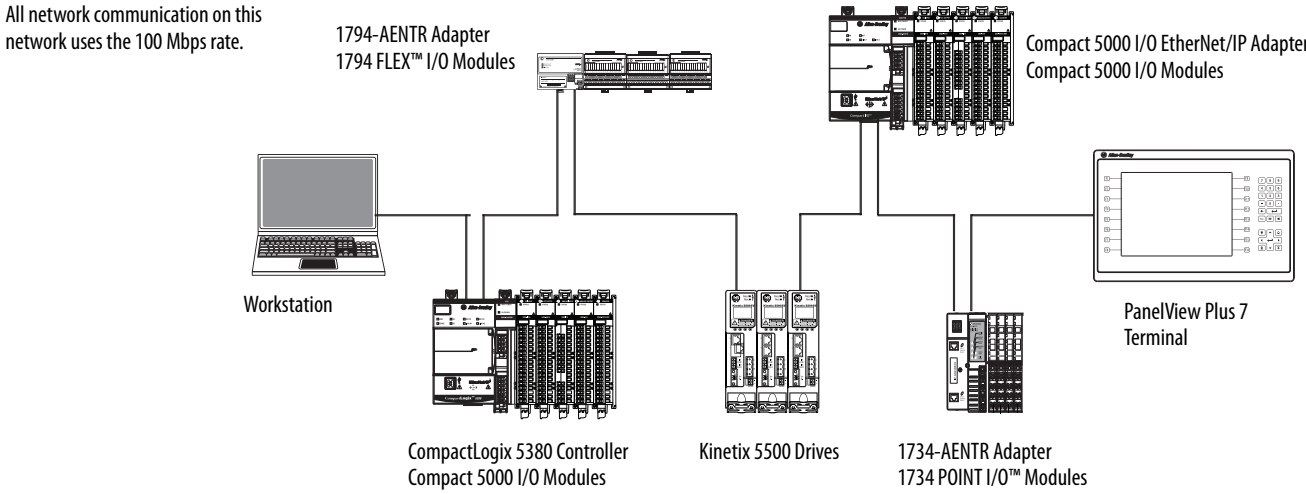
- You can use the 1 Gbps network communication rate on the controller ports when some network devices support a maximum network communication rate of 100 Mbps. However, in this case, the controller **must be connected** to those devices through a **managed switch**.

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



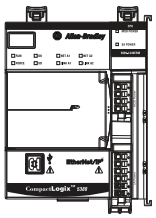
We recommend that you do not use the 1 Gbps network communication rate on the controller ports if it operates on a linear or DLR network topology and at least one device on the network supports the maximum network communication rate of 100 Mbps.

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

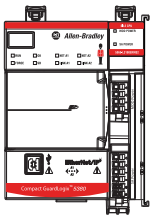


Socket Interface

CompactLogix

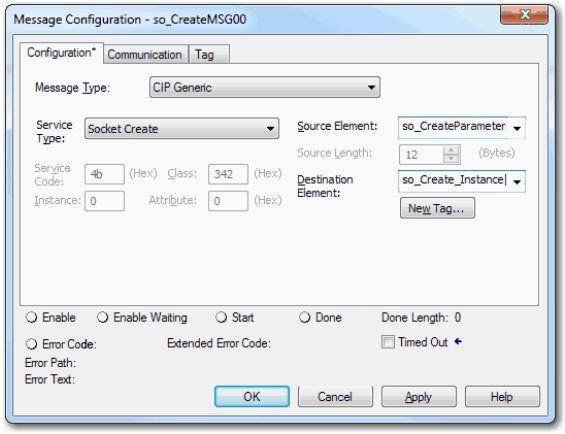


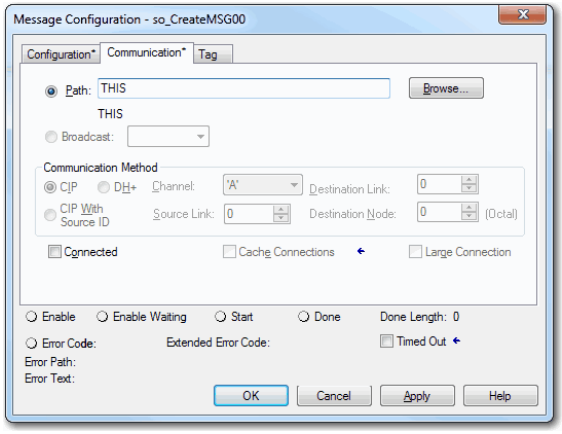
Compact GuardLogix



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.

You must use MSG instructions that configure and operate the socket interface as Unconnected, and use the Message to Self path. To communicate with another device, you must understand the application protocol of the other device. The following are example screens of a MSG instruction that is used with a socket interface.





The controllers support up to 32 socket instances.

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

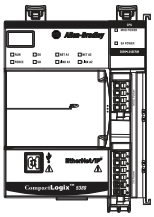
- A significant difference between CompactLogix 5380 or Compact GuardLogix 5380 controllers and other Logix 5000™ controllers is the communication path. CompactLogix 5380 controllers do not require a separate EtherNet/IP network communication module, for example, a 1756-EN2TR communication module. For the CompactLogix 5380 and Compact GuardLogix 5380 controllers, the MSG instruction is sent to the controller itself by using the path 'THIS'.
- 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 165.

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

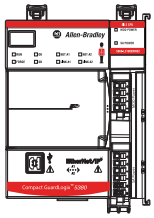
Notes:

Use EtherNet/IP Modes

CompactLogix



Compact GuardLogix



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

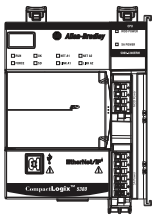
- Dual-IP
- Linear/DLR

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.

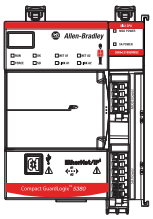
Other chapters in this publication describe how to perform more general tasks in the Studio 5000 Logix Designer® application and RSLinx® Classic software. If necessary, read those chapters to understand better the tasks that are described in this chapter.

Available Network Levels

CompactLogix



Compact GuardLogix



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 149.

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:

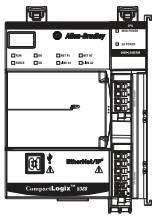
- You are not required to connect the controller to an enterprise-level network to connect to device-level networks.
- You can connect port A1, port A2, or ports A1 and A2 to device-level networks.

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

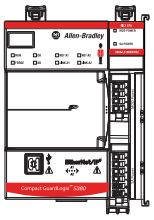
- IP address (Required)
- Subnet mask, also called the network mask (Required)
- Gateway address (Optional)
- Host name (Optional)

EtherNet/IP Modes

CompactLogix



Compact GuardLogix



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 the EtherNet/IP Modes on page 150.

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 149.

Figure 25 shows a CompactLogix 5380 controller using Dual-IP mode in with connections to an enterprise-level network and a device-level network.

Figure 25 - CompactLogix 5380 Controller in Dual-IP Mode with Enterprise-level and Device-level Network Connections

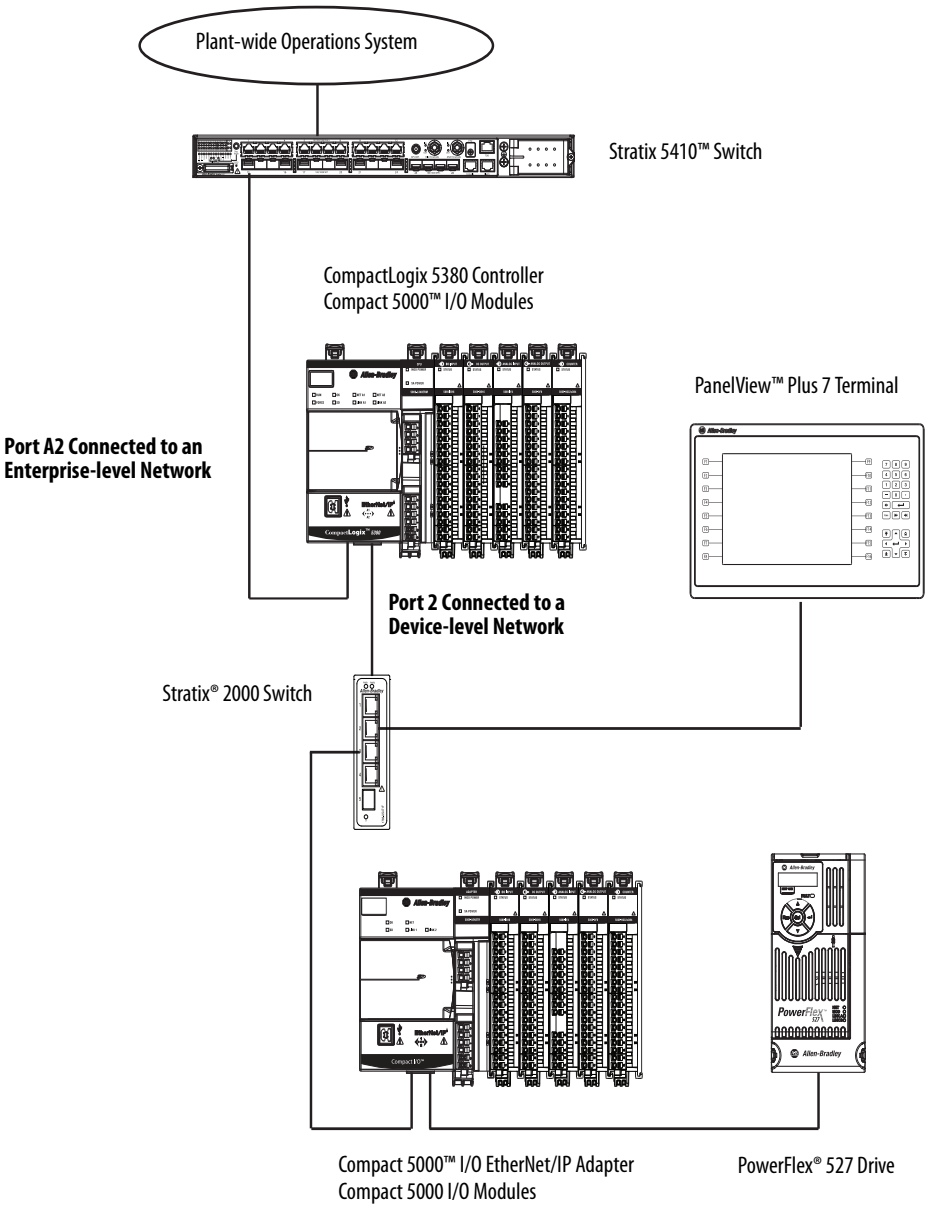
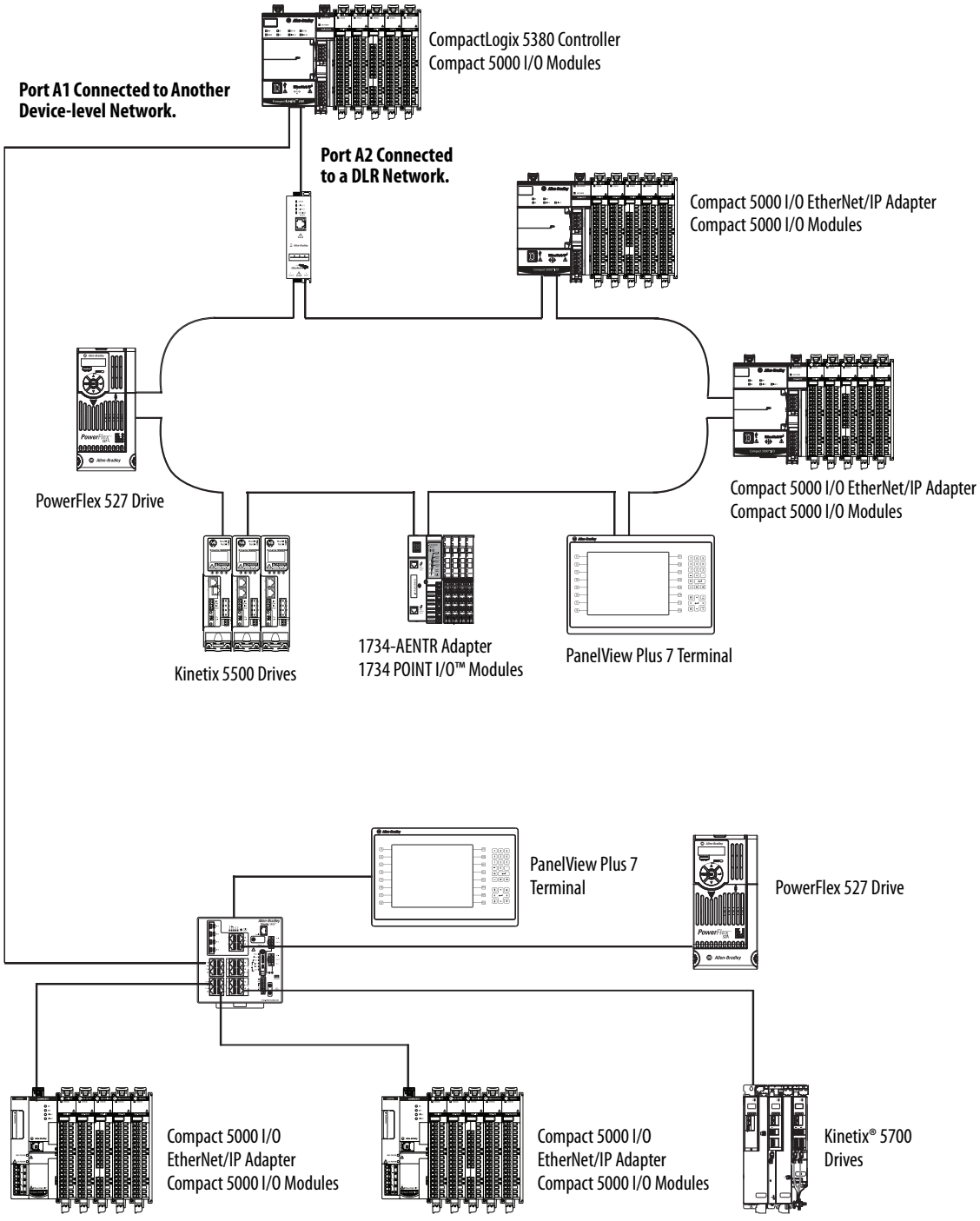


Figure 26 shows a CompactLogix 5380 controller using Dual-IP mode in with connections to separate device-level networks, including a DLR network.

Figure 26 - CompactLogix 5380 Controller in Dual-IP Mode with Device-level Network Connections Only

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.



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. That is, there is only one network configuration. The two physical ports allow the controller to connect to linear or DLR media topologies if desired.

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 158.

Figure 27 - CompactLogix 5380 Controller in Linear/DLR Mode in a DLR Network

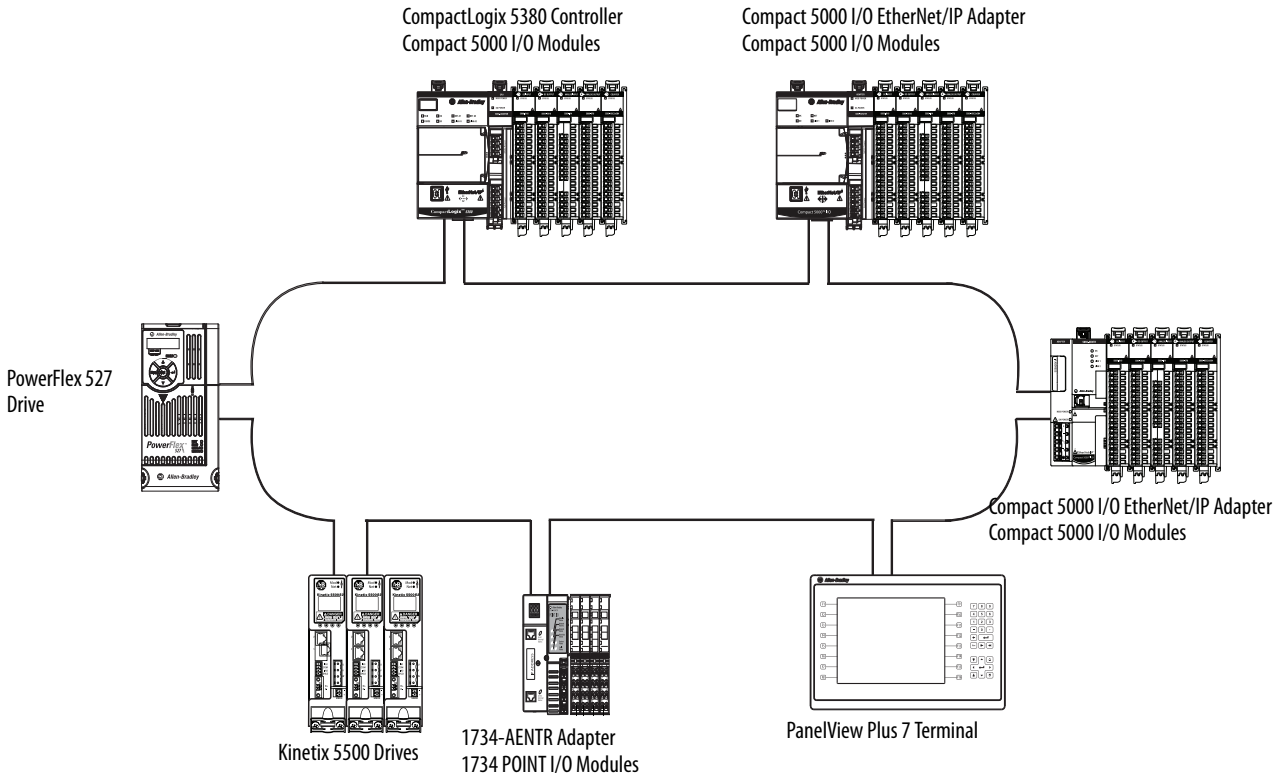


Figure 28 - Compact GuardLogix 5380 Controller in Linear/DLR Mode in a Linear Network

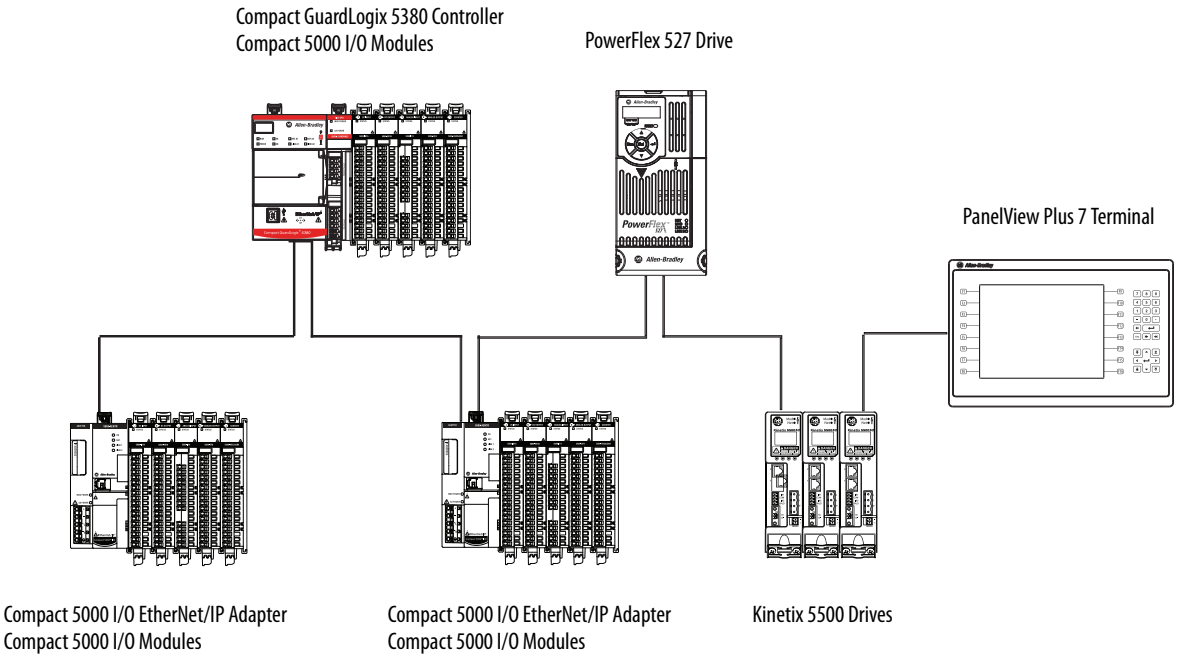
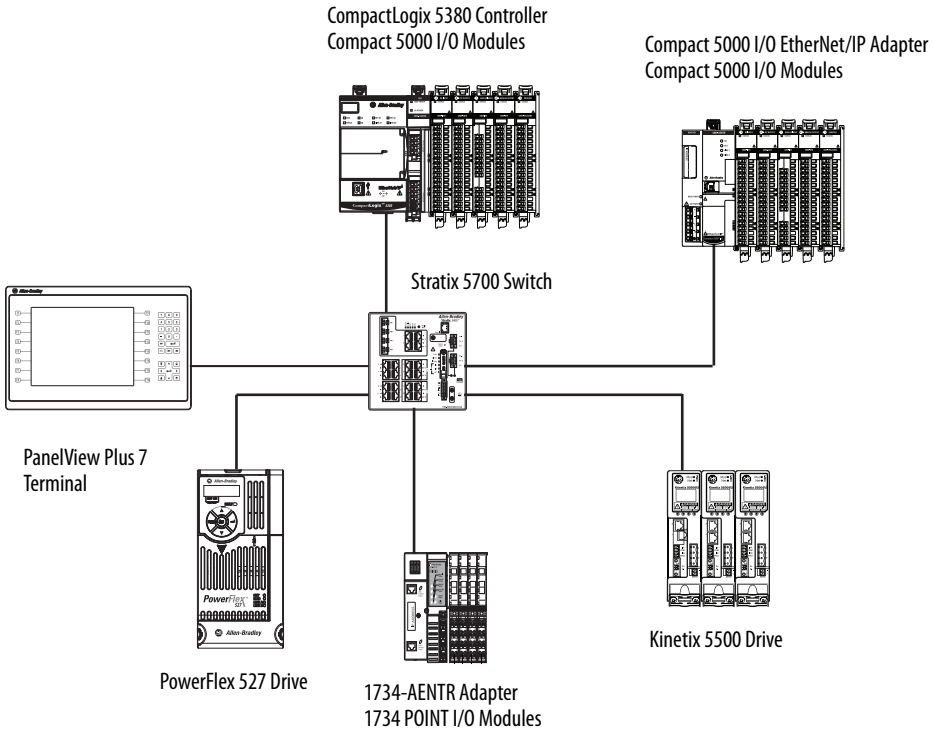
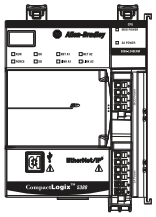


Figure 29 - CompactLogix 5380 Controller in Linear/DLR Mode in a Star Network

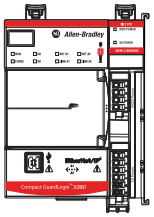


Overlapping IP Address Ranges

CompactLogix



Compact GuardLogix



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 147.

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.

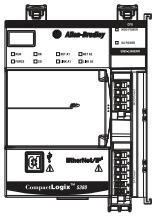
Port Number	IP Address	Subnet Mask/ Network Mask	IP Address Range (Low to High)
A1	192.168.1.5	255.255.252.0	192.168.0.1…192.168.3.254
A2	192.168.2.1	255.255.255.0	192.168.2.1…192.168.2.254

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

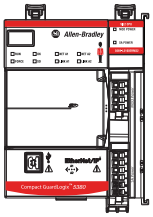
In the first example, the value is 255.255.255.0. In the second example, the value 255.255.252.0.

Configure the EtherNet/IP Modes

CompactLogix



Compact GuardLogix



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

- Logix Designer application, version 29.00.00 or later
- RSLinx® Classic software, version 3.81.00 or later
- With the Logix Designer application, version 28.00.00, the 5069-L320ER and 5069-L340ERM controllers only support Linear/DLR mode.

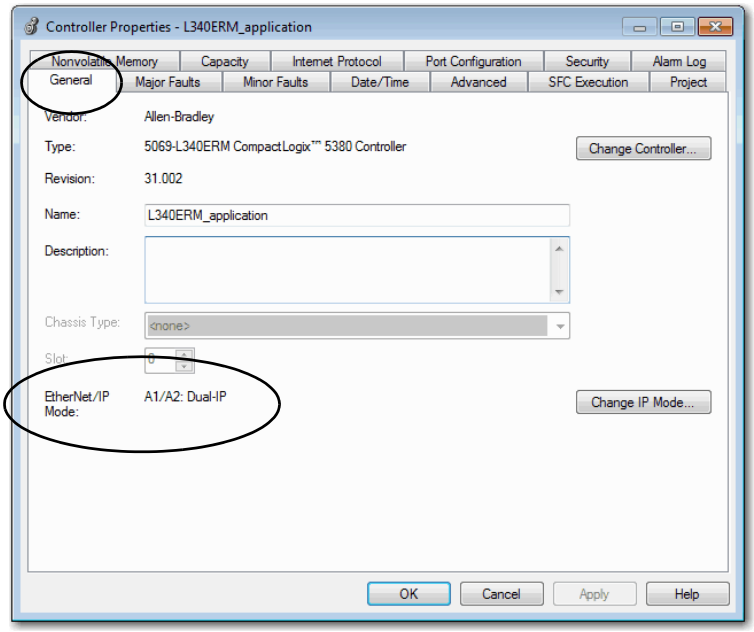
IMPORTANT Keep in mind that the applicable minimum software versions vary by controller catalog number. That is, you can use some controllers in lower software minimum versions than others.

For more information how to determine what the minimum software version requirements are for your controller, see Controller Firmware and Logix Designer Application Compatibility on page 16.

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 29.00.00 or later, the EtherNet/IP Mode is Dual-IP by default and is displayed on the General tab in the Controller Properties dialog box.

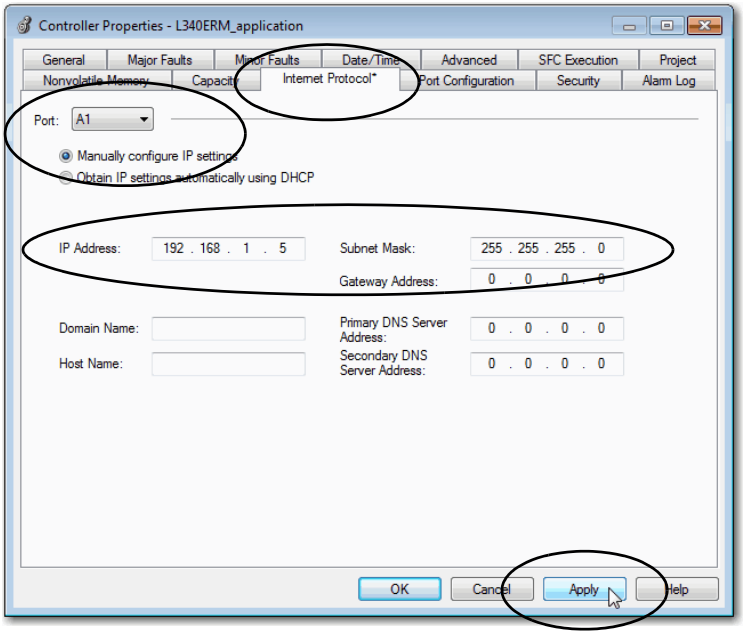


You set the IP address and Subnet Mask on the Internet Protocol tab.

TIP 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 IP Address and Network Mask values.
7. Click Apply.



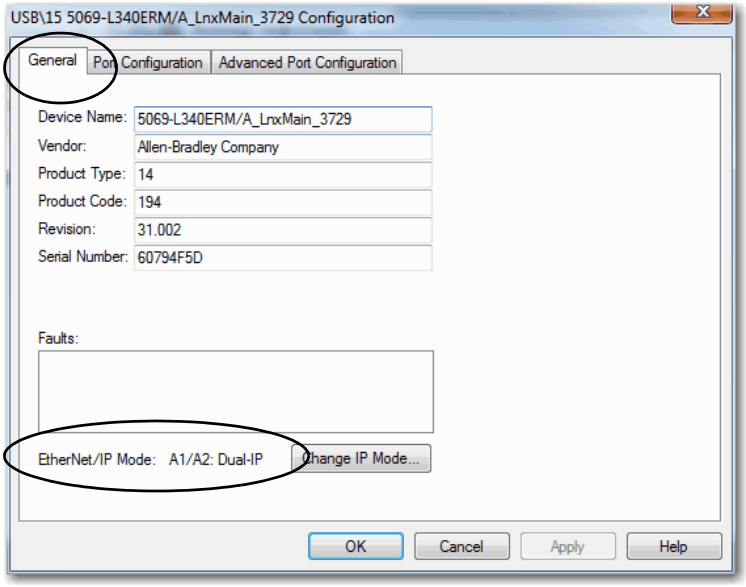
8. Repeat the previous steps, beginning at step 4

   In step 4, make sure that you choose A2 from the Port pull-down menu.

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.

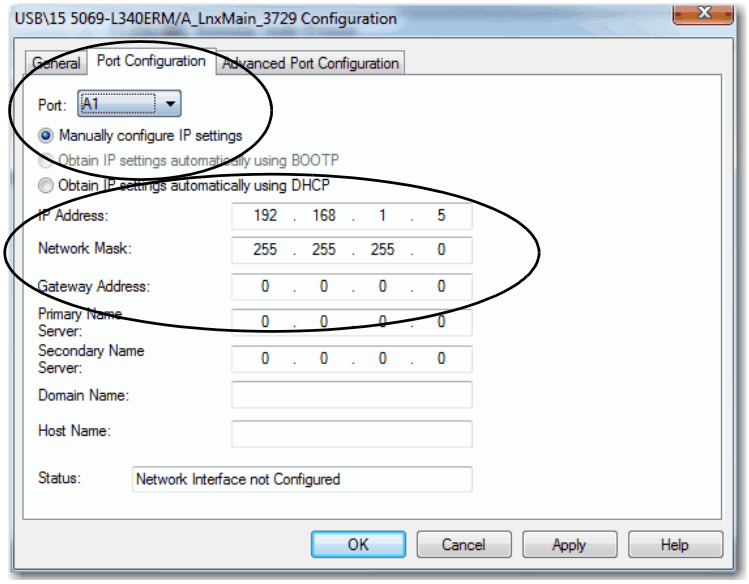
For example, this graphic displays that the controller is in Dual-IP mode.



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

TIP 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.



5. Repeat the steps.

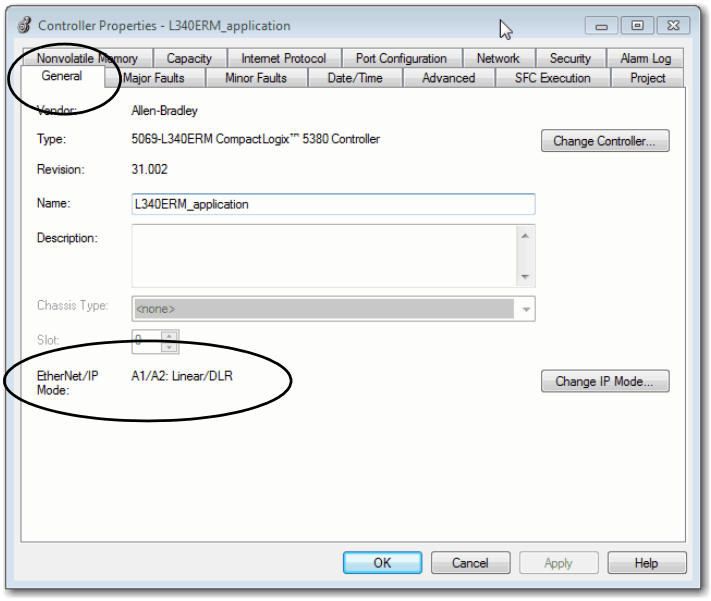
   In step 1, make sure that you choose A2 from the Port pull-down menu.

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 158.

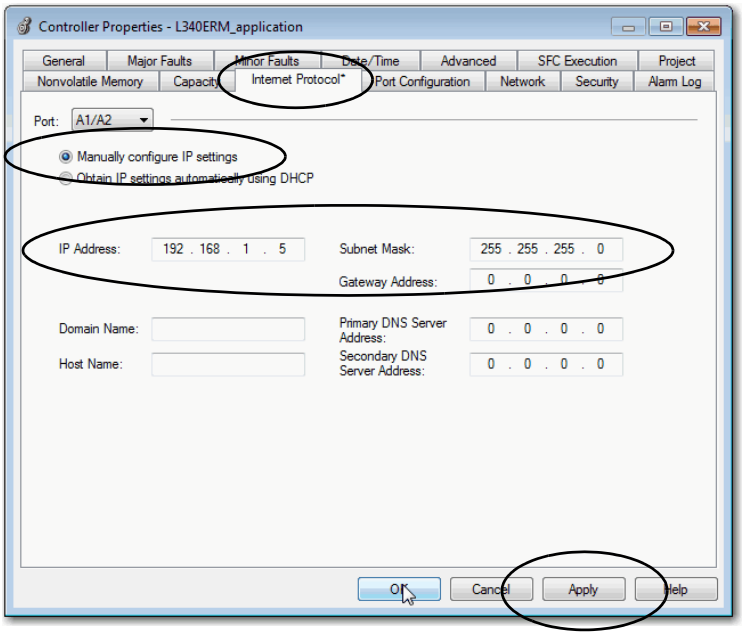
After you change the EtherNet/IP mode to Linear/DLR mode, the new mode choice is displayed on the General tab in the Controller Properties dialog box.



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

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 IP Address and Network Mask values.
5. Click Apply.

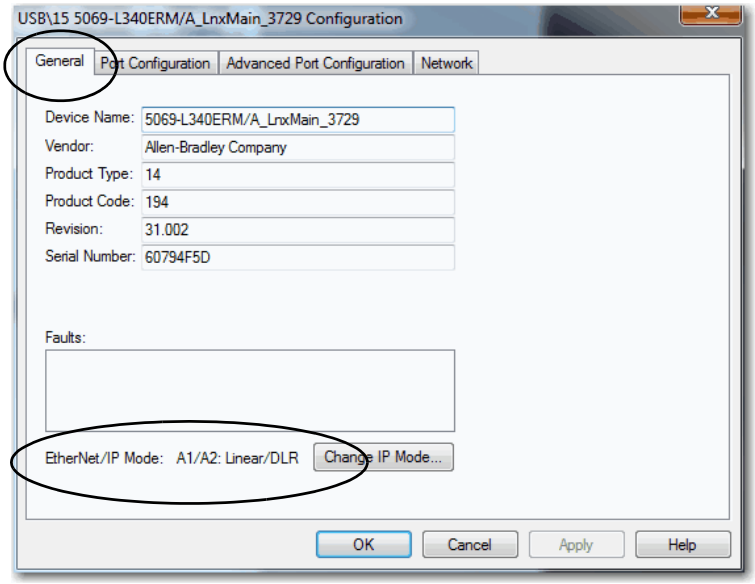


Configure Linear/DLR Mode in RSLinx Classic Software

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.

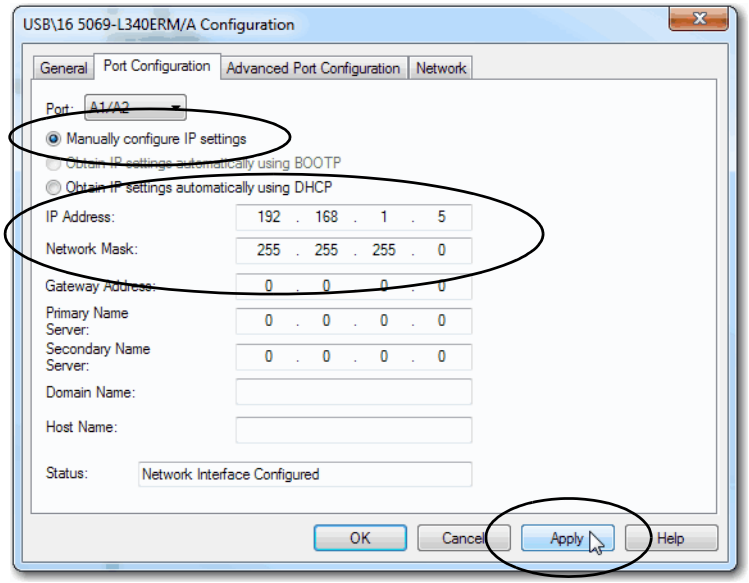
IMPORTANT For more information on how to change the controller EtherNet/IP mode, see Change the EtherNet/IP Mode on page 158.

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



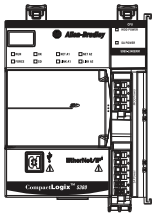
You set the IP Address and Subnet Mask on the Internet Protocol tab.

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.

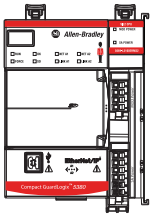


Change the EtherNet/IP Mode

CompactLogix



Compact GuardLogix



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 12 - Effect of Changing the EtherNet/IP Mode

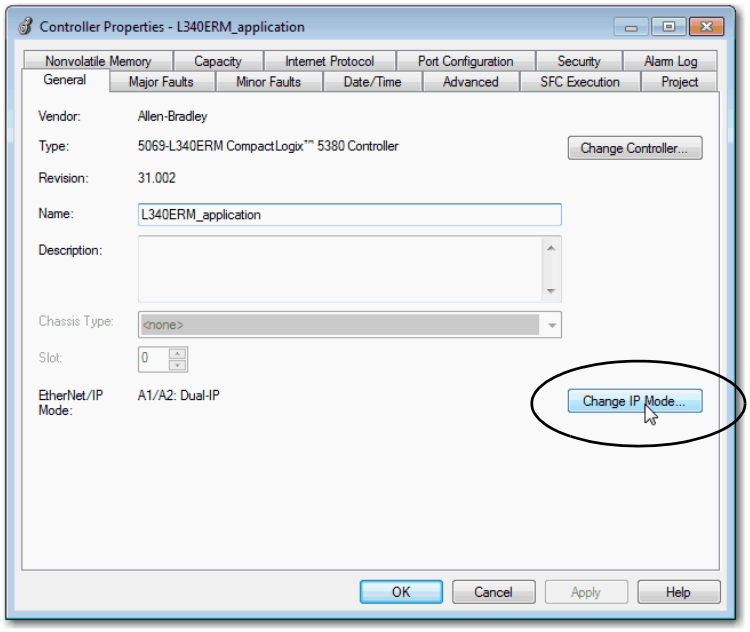
EtherNet/IP Mode Change	Effects
Dual-IP Mode to Linear/DLR Mode	• The port A2 IP address, network mask, default gateway settings are applied to the A1/A2 port. • The MAC address of port A1 is applied to port A1/A2. This scenario exists if the controller firmware is upgraded to revision 29.011 or greater 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

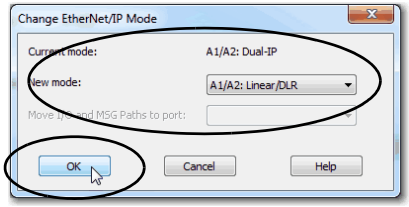
IMPORTANT This example shows the EtherNet/IP mode change from Dual-IP mode to Linear/DLR mode. The same tasks apply to change from Linear/DLR mode to Dual-IP mode.

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.



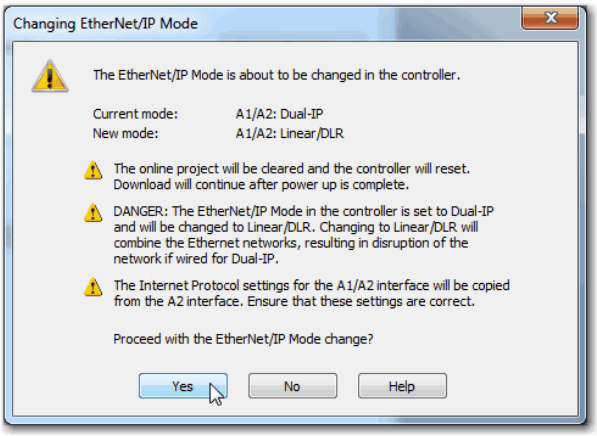
3. From the New mode pull-down menu, choose the new mode and click OK.



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 12 on page 158.



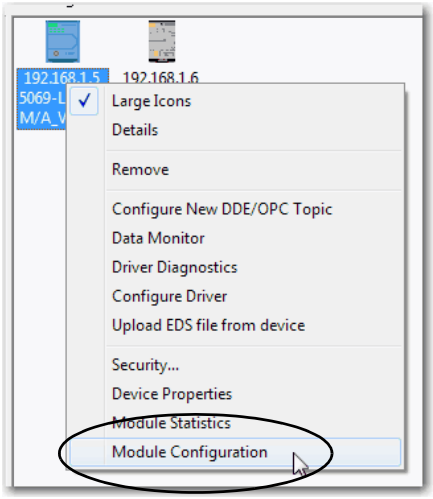
8. Click Yes to continue.

Change the EtherNet/IP Mode in RSLinx Classic Software

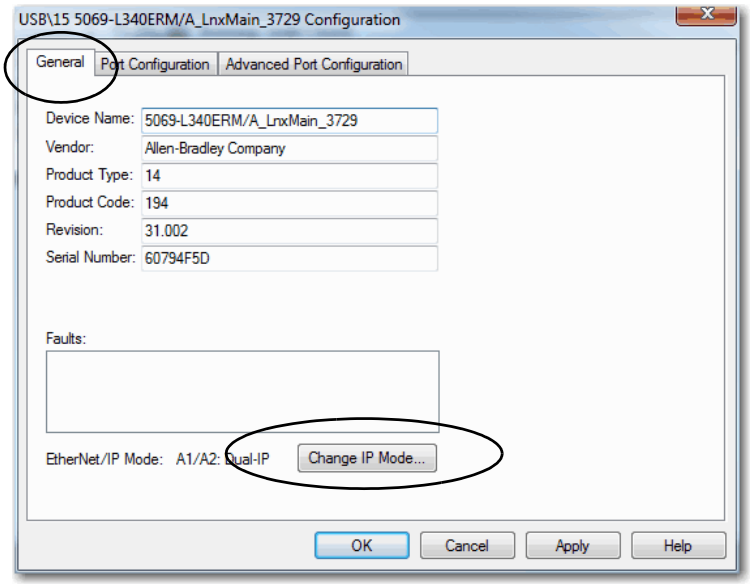
To change the EtherNet/IP mode in RSLinx Classic software, complete these steps.

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

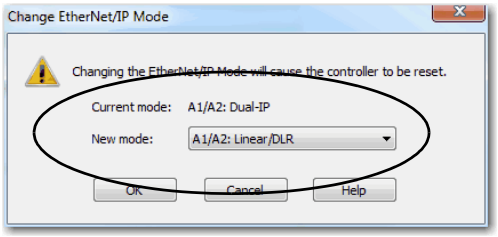
   You cannot change the IP Address or Subnet Mask if the controller is in Run mode.
3. Right-click the controller and choose Module Configuration.



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



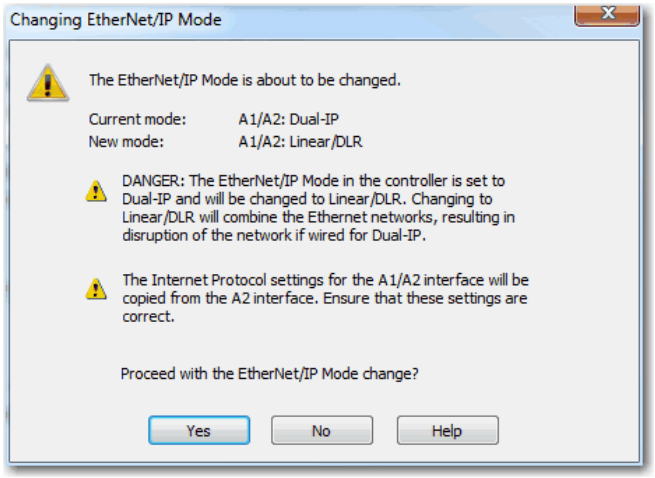
5. From the New mode pull-down menu, choose the new mode and click OK.



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 12 on page 158.



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 Table 5 - EtherNet/IP Network Parameters for DNS Addressing on page 66.

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 164.
- 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

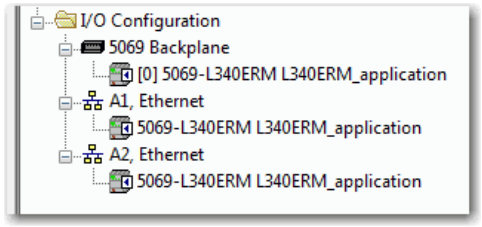
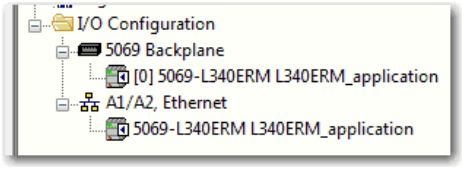
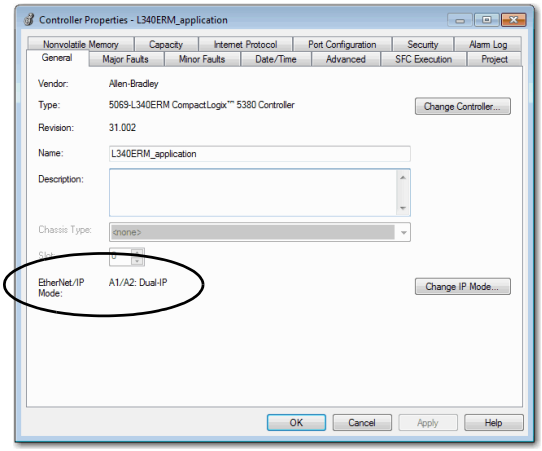
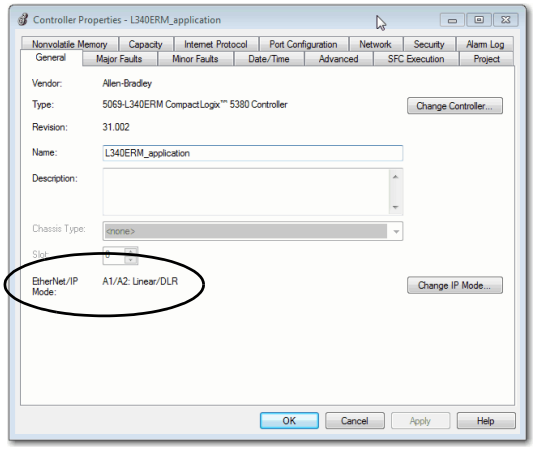
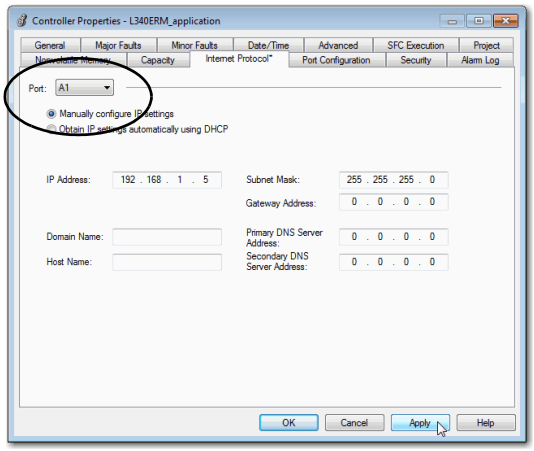
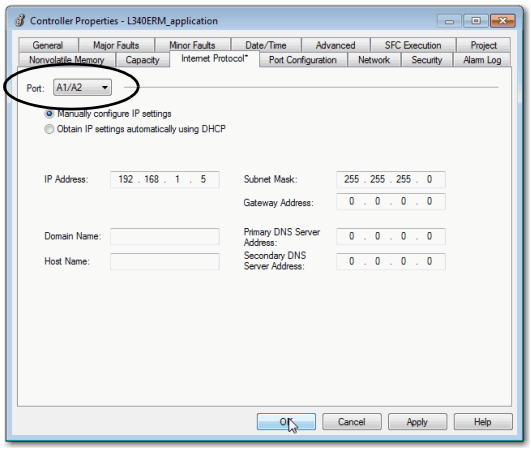
If the controller operates in Linear/DLR mode, the path is 2.

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

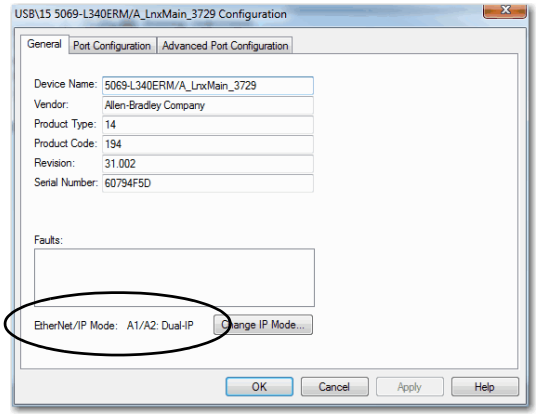
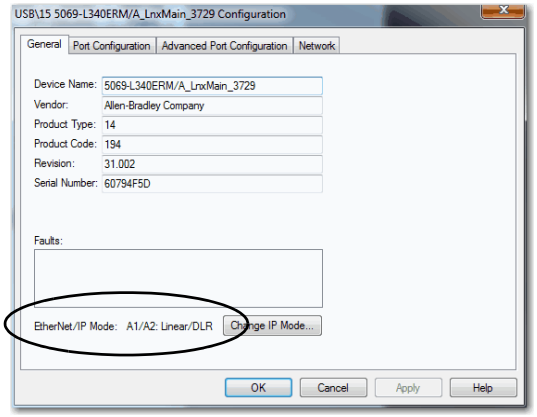
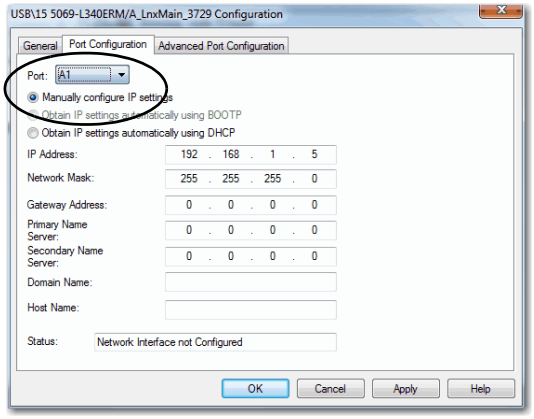
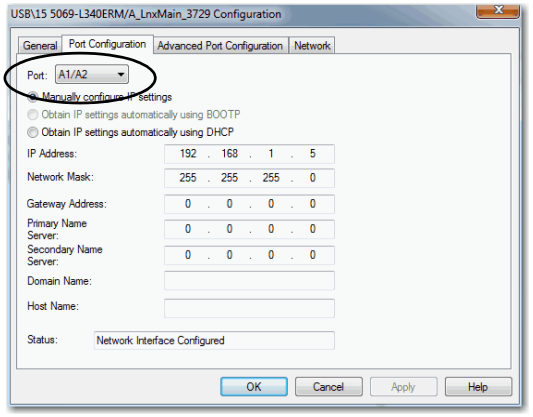
Table 13 - EtherNet/IP Mode Display Differences in the Logix Designer Application

	EtherNet/IP Mode	
Section in Application	**Dual-IP Mode**	**Linear/DLR Mode**
I/O Configuration Tree in Controller Organizer		
General Tab on Controller Properties Dialog Box		
Internet Protocol on Controller Properties Dialog Box	 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 143.	

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

Table 14 - EtherNet/IP Mode Display Differences in the RSLinx Classic Software

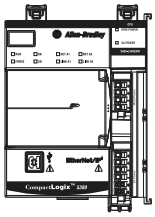
	EtherNet/IP Mode	
Section in Software	**Dual-IP Mode**	**Linear/DLR Mode**
General Tab		
Port Configuration Tab	 If you connect port A1 to a device-level network, some parameters appear as configurable but are not used. For more information on what parameters you configure to connect a port to a device-level network, see Device-level Network on page 143.	

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.

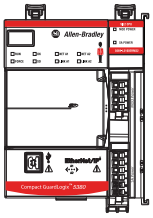
Controller IP Address and Firmware Updates

To operate properly, CompactLogix 5380 and Compact GuardLogix 5380 controllers require an IP address, and the firmware revision that is compatible with the version of Studio 500 Logix Designer you are using.

CompactLogix



Compact GuardLogix



IMPORTANT This section does not apply to the Compact GuardLogix 5380 controllers because you must use firmware revision 31.011 or later with those controllers.

The conditions that are described exist with controllers that use firmware revisions earlier than 31.011.

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. For more information, see Change the EtherNet/IP Mode on page 158. 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.	

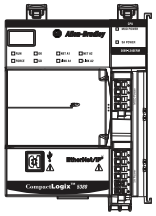
Controller State Before Making Changes	Description	Firmware Revision of Update/Change	Task Completion Order	Result of Completing Tasks in Order Indicated
Operating	• IP address set on port A1/A2 • Firmware revision 28.xxx is installed	Revision 29.011 or later	Update controller firmware	• EtherNet/IP 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. For more information, see Change the EtherNet/IP Mode on page 158.
	• 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:

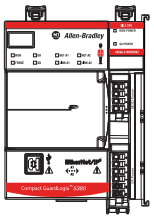
Manage Controller Communication

Connection Overview

CompactLogix



Compact GuardLogix

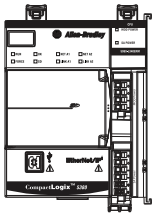


Connections are used when the system contains these conditions:

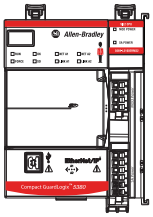
- I/O modules, communication modules, and adapters are present in the I/O configuration of the user project.
- Produced or Consumed tags are configured in the user project.
- Connected Messages are executed in the user application.
- External devices, programming terminals, or HMI terminals communicate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

Controller Communication Interaction with Control Data

CompactLogix



Compact GuardLogix



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 15 highlights the controller behavior.

Table 15 - CompactLogix 5380 and Compact GuardLogix 5380 Controller Behavior

	Tag Access					
Application Construct	**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 - Hel0ps 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 16 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.

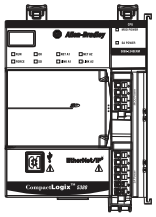
Table 16 - Data Elements

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

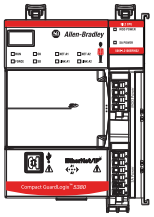
TIP We recommend that you perform this test on a buffered copy of the data and not the actual data element being written to by the communications core. If you use buffered data, you help prevent the risk of the communication core changing data after you have passed the data valid test.

Produce and Consume (Interlock) Data

CompactLogix



Compact GuardLogix



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 30 - Example Produced and Consumed Tags

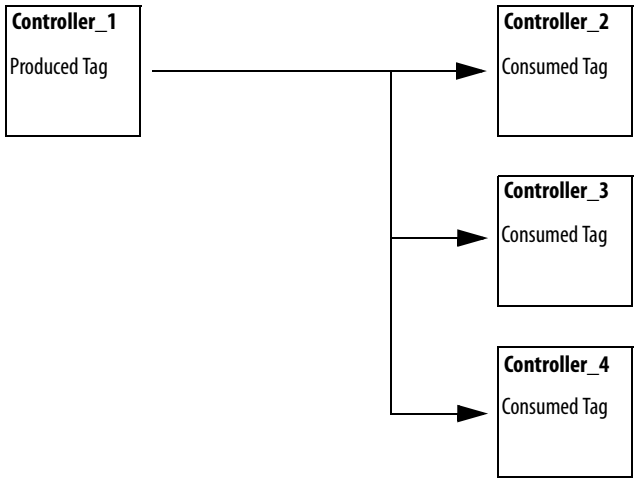


Table 17 describes the system-shared tags.

Table 17 - 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 Produced/Consumed Safety Tags on page 247.

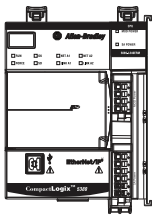
Requested Packet Interval (RPI) of Multicast Tags

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.

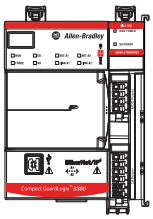
For more information about produced/consumed tags, see the Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011.

Send and Receive Messages

CompactLogix



Compact GuardLogix



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 18 - 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 19 to decide to cache a connection.

Table 19 - 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.

TIP Cached connections transfer data faster than uncached connections. The controller can cache as many as 256 connections.

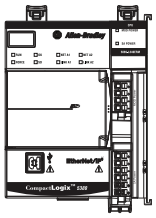
Standard I/O Modules

CompactLogix™ 5380 and Compact GuardLogix® 5380 systems support these I/O module options:

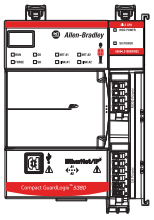
- Local I/O modules
- Remote I/O modules

Local I/O Modules

CompactLogix



Compact GuardLogix



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 20 lists the number of local I/O modules that controllers support.

Table 20 - 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-L310ER-NSE	5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERS2, 5069-L310ERMS2	8
5069-L320ER, 5069-L320ERM	5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2, 5069-L320ERMS2K	16
5069-L330ER(1), 5069-L330ERM(1), 5069-L340ER, 5069-L340ERM, 5069-L350ERM, 5069-L380ERM, 5069-L3100ERM	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	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 Rockwell Automation® Knowledgebase article #942580, '5380 CompactLogix controllers limited to 16 local modules in version 29 of Studio 5000®.' The document is available at http://www.rockwellautomation.com/knowledgebase.
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 example factors that you must consider when you decide how to use local I/O modules in a CompactLogix 5380 system:

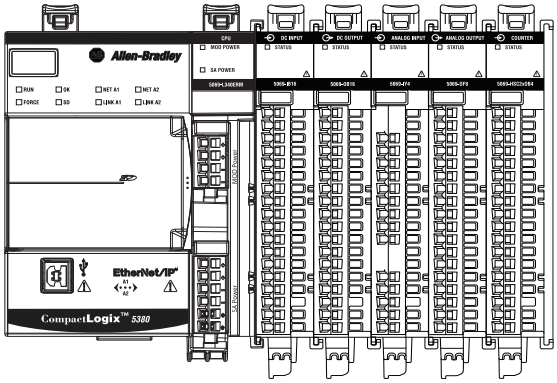
- Number of local I/O modules that the controller supports
- Features available on different modules, for example, sequence of events per point timestamping on only some Compact 5000 I/O digital input modules
- I/O module power usage, including MOD power and SA power

For more information on Compact 5000 I/O modules, see Additional Resources on page 12.

Figure 31 - CompactLogix 5380 and Compact GuardLogix 5380 Systems

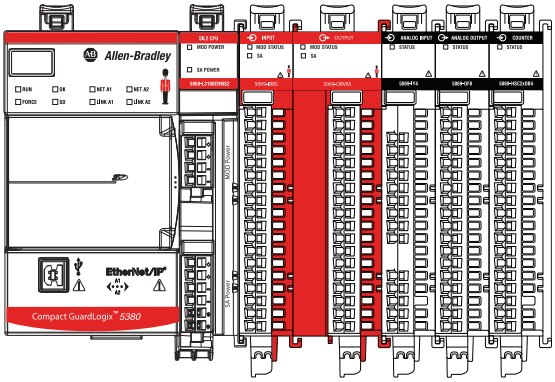
CompactLogix 5380 Controller

Compact 5000™ I/O Local Modules



Compact GuardLogix 5380 Controller

Compact 5000 I/O Local Modules



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 85.

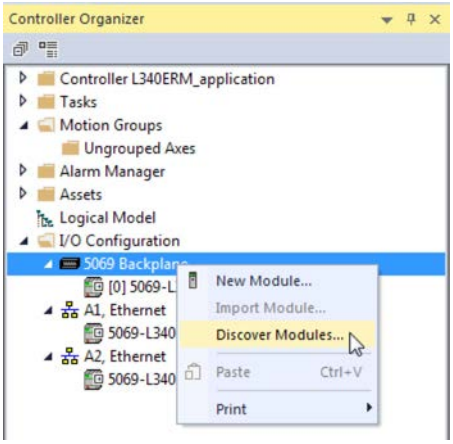
There are two methods to add local I/O modules to the project:

- Discover Modules
- New Module

Discover Modules

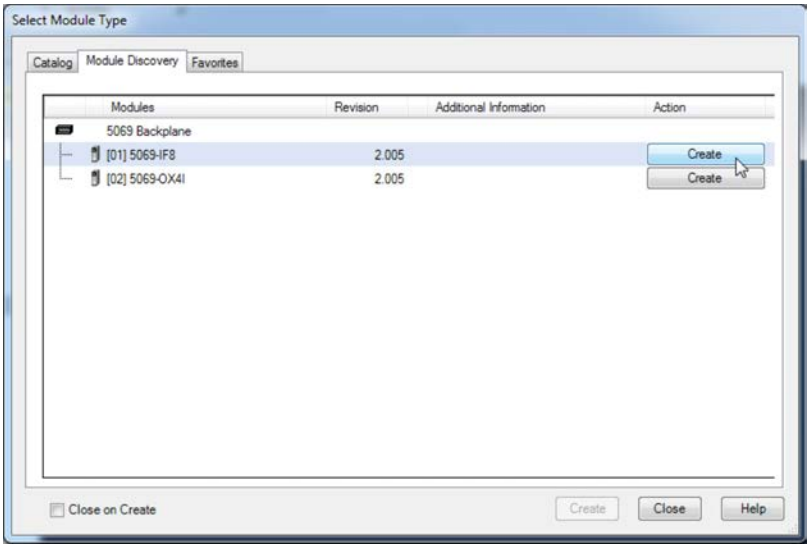
The Discover Modules feature is useful when I/O modules are already installed and you can connect the Logix Designer application to the controller. To use Discover Modules to add a local I/O module, complete these steps.

1. Go online with your Logix Designer application.
2. Right-click 5069 Backplane and choose Discover Modules.

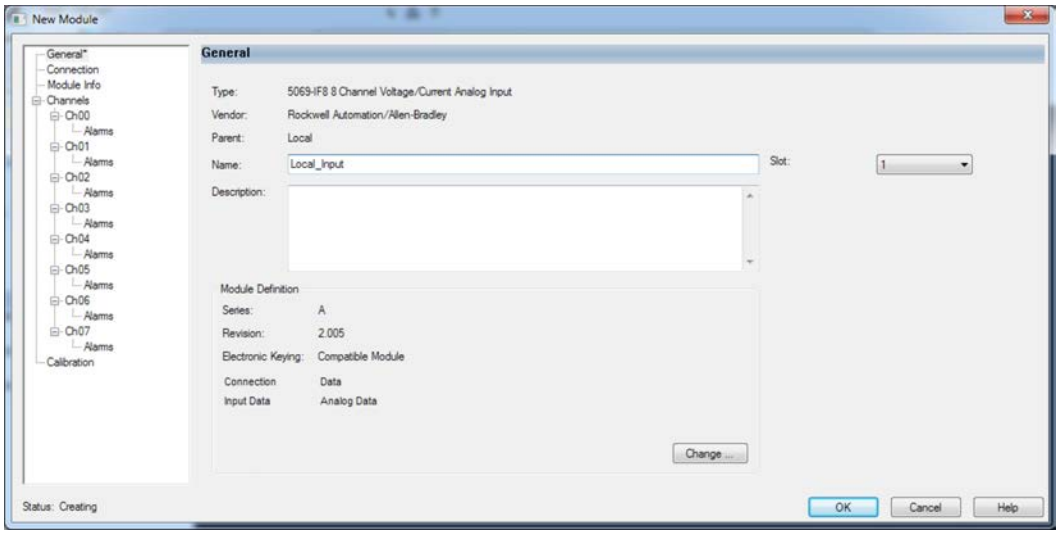


The Logix Designer application automatically detects available modules that are installed in the system.

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

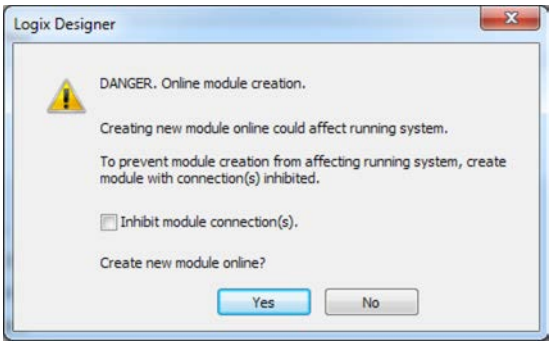


4. At the New Module window, configure the module properties and click OK.



5. At the warning dialog box, click Yes.

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



6. Close the Select Module Type dialog box.

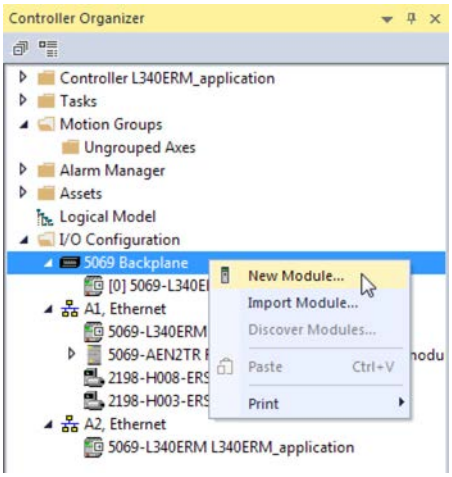
To add additional local I/O modules:

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

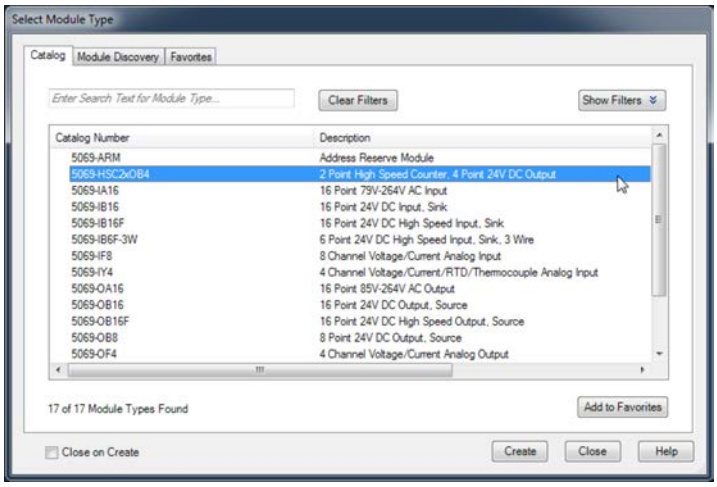
New Module

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 module, complete these steps.

1. Right-click 5069 Backplane and choose New Module.



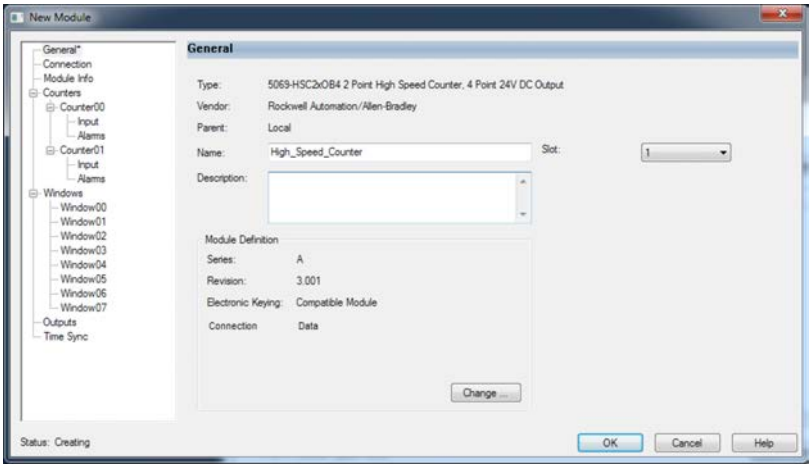
2. Select the module and click Create.



The New Module dialog box appears.

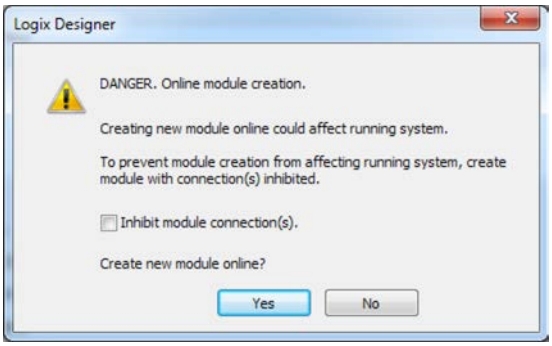
3. On the General tab, set the Series and Revision parameters.
4. Configure the rest of the module as need. For information on electronic keying, see Electronic Keying on page 184.
5. When complete, click OK.

TIP 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.



6. If you add a module while online, at the warning dialog box, click Yes.

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



7. Close the Select Module Type dialog box.

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.

For more information on how to use local I/O modules in a CompactLogix 5380 system, see the resources that are listed in Additional Resources on page 12.

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.

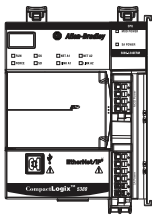
If an I/O connection to a device is interrupted, the result can be a loss of data.

More Information

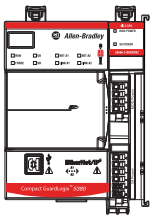
For more detailed information on Electronic Keying, see Electronic Keying in Logix 5000 Control Systems Application Technique, publication LOGIX-AT001.

Remote I/O Modules

CompactLogix



Compact GuardLogix



Remote I/O modules do not reside in the CompactLogix 5380 or Compact GuardLogix 5380 control system. 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 137

Figure 32 - Remote I/O Modules in a CompactLogix 5380 System on a DLR Network Topology

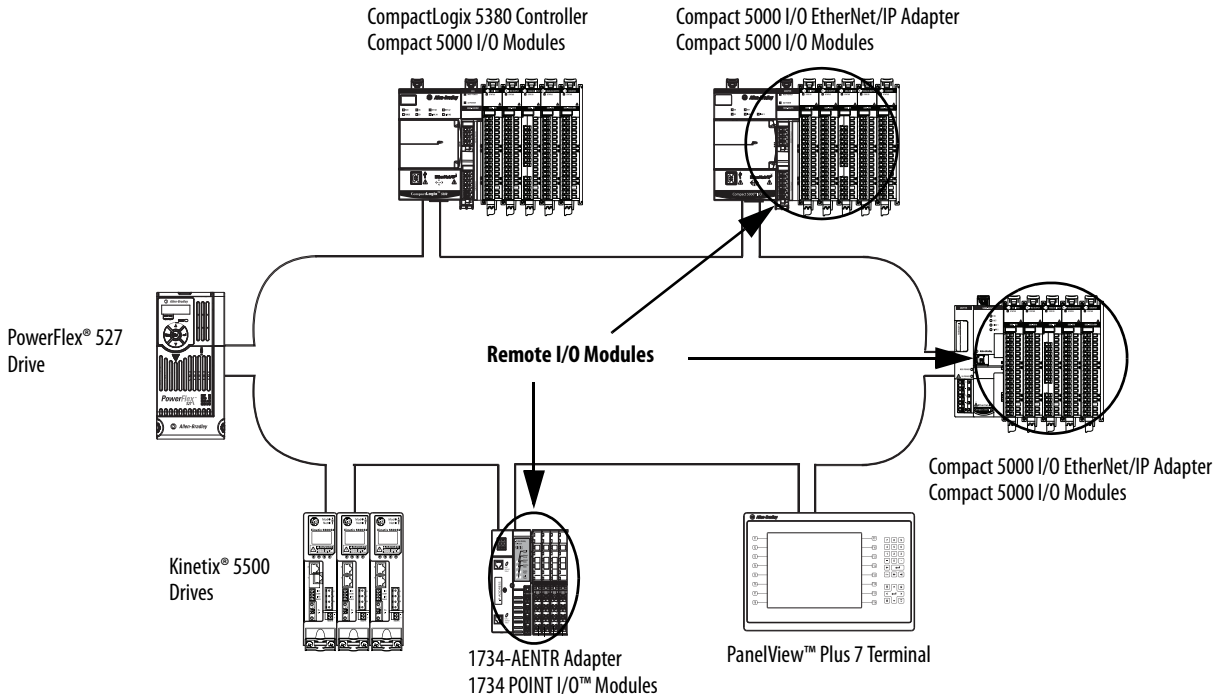


Figure 33 - Remote I/O Modules in a CompactLogix 5380 System on a Linear Network Topology

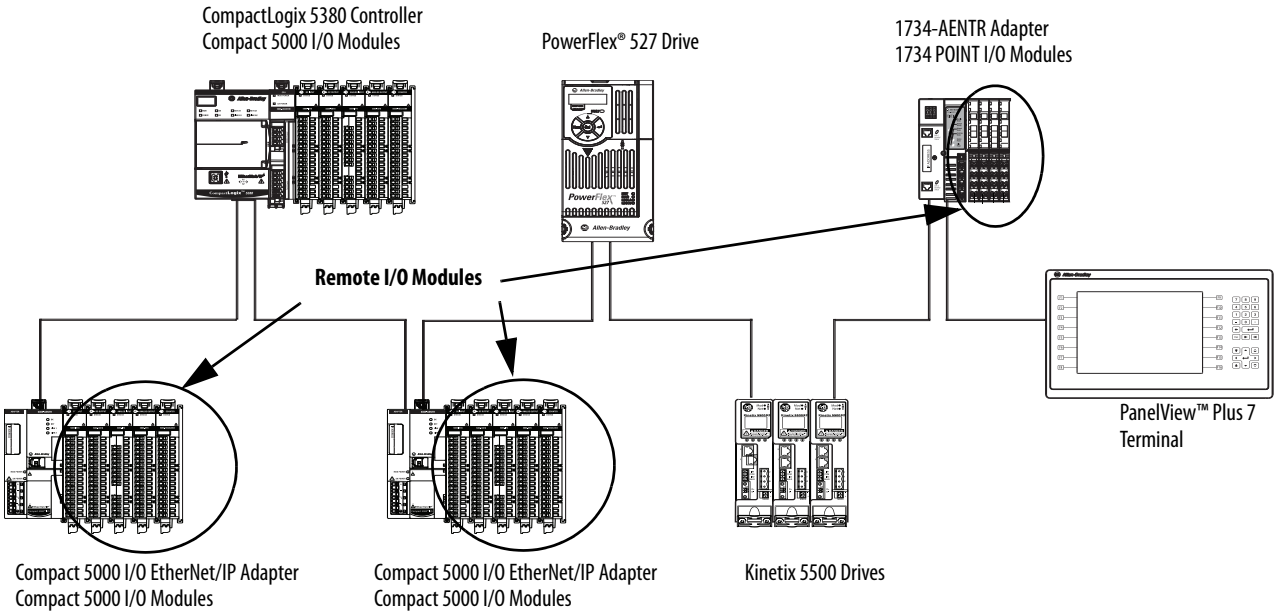
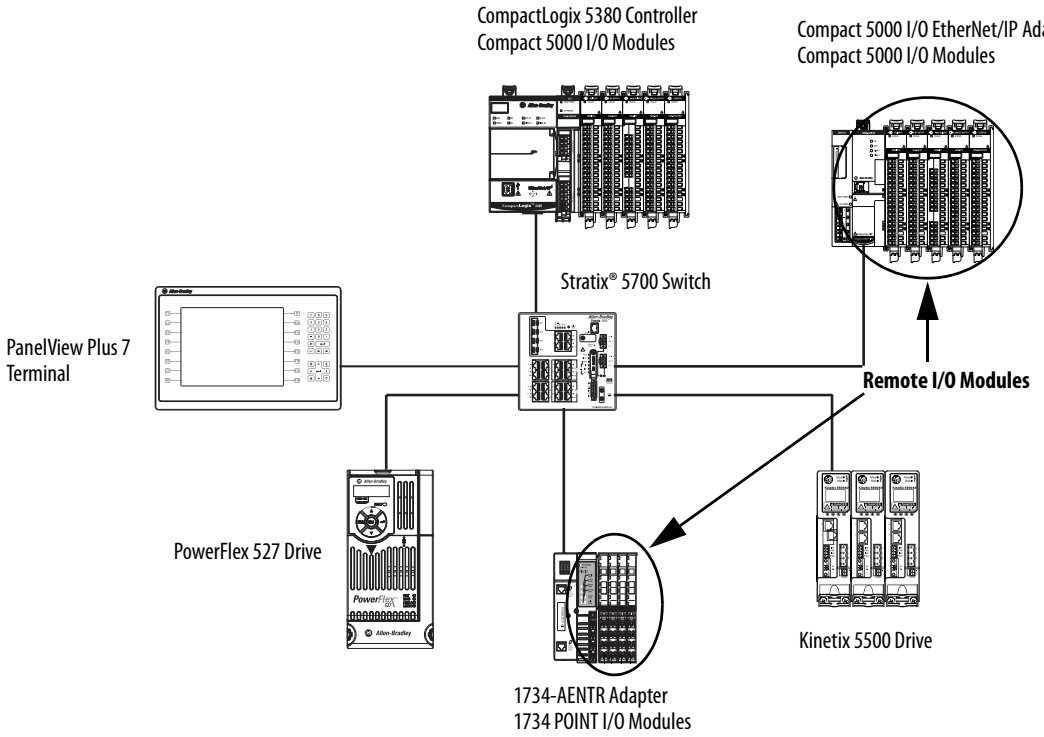


Figure 34 - Remote I/O Modules in a CompactLogix 5380 System on a Star Network Topology



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

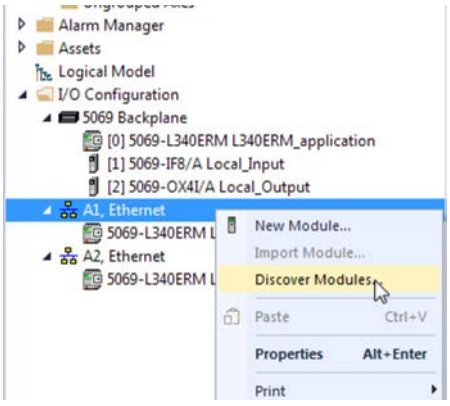
The Discover Modules feature is useful when I/O modules are already installed and connected to the network. When you use Discover Modules to find Ethernet devices, the Logix Designer application browses based on how Ethernet browsing is configured in RSLinx® Classic software.

- 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 188.
- 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 188.

The tasks in this section apply when you use the EtherNet/IP driver in RSWho to browse the network.

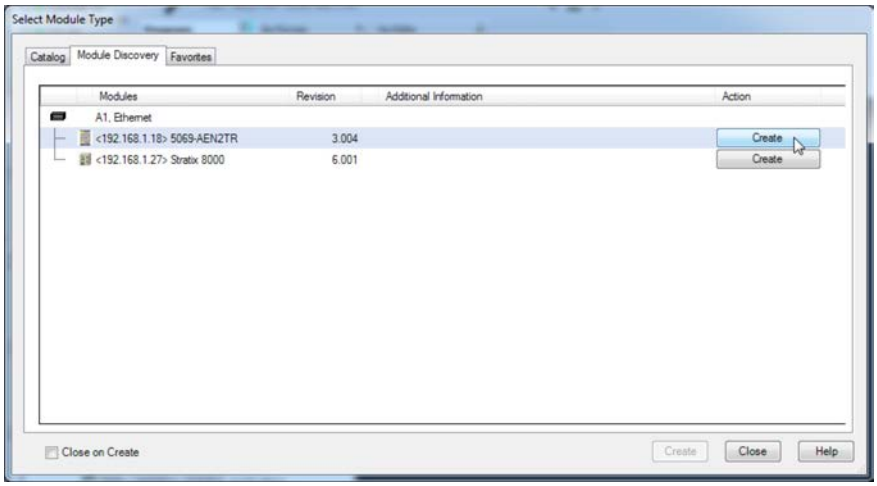
To use Discover Modules to add a remote I/O module, complete these steps.

1. Go online with your Logix Designer application.
2. Right-click Ethernet and choose Discover Modules.

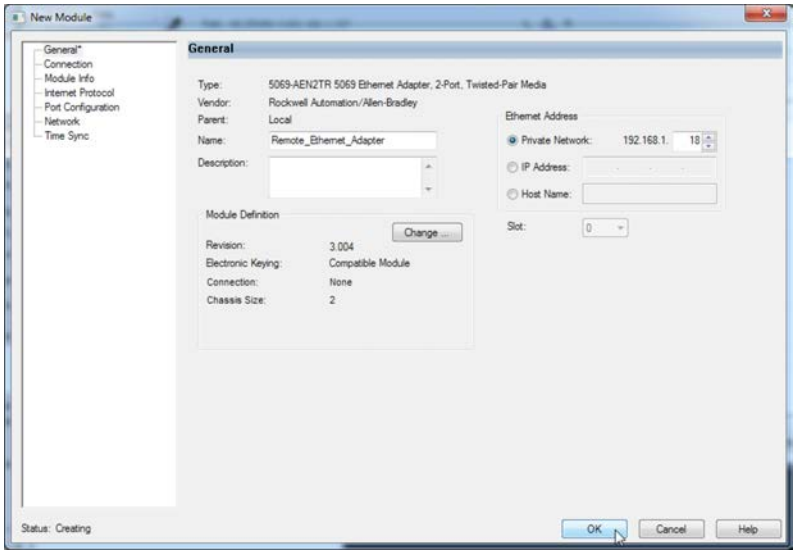


The Logix Designer application automatically detects available modules that are installed in the system.

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

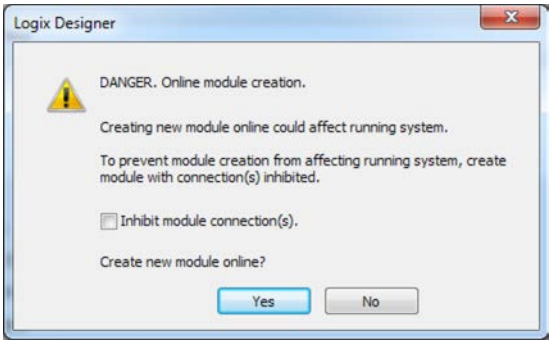


4. At the New Module window, configure the module properties and click OK.

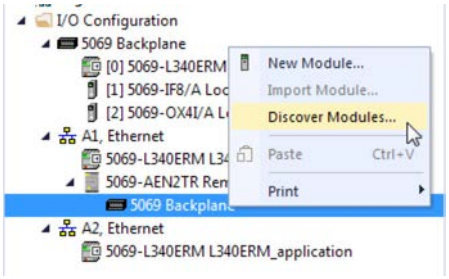


5. At the warning dialog box, click Yes.

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

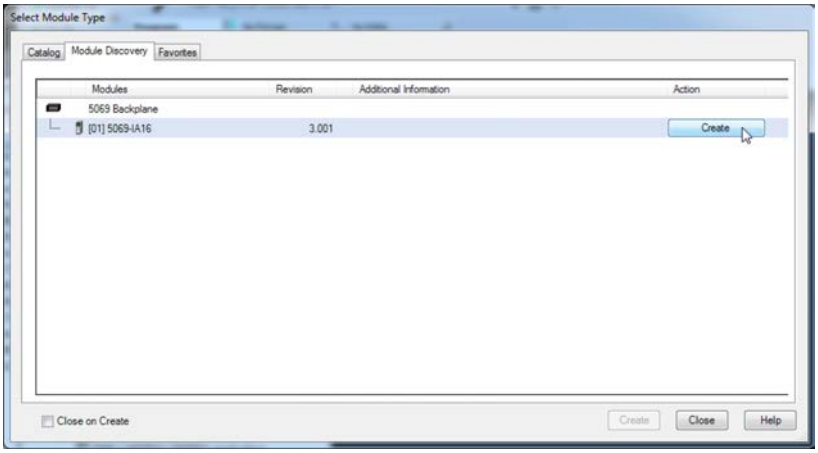


6. Close the Select Module Type dialog box.
7. Right-click 5069 Backplane and choose Discover Modules.

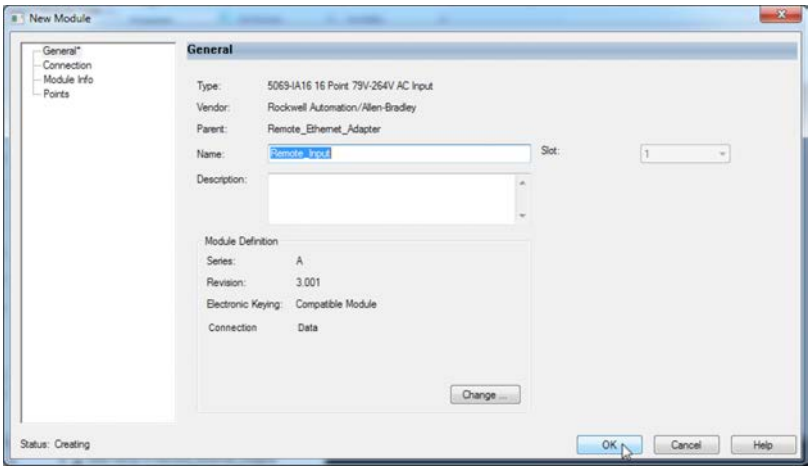


The Logix Designer application automatically detects available modules that are installed in the system.

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

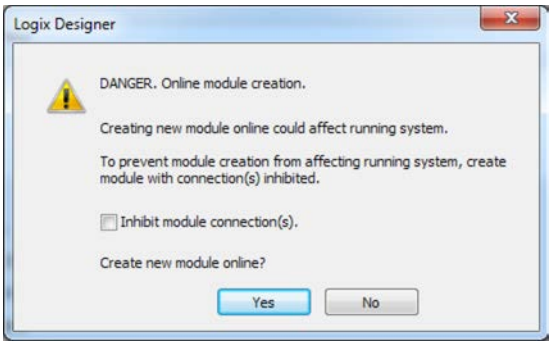


9. At the New Module window, configure the module properties and click OK.



10. At the warning dialog box, click Yes.

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



11. Close the Select Module Type dialog box.

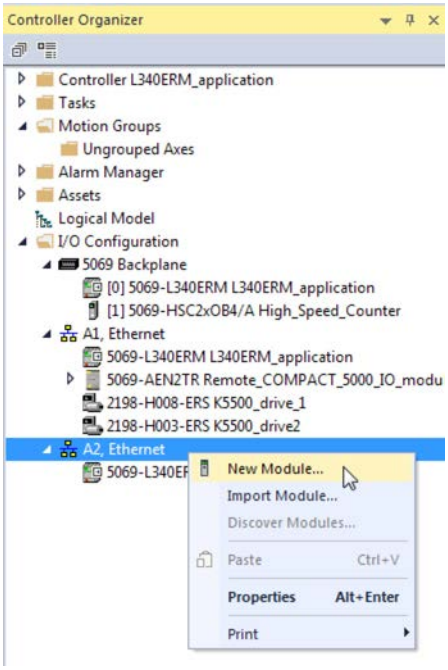
After you add the remote I/O module, consider the following:

- 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.

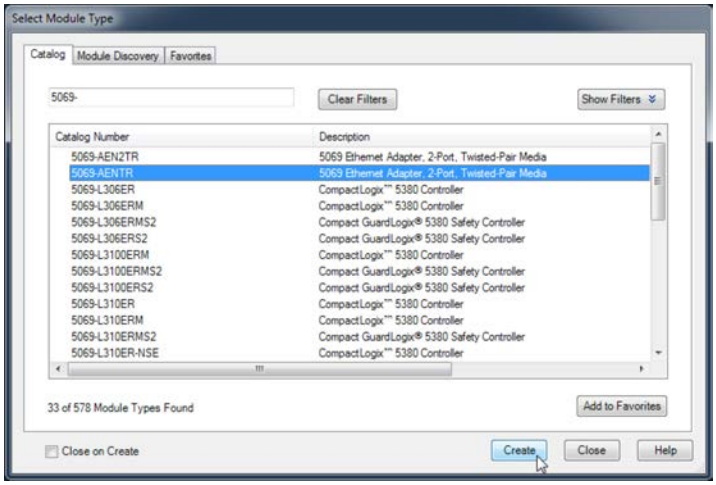


2. Select the EtherNet/IP adapter and click Create.

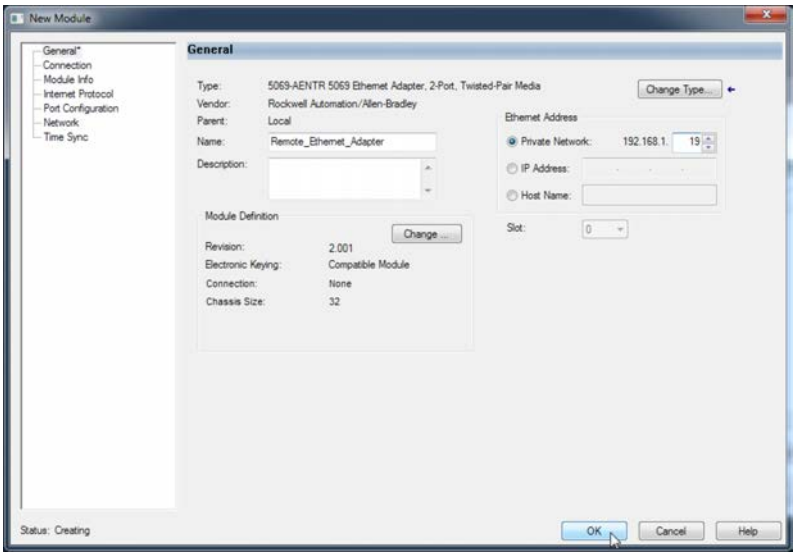
TIP

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.

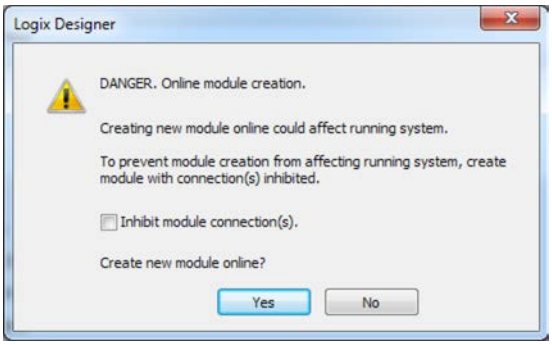


3. At the New Module window, configure the module properties and click OK.



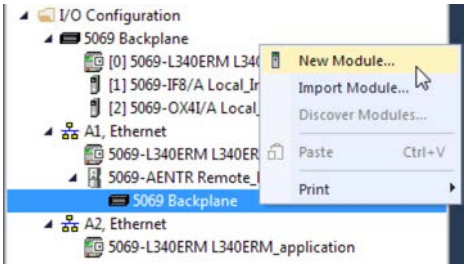
4. If you add a module while online, then at the warning dialog box, click Yes.

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



5. Close the Select Module Type dialog box.

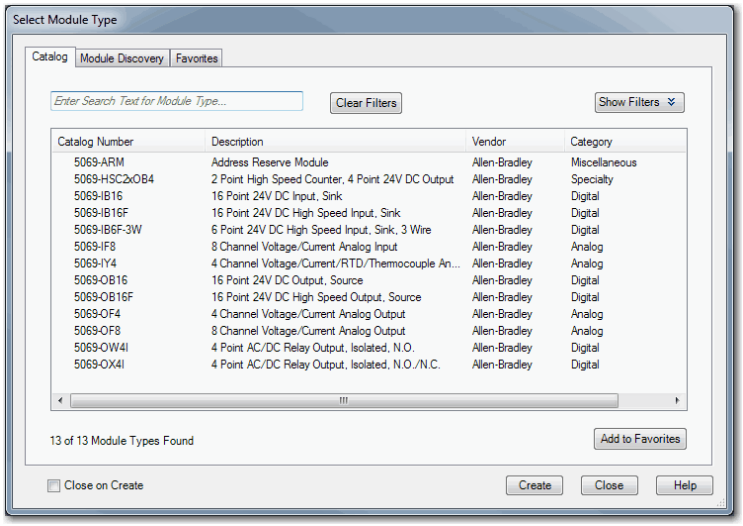
6. Right-click the newly added EtherNet/IP communication module or the backplane and choose New Module.



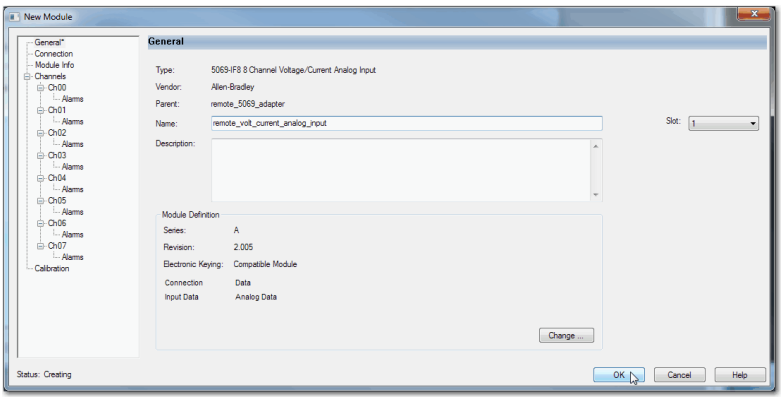
7. Select the I/O module that you want to add and click Create.

TIP If you must add multiple I/O modules to the same remote location, we recommend that you clear the Close on Create checkbox before you click Create.

If the Close on Create checkbox is cleared, when you complete configuration for an I/O module, the Select Module Type dialog box appears automatically and you can skip step 6.

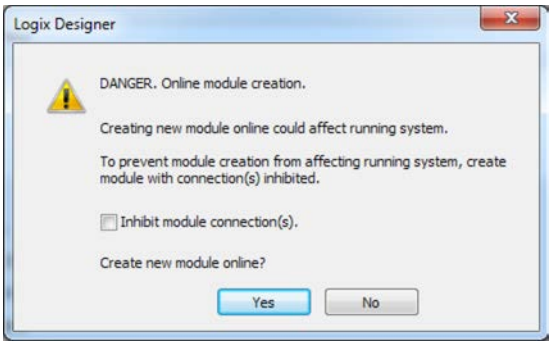


8. Configure the I/O module.
9. At the New Module window, configure the module properties and click OK.



10. If you add a module while online, then at the warning dialog box, click Yes.

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



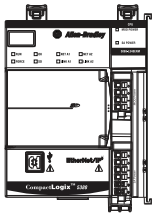
11. Close the Select Module Type dialog box.

After you add the remote I/O module, consider the following:

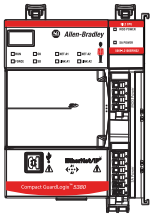
- To add remote I/O modules in the same remote location:
  - If you cleared the Close on Create checkbox when you created the first I/O module, repeat steps 7...8.
  - If you did not clear the Close on Create checkbox when you created the first I/O module, repeat steps 6...8.
- To add remote I/O modules in another new remote location, repeat steps 1...11.

Add to the I/O Configuration While Online

CompactLogix



Compact GuardLogix



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.

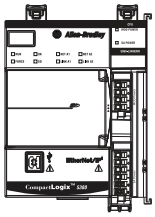
- Compact 5000 I/O modules - As local or remote I/O modules
- Compact 5000 I/O EtherNet/IP adapters
- 1756 ControlLogix EtherNet/IP modules
- 1756 ControlLogix I/O modules

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

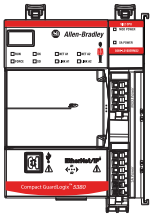
- 1756 ControlLogix Motion modules (1756-M02AE, 1756-HYD02, 1756-M02AS, 1756-M03SE, 1756-M08SE, 1756-M08SEG, 1756-M16SE)
- ControlLogix 1756-RIO
- ControlLogix 1756-SYNCH
- Safety I/O

Determine When Data Is Updated

CompactLogix



Compact GuardLogix



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:

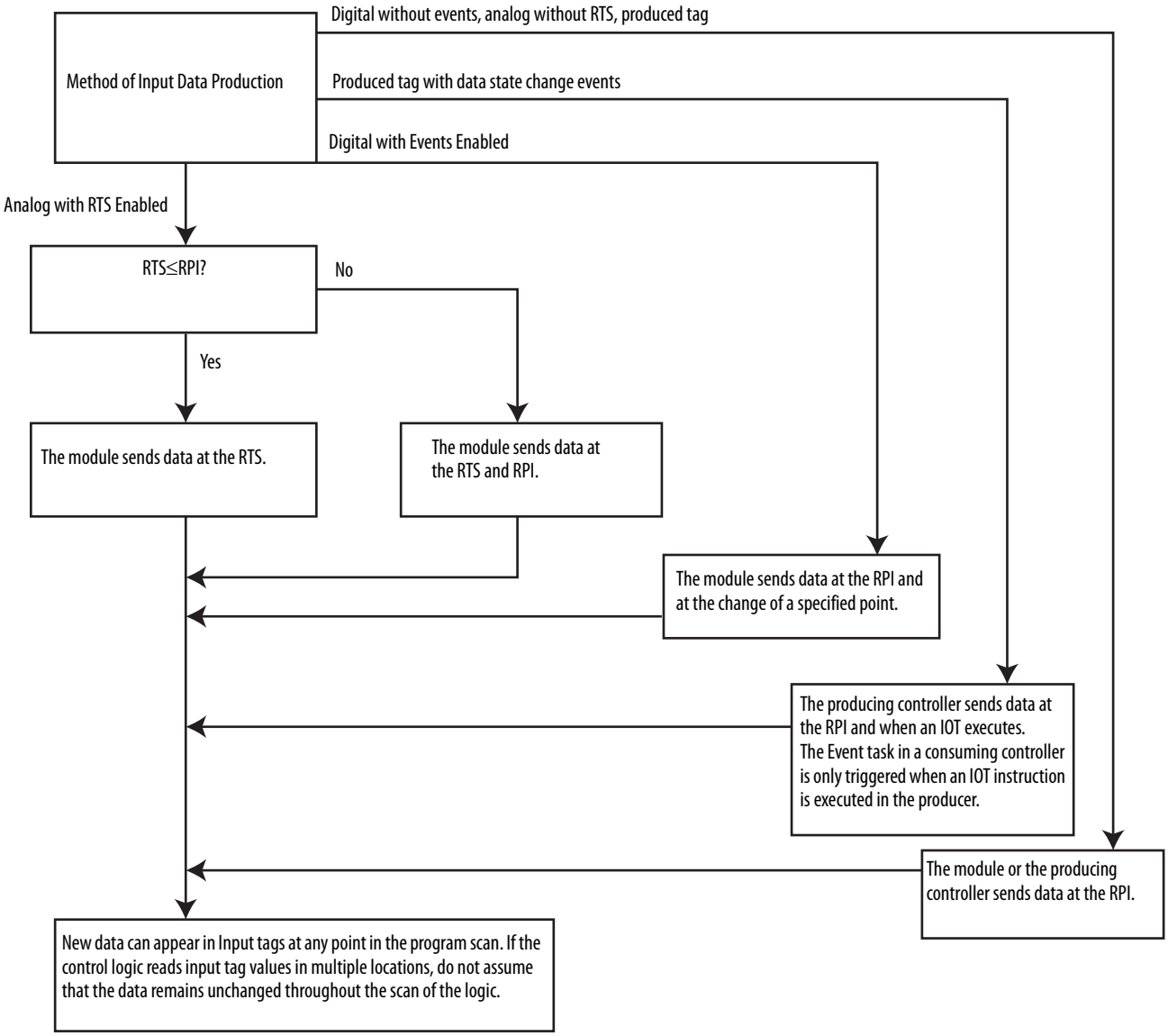
- Input Data Update Flowchart
- Output Data Update Flowchart

Input Data Update Flowchart

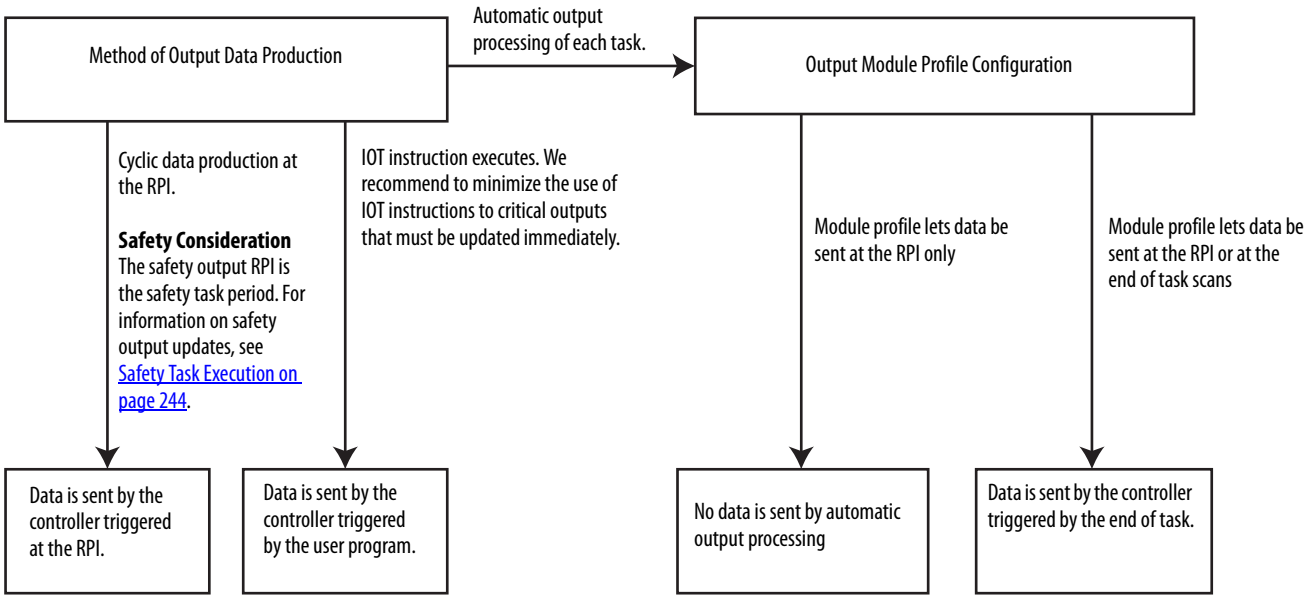
IMPORTANT **Safety Consideration**

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.

See Safety Task Execution on page 244.



Output Data Update Flowchart

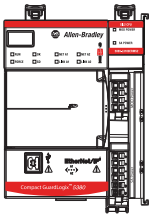


Notes:

Safety I/O Devices

Add Safety I/O Devices

Compact GuardLogix



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

- Node address for DeviceNet networks

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.

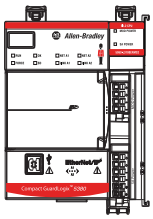
The controller can communicate with devices on DeviceNet. However, typically Compact GuardLogix 5380 controllers use EtherNet/IP networks to communicate with safety devices.

- IP address for EtherNet/IP networks
- Safety network number (SNN). To set the SNN, see page 204.
- Configuration signature. See page 209 for information on when the configuration signature is set automatically and when you must set it.
- Reaction time limit. See page 208 for information on setting the reaction time limit.
- Safety input, output, and test parameters complete the module configuration

IMPORTANT
- You cannot add Safety I/O Devices while online with the controller.
- You can configure safety I/O devices via the Compact GuardLogix 5380 controller by using the Studio 5000 Logix Designer® application.
- The Discover Modules feature is not compatible with safety I/O devices.

Configure Safety I/O Devices

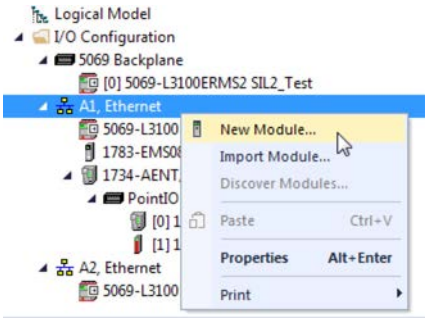
Compact GuardLogix



Add the safety I/O device to the I/O Configuration folder.

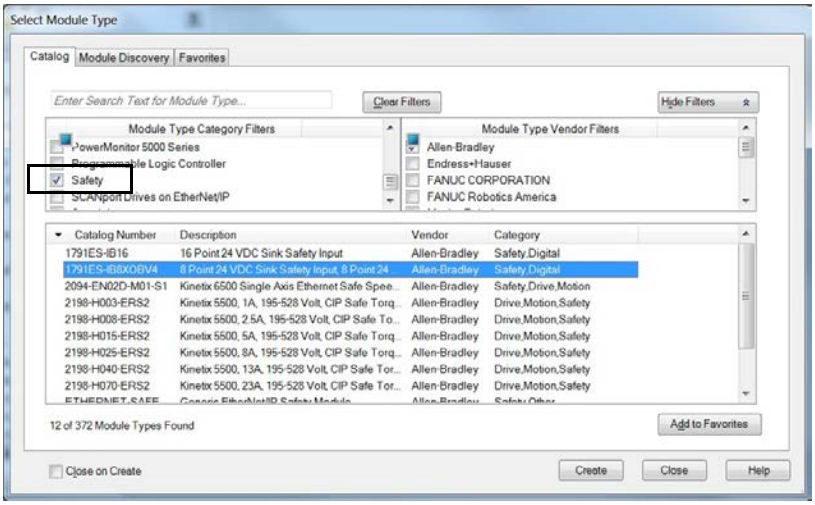
TIP Some safety I/O devices support both standard and safety data. The Module Definition defines what data is available.

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



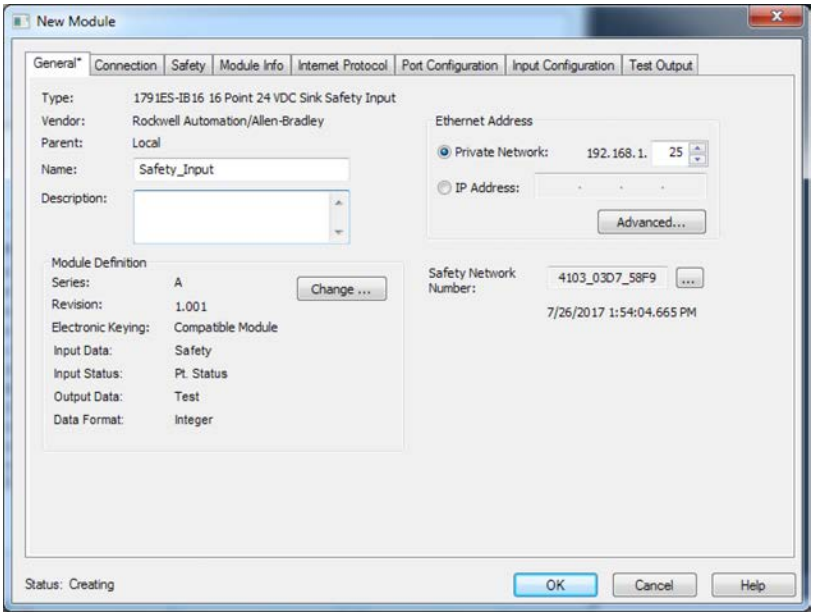
2. From the Catalog tab, select the safety I/O device.

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



3. Click Create.

4. Type a name for the new device.



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

IMPORTANT For safety I/O devices, do not use Disable Keying.
For more information on Electronic Keying, see page 184.

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

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

   If your network uses network address translation (NAT), see Using Network Address Translation (NAT) with CIP Safety Devices on page 202.

7. To modify the Safety Network Number, click the ... button (if necessary).

   See page 204 for details.

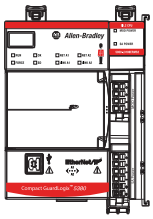
8. Set the Connection Reaction Time Limit by using the Safety tab.

   See page 208 for details.

9. 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

Compact GuardLogix



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.

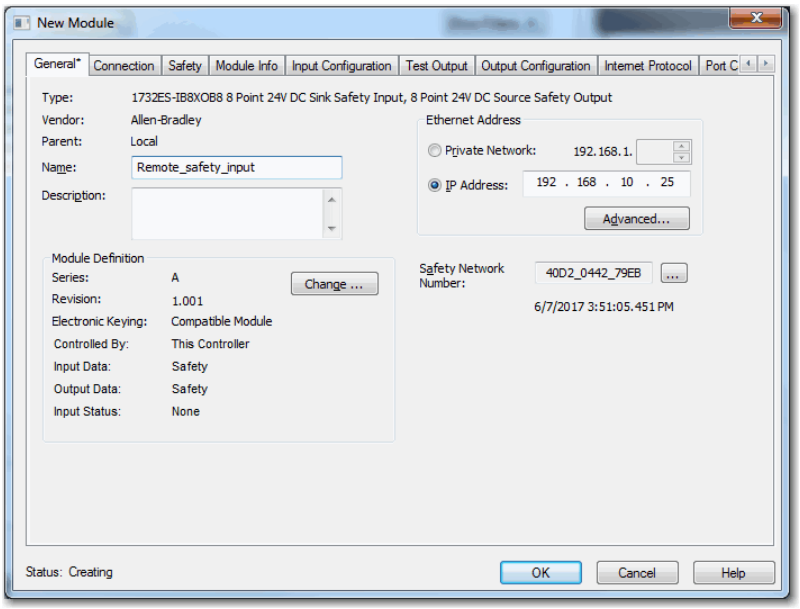
This section only applies to safety users where the controller and the devices it talks to are on separate sides of the NAT-configured router or switch.

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.

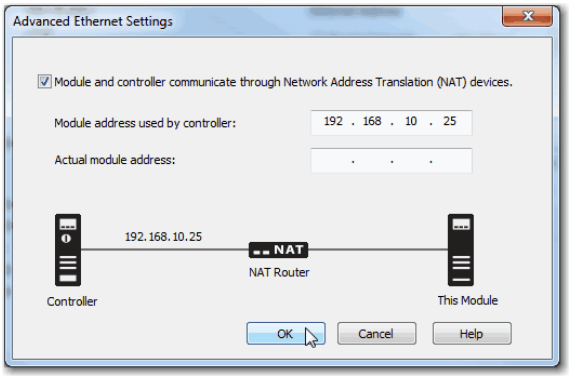
If you are using NAT to communicate with a CIP Safety device, follow these steps to set the IP address.

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.



2. To open the Advanced Ethernet Settings dialog box, click Advanced.



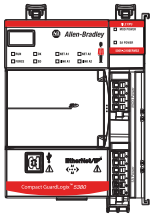
3. Check the checkbox to indicate that this module and the controller communicate through NAT devices.
4. Type the Actual module address.

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

5. Click OK.

Set the SNN of a Safety I/O Device

Compact GuardLogix



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.

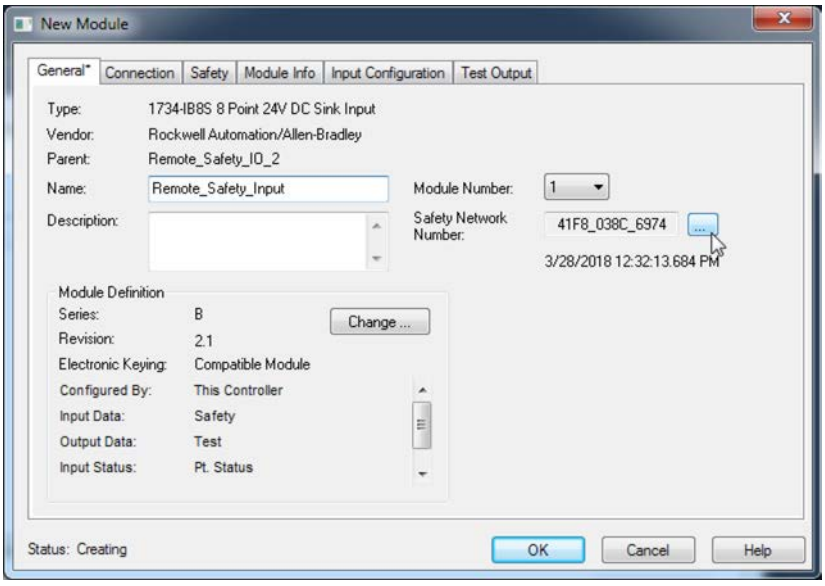
If your application requires you to manually assign the SNN of safety I/O devices, you only have to assign the SNN of the first safety I/O device you add in a remote network or backplane. Logix Designer then assigns the SNN of the first device to any additional devices that you add to that same remote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

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

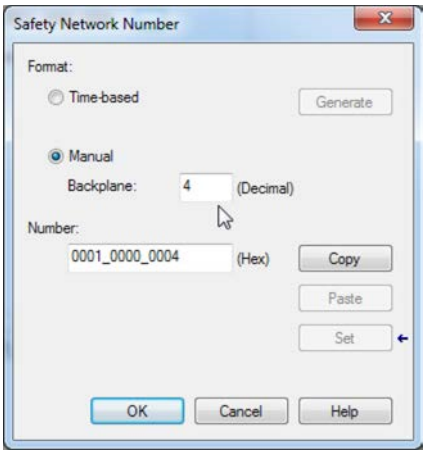
Change a Safety I/O Device SNN

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

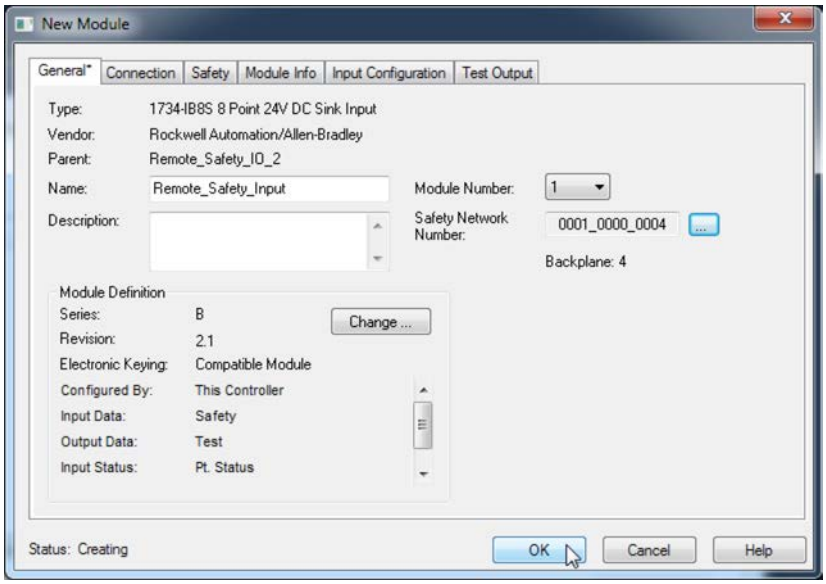
1. Right-click the remote EtherNet/IP communication module in the I/O Configuration tree, and select New Module.
2. Select your safety I/O device, and click Create.
3. On the New Module configuration dialog, click ... to the right of the safety network number.



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



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



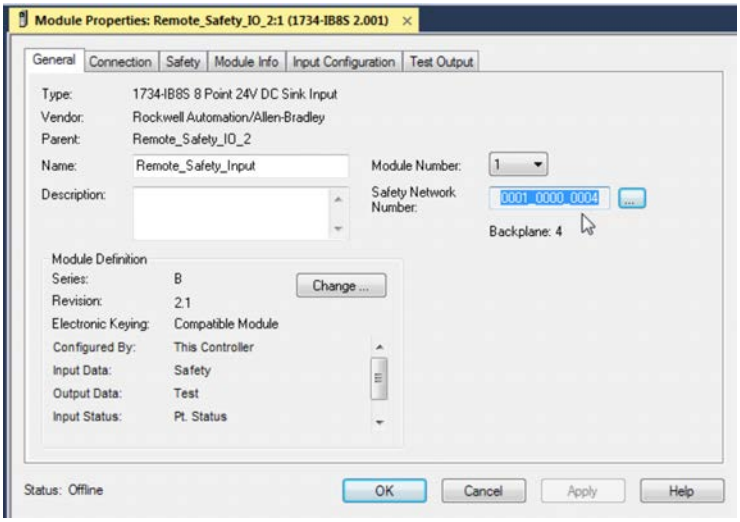
Copy and Paste a Safety I/O Device Safety Network Number (SNN)

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

Copy a Safety I/O Device SNN

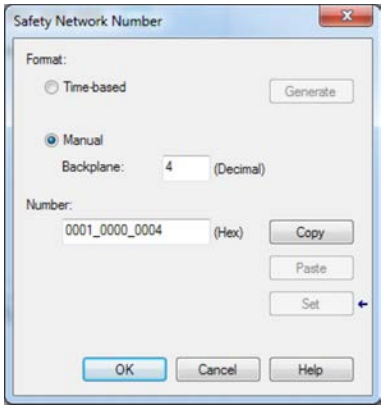
From the Module Properties General Tab:

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



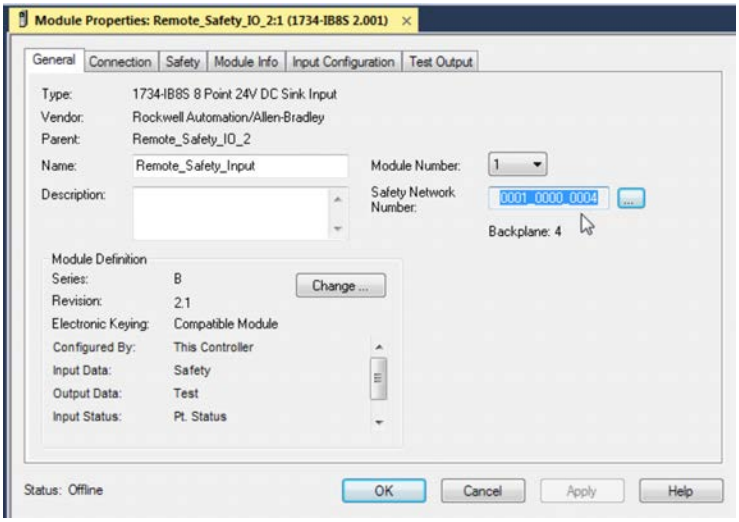
From the Safety Network Number dialog:

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

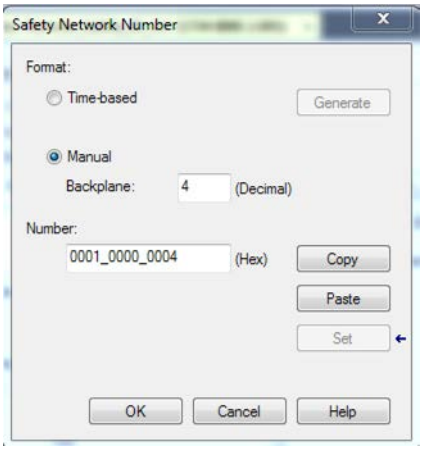


Paste a Safety I/O Device SNN

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



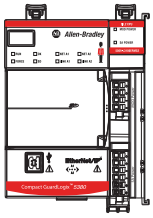
2. On the Safety Network Number dialog, either click Paste, or click in the SNN field and Press Ctrl-V.



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

Connection Reaction Time Limit

Compact GuardLogix



These three values define the Connection Reaction Time Limit (CRTL).

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

If you adjust these values, then you can adjust the Connection Reaction Time Limit. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state (OFF).

IMPORTANT The default values generate an Input connection reaction time limit of 40 ms. If no edits are made to the defaults, verify that this connection reaction time limit is used in the safety reaction time calculations.

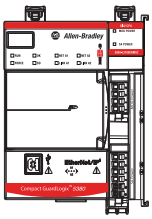
We recommend that you do not decrease the timeout multiplier and network delay multiplier from the default, as this could lead to nuisance connection drops.

IMPORTANT For applications with large banks of POINT Guard Safety I/O, the default connection reaction time limit can result in connection loss to the safety I/O modules. In these cases, it can be necessary to increase the RPI value from the default. Make sure that the new connection reaction time limit is used in the safety reaction time calculations.

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

Safety I/O Device Signature

Compact GuardLogix

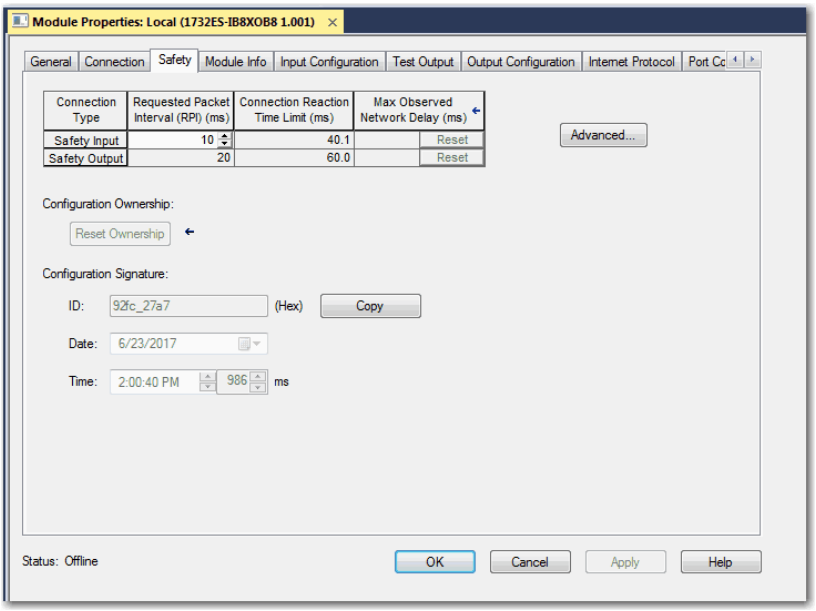


Each safety device has a unique configuration signature that defines the module configuration. The configuration signature is composed of an ID number, date, and time, and is used to verify the configuration of the module.

Configuration Via the Logix Designer Application

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

Figure 35 - View and Copy the Configuration Signature



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

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

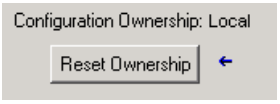
When the controller project is online, the Safety tab of the Module Properties dialog box displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the safety network number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

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

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

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

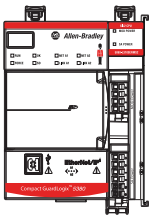
1. Right-click the module and choose Properties.
2. Click the Safety tab.
3. Click Reset Ownership.



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

I/O Device Address Format

Compact GuardLogix



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

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

A Safety I/O module address follows this example.

EXAMPLE Modulename.Type.Member

Table 21 - Safety I/O Device Address Format

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

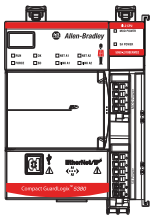
(1) This member is required.

Table 22 - More Resources

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

Replace a Safety I/O Device

Compact GuardLogix



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

Configuration Ownership

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

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

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

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

Replacement Configuration

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

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

Table 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 module via a 1788-EN2DN linking device	Logix Designer application	Below
1734 POINT Guard I/O™ module via a 1788-EN2DN linking device and a 1734-PDN adapter	RSNetWorx™ for DeviceNet software	See the POINT Guard I/O Safety Modules User Manual, publication 1734-UM013.

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

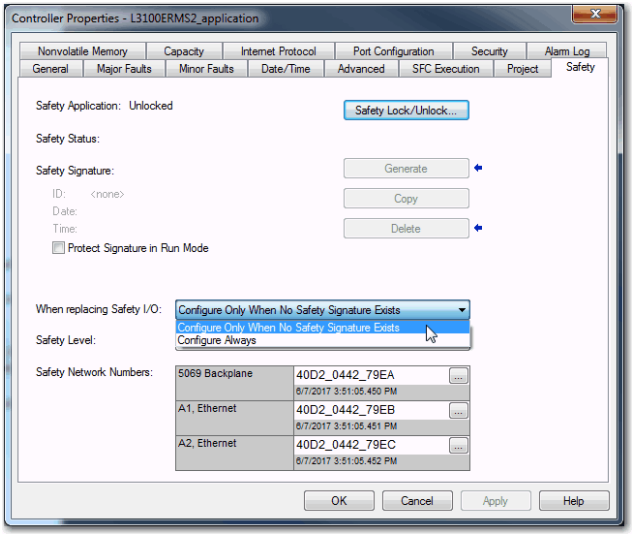
  For more information, see Replacement with 'Configure Only When No Safety Signature Exists' Enabled on page 214.

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

  For more information, see Replacement with 'Configure Always' Enabled on page 219.

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

Figure 36 - Safety I/O Device Replacement



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

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

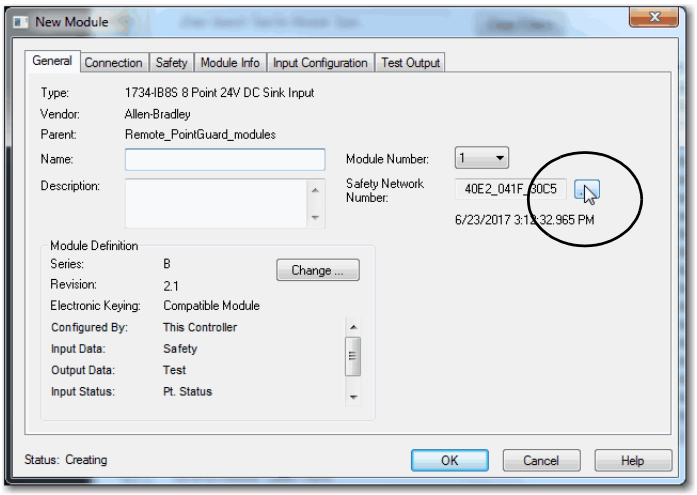
If the project is configured as 'Configure Only When No Safety Signature Exists', follow the appropriate steps in Table 24 to replace a safety I/O device based on your scenario. After you complete the steps, the DeviceID matches the original, and this enables the safety controller to download the proper device configuration, and re-establish the safety connection.

Table 24 - Replacing a Module

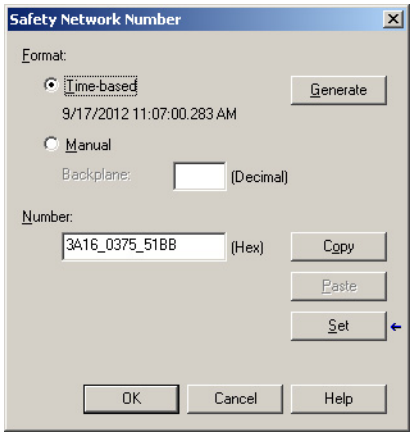
Compact GuardLogix Safety Signature Exists	Replacement Module Condition	Action Required
No	No SNN (Out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (Out-of-box)	See Scenario 1 - Replacement Device Is Out-of-box and Safety Signature Exists on page 214.
Yes	Different SNN from original safety task configuration	See Scenario 2- Replacement Device SNN Is Different from Original and Safety Signature Exists on page 216.
No		See Scenario 3 - Replacement Device SNN Is Different from Original and No Safety Signature Exists on page 218.

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

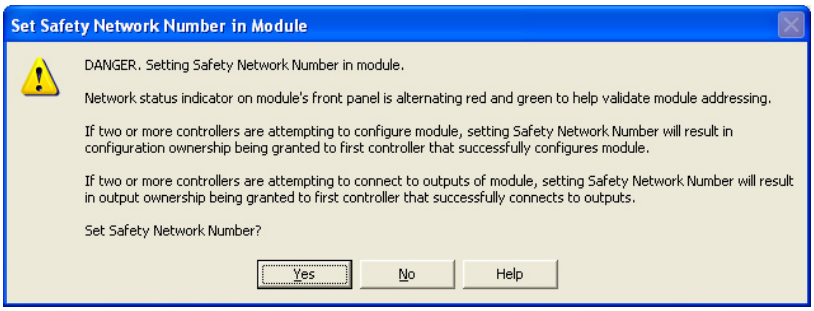
1. Remove the old I/O device and install the new device.
2. Right-click the replacement safety I/O device and choose Properties.
3. To open the Safety Network Number dialog box, click ... to the right of the safety network number.



4. Click Set.



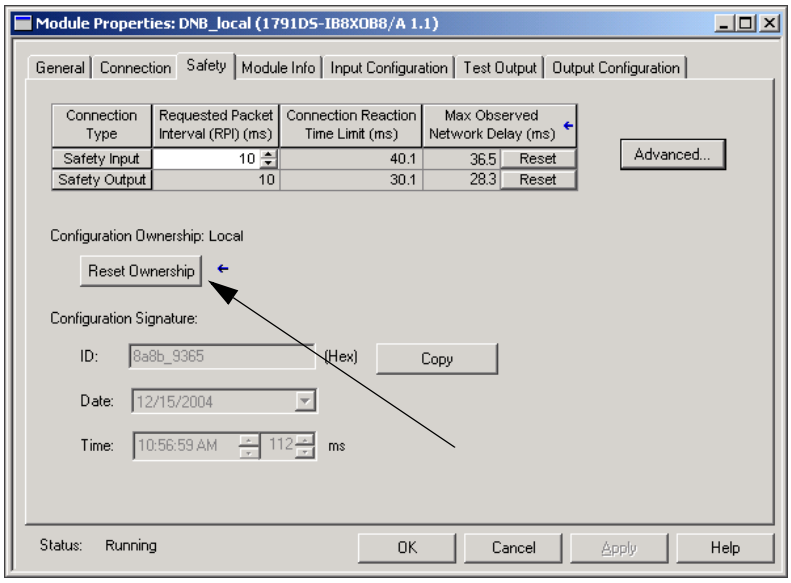
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.



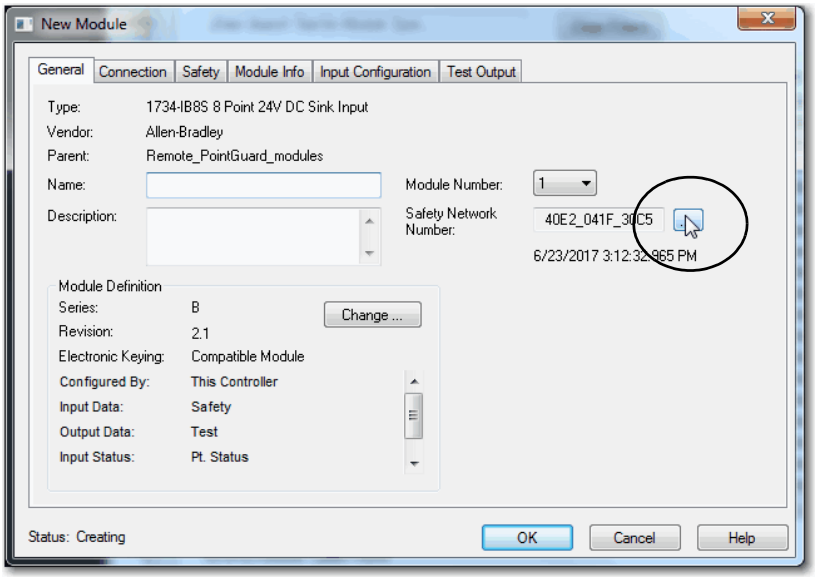
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

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

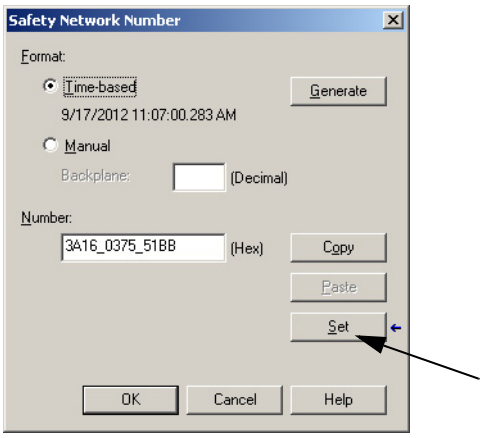
1. Remove the old I/O device and install the new device.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.
4. Click Reset Ownership.



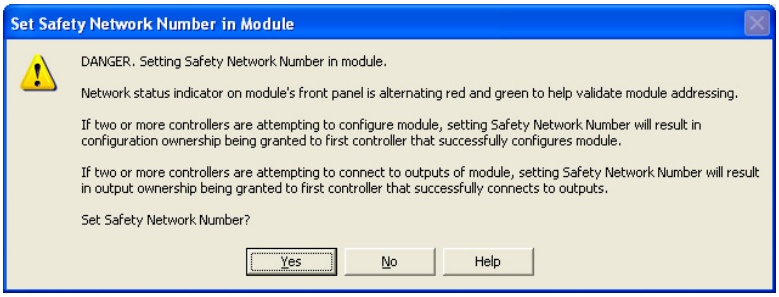
5. Click OK.
6. Right-click the device and choose Properties.
7. To open the Safety Network Number dialog box, click ... to the right of the safety network number.



8. Click Set.



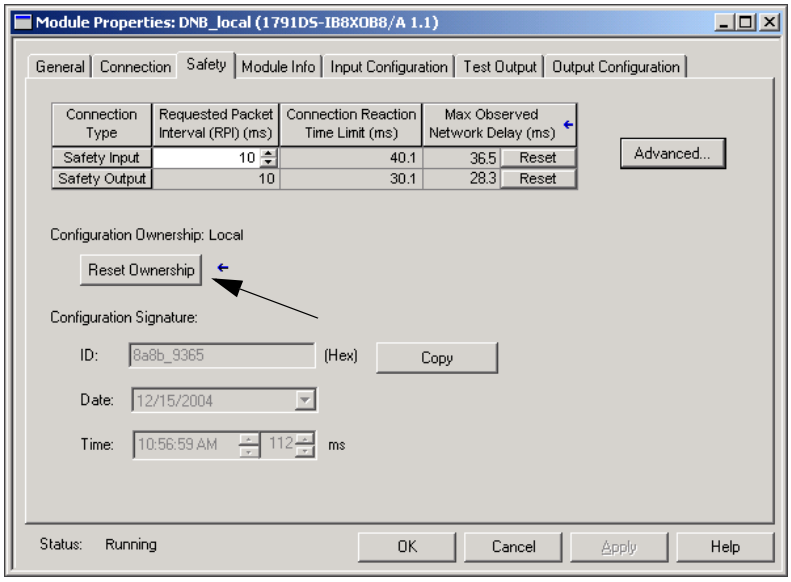
9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.



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

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

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



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

Replacement with 'Configure Always' Enabled

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

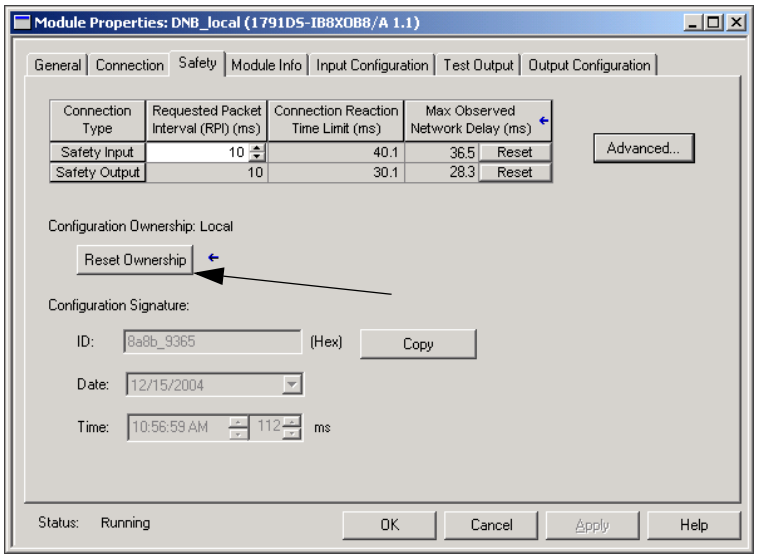
Do not place devices that are in the out-of-box condition on a CIP Safety network when the Configure Always feature is enabled, except while following this replacement procedure.

When the 'Configure Always' feature is enabled in the controller project, the controller automatically checks for and connects to a replacement device that meets all of 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 project is configured for 'Configure Always', follow the appropriate steps to replace a safety I/O device.

1. Remove the old I/O device and install the new device.
   a. If the device is in out-of-box condition, go to step 6.
   No action is needed for the Compact GuardLogix 5380 controller to take ownership of the device.
   b. If an SNN mismatch error occurs, go to the next step to reset the device to out-of-box condition.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.



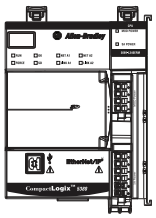
4. Click Reset Ownership.
5. Click OK.
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

Notes:

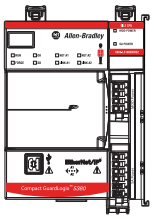
Develop Standard Applications

Elements of a Control Application

CompactLogix



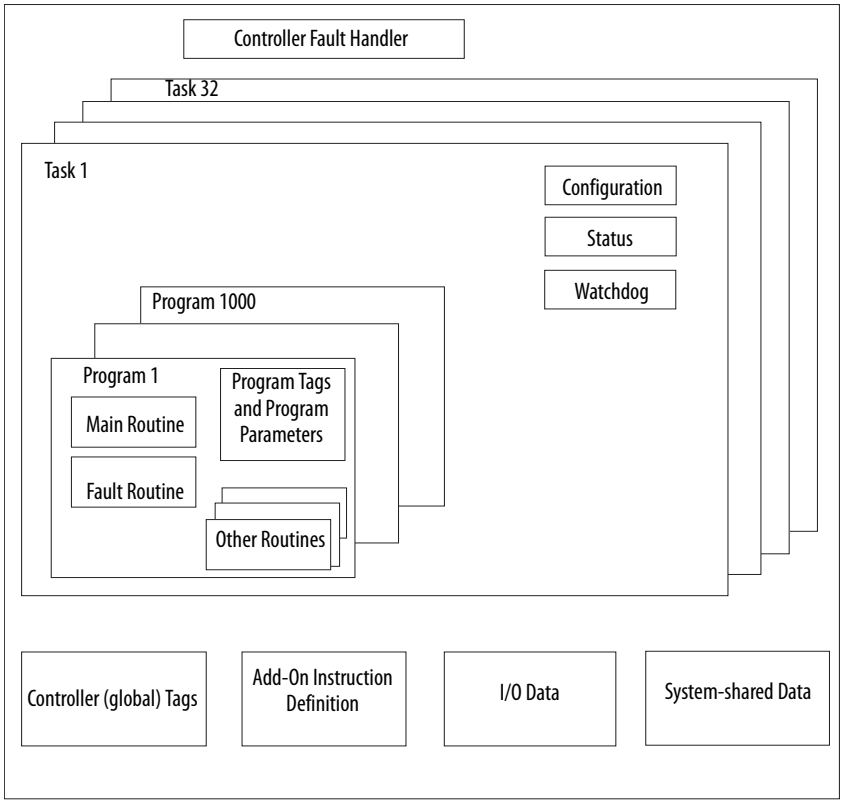
Compact GuardLogix



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 37 - 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.

TIP A large number of tasks can make it difficult to optimally tune your system.

Figure 38 - Task Within a Control Application

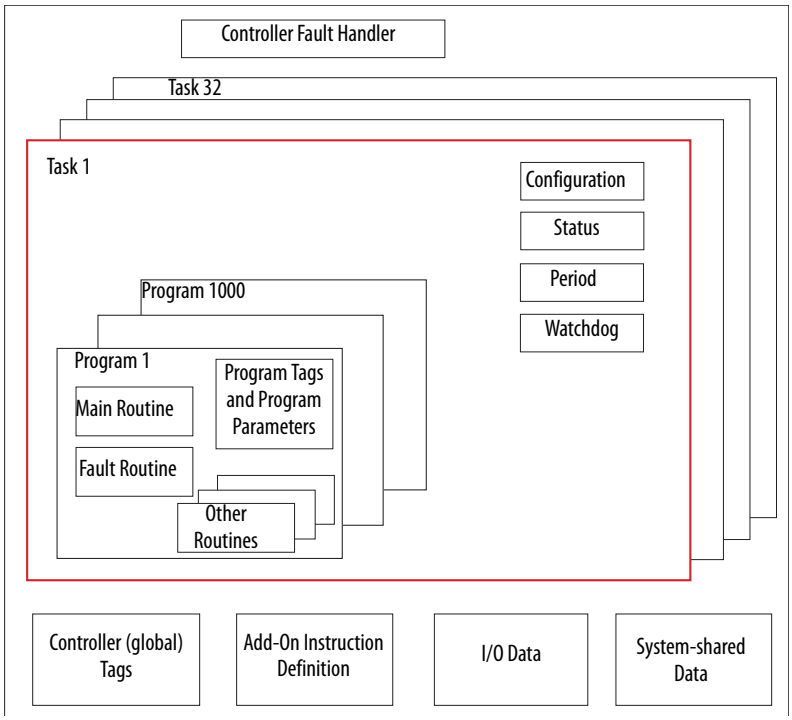
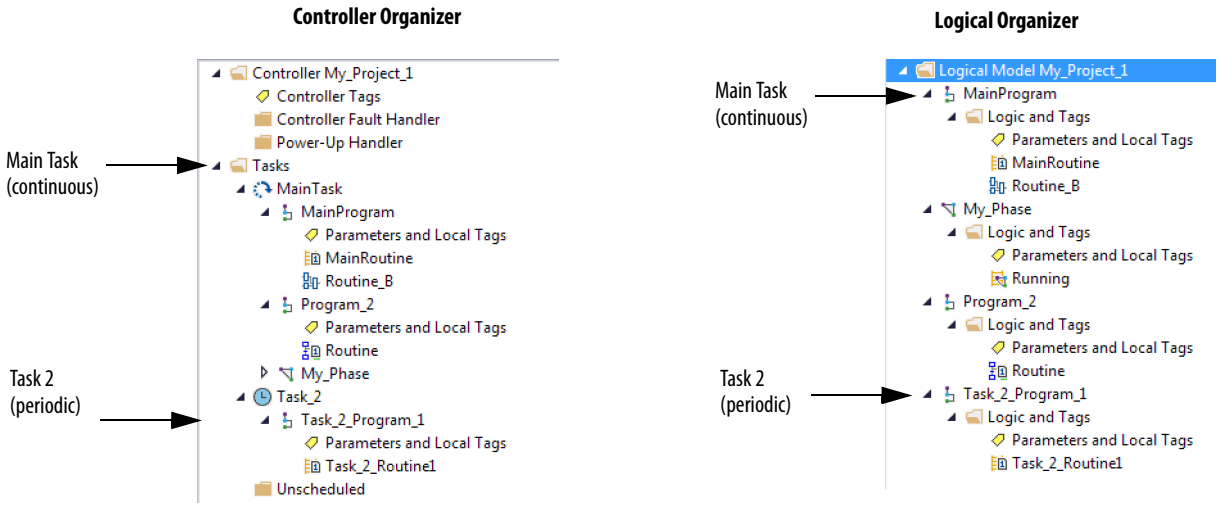


Figure 39 - Tasks



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 40 - Configuring the Task Type

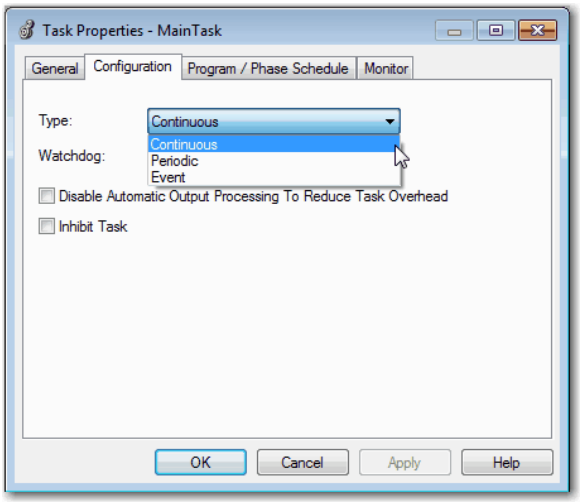


Table 25 explains the types of tasks you can configure.

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

TIP 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

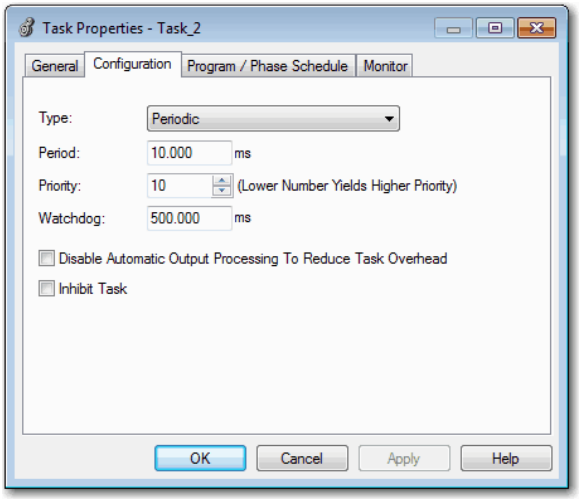
Each task in the controller has a priority level. The operating system uses the priority level to determine which task to execute when multiple tasks are triggered. A higher priority task interrupts any lower priority task. The continuous task has the lowest priority and a periodic or event task interrupts 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 41 - Configure Task Priority



Programs

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

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

Each program contains the following:

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

Figure 42 - Program Within a Control Application

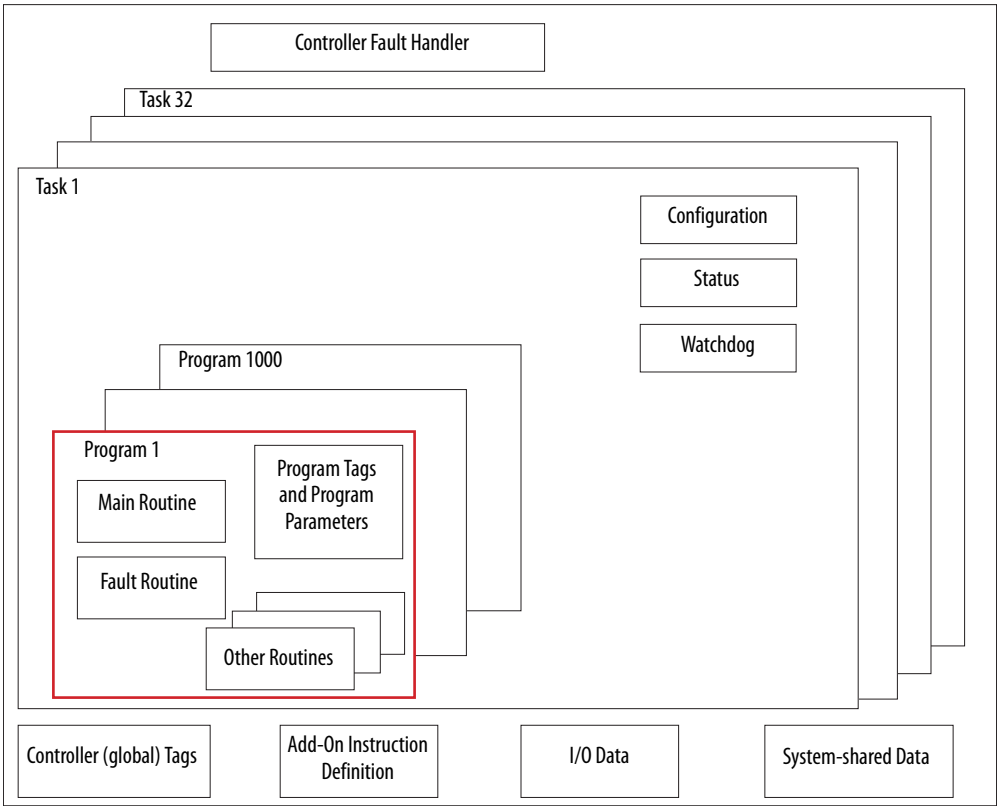
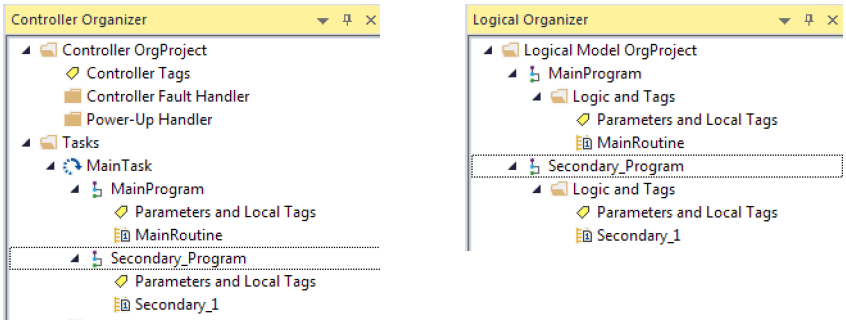


Figure 43 - Programs



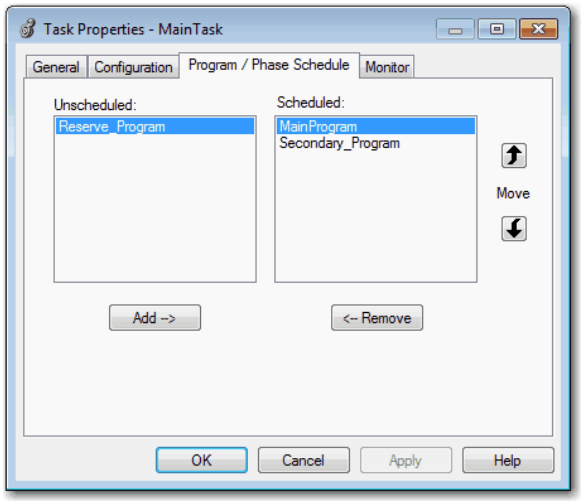
Scheduled and Unscheduled Programs

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

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

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

Figure 44 - Scheduling an Unscheduled 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 45 - Routines in a Control Application

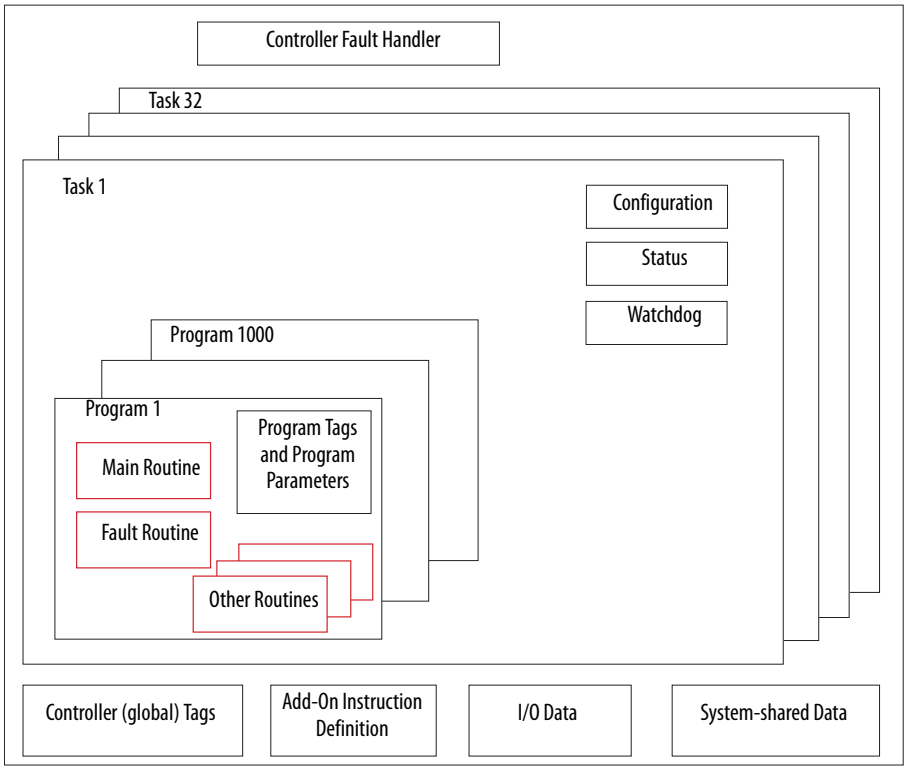
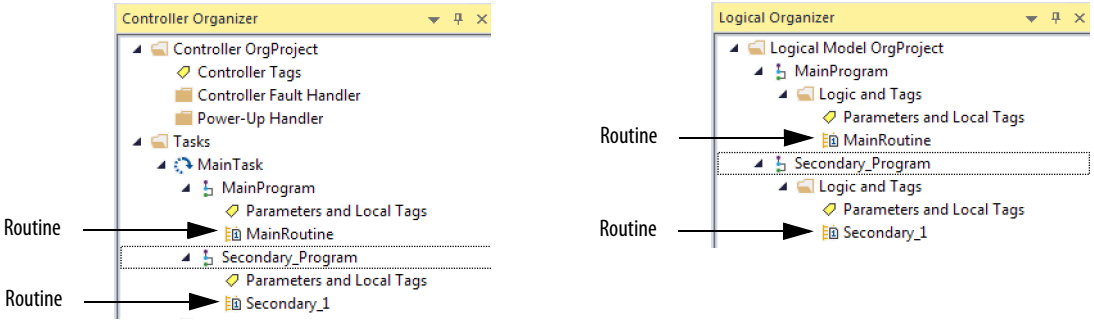


Figure 46 - Routines



Parameters and Local Tags

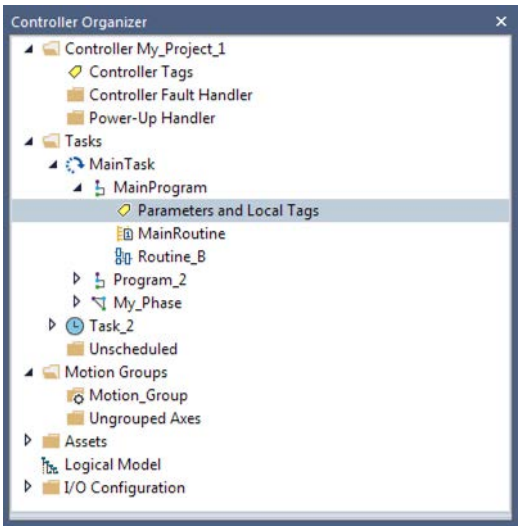
With a Logix 5000™ controller, you use a tag (alphanumeric name) to address data (variables). In Logix 5000 controllers, there is no fixed, numeric format. The tag name identifies the data and lets you do the following:

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

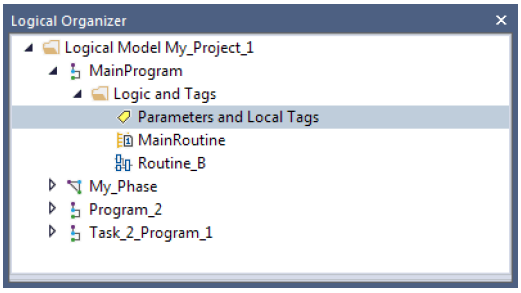
This example shows data tags that are created within the scope of the Main Program of the controller.

Figure 47 - Tags Example

Controller Organizer —Main Program Parameters and Local Tags



Logical Organizer —Main Program Parameters and Local Tags



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

Analog I/O Device

Integer Value
Storage Bit
Counter
Timer

Digital I/O Device

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.

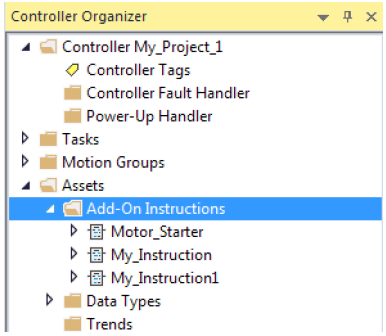
Table 26 - Add-On Instruction Capabilities

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.

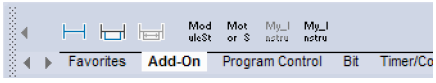
Once defined in a project, Add-On Instructions behave similarly to the built-in instructions in Logix 5000 controllers.

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 48 - Add-On Instructions (Studio 5000 Logix Designer Version 31 Example)



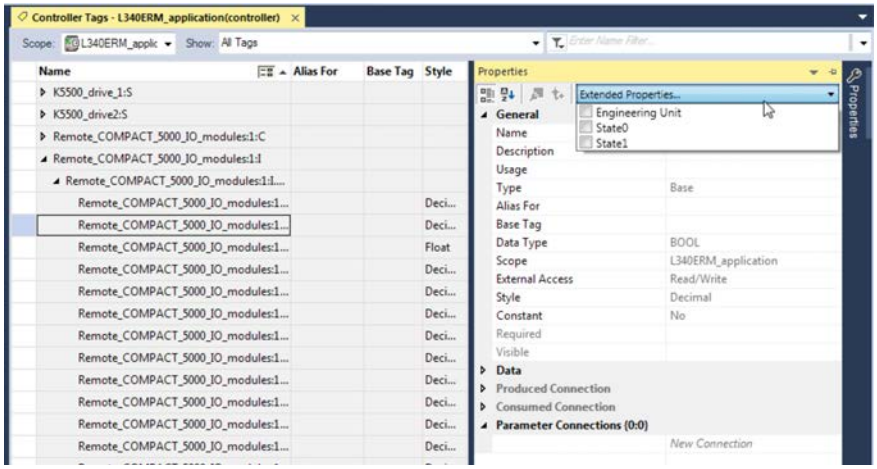
Instruction Toolbar



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.



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.

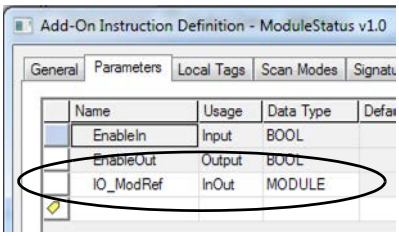
For more information on Extended Properties, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

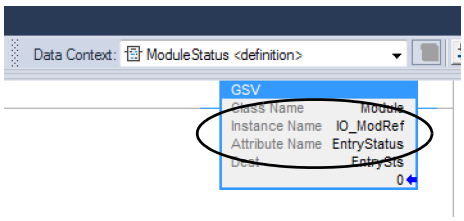
Access the Module Object from an Add-On Instruction

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.





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:

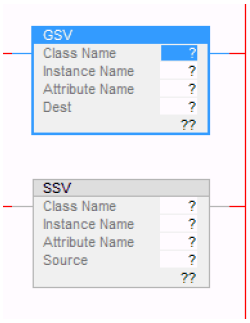
- EntryStatus
- FaultCode
- FaultInfo
- FWSupervisorStatus
- ForceStatus
- Instance
- LEDStatus
- Mode
- Path

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 49 - GSV and SSV Instructions for Monitoring and Setting Attributes



When you add a GSV/SSV instruction to the program, the object classes, object names, and attribute names for the instruction are shown. For the GSV instruction, you can get values for the available attributes. For the SSV instruction, only the attributes 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 Rockwell Automation® Knowledgebase for answer ID 38535: http://www.rockwellautomation.com/knowledgebase.

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

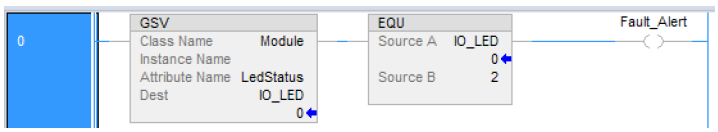
For more information about I/O faults, see the Logix 5000 Controllers Major, Minor, and I/O Faults Programming Manual, publication 1756-PM014.

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 50 - GSV Used to Identify I/O Timeout



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 Monitor Safety Connections on page 269.

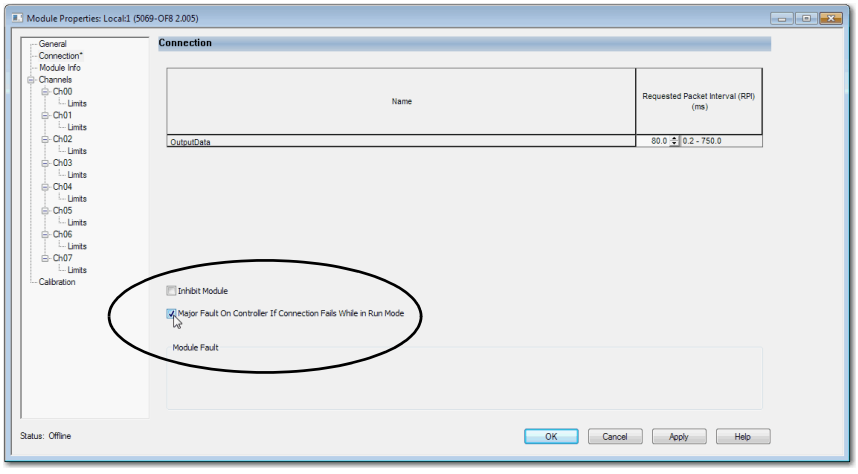
Automatic Handling of I/O Module Connection Faults

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 Safety Applications on page 241.

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 51 - I/O Connection Fault Causes Major Fault



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 237 to call the logic.

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

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

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

Sample Controller Projects

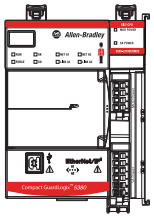
Logix Designer includes sample projects that you can copy and modify to fit your application. To access the sample projects, choose Sample Project in the Studio 5000® interface.

Figure 52 - Opening Sample Projects

Notes:

Develop Safety Applications

Compact GuardLogix



This chapter explains the components that constitute a safety project and provides information on using features that help protect safety application integrity, such as the safety signature and safety-locking.

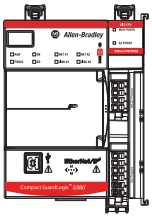
The GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012 addresses the following topics:

- Guidelines and requirements for developing and commissioning SIL 2/PLd 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 necessary
- Locking the safety application
- Calculating system reaction time

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

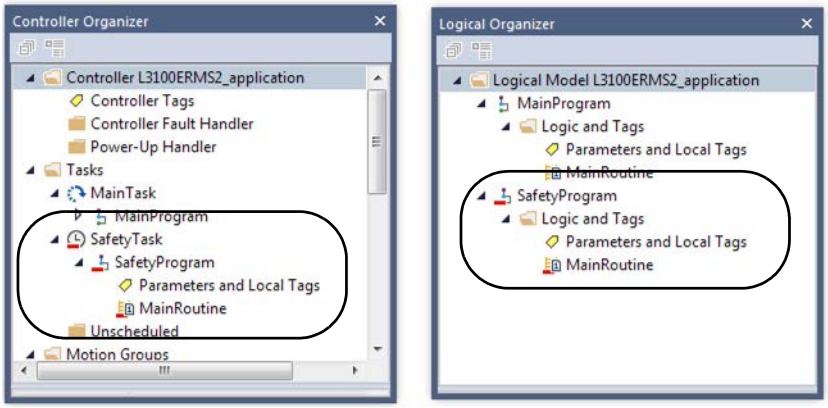
Safety Task

Compact GuardLogix



When you create a safety controller project, the Studio 5000 Logix Designer® application automatically creates a safety task with a safety program and a main (safety) routine.

Figure 53 - Safety Task in the Controller Organizer and Logical Organizer



Within the safety task, you can use multiple safety programs, which are composed of multiple safety routines. The Compact GuardLogix® 5380 controllers support one safety task. The safety task cannot be deleted.

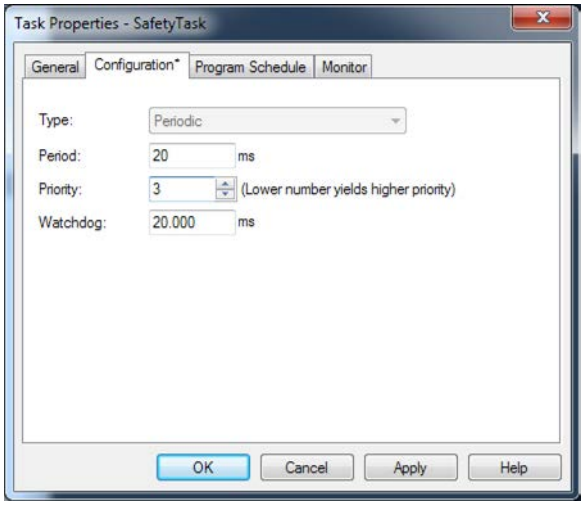
You cannot schedule standard programs or execute standard routines within the safety task.

Safety Task Period

The safety task is a periodic timed task. You set the task priority and watchdog time via the Task Properties - Safety Task dialog box.

To open the dialog box, right-click the Safety Task and choose Properties.

Figure 54 - Configure the Safety Task Period



To get the most consistent safety task execution time, and to minimize safety task watchdog faults, we recommend running the safety task as the highest priority user task.

You specify the safety task period (in ms) and the safety task watchdog (in ms). The safety task period is the elapsed time between successive starting times for the safety task. The safety task watchdog is the maximum time allowed from the start of safety task execution to its completion.

The safety task period is limited to a maximum of 500 ms and cannot be modified online. Be sure that the safety task has enough time to finish logic execution before it is triggered again. If a safety task watchdog timeout occurs, a nonrecoverable safety fault is generated in the safety controller.

The safety task period directly affects system reaction time.

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

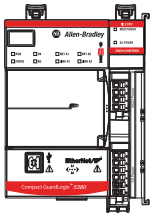
Safety Task Execution

The safety task executes in the same manner as a standard periodic task, with these exceptions:

- All safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution. For more information on safety tag mapping, see page 256.
- Safety output packets (produced tags and output modules) are generated at the conclusion of safety task execution.
- When the controller does not have a safety signature and is not safety locked, the safety task can be held off until an online edit of a safety element completes.

Safety Programs

Compact GuardLogix

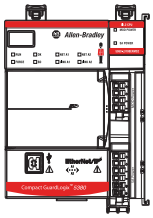


Safety programs have all attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines. One safety routine must be designated as the main routine, and another safety routine can be designated as the fault routine.

Safety programs cannot contain standard routines or standard tags.

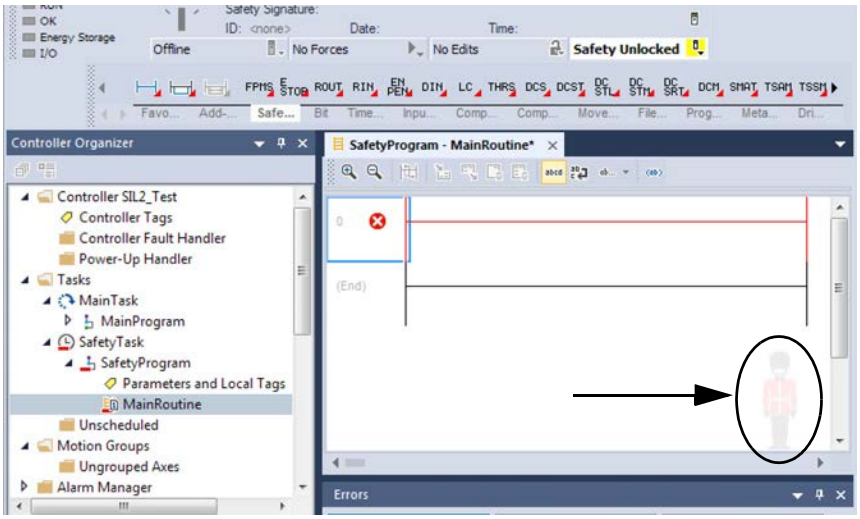
Safety Routines

Compact GuardLogix



Safety routines have all attributes of standard routines, except that they exist only in a safety program. Only ladder diagram is supported for safety routines

A watermark feature visually distinguishes a safety routine from a standard routine.



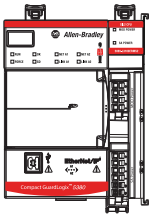
Safety Add-On Instructions

You can create safety Add-On Instructions to be used in Safety applications. Safety Add On Instructions feature a safety instruction signature for use in safety-related applications up to and including SIL 2-rated applications.

For more information, see the Logix 5000 Controllers Add On Instructions Programming Manual, publication 1756-PM010.

Safety Tags

Compact GuardLogix



Safety tags have all attributes of standard tags with the addition of mechanisms that are certified to provide SIL 2/PLd data integrity.

When you create a tag, you assign the following properties:

- Name
- Description (optional)
- Tag type
- Data type
- Scope
- Class
- Style
- External Access
- If the tag value is a constant

IMPORTANT You cannot create a standard alias tag of a safety tag. Instead, standard tags can be mapped to safety tags using safety tag mapping. See Safety Tag Mapping on page 256.

The Logix Designer application can write to safety tags directly via the Tag Monitor when the Compact GuardLogix 5380 controller is safety-unlocked, does not have a safety signature, and is operating without safety faults.

The controller does not allow writes to safety tag data from external human machine interface (HMI) devices or via message instructions from peer controllers. HMI devices can have read-only access to safety tags (depending on the External Access setting).

Valid Data Types

The data type defines the type of data that the tag stores, such as bit or integer.

Data types can be combined to form structures. A structure provides a unique data type that matches a specific need. Within a structure, each individual data type is called a member. Like tags, members have a name and data type. You can create your own structures, such as arrays or user-defined data types.

Logix controllers contain predefined data types for use with specific instructions. Safety tags can be composed of the following:

- All primitive data types (for example, BOOL, SINT, INT, DINT, LINT, REAL)
- Predefined types that are used for safety application instructions
- User-defined types or arrays that are composed of the two types above

Scope

The scope of a tag determines where you can access the tag data. When you create a tag, you define it as a controller tag (global data) or a program tag for a specific safety or standard program (local data). Safety tags can be controller-scoped or safety program-scoped.

Controller-scoped safety tags can be read by either standard or safety logic or other communication devices, but can be written by only safety logic or another safety controller. Program-scoped safety tags are accessible only by local safety routines. These are routines that reside within the safety program.

When you create program-scoped tags, the class is automatically specified, depending on whether you created the tag in a standard or a safety program. When you create controller-scoped tags, you must manually select the tag class.

When safety tags are controller-scoped, all programs have access to the safety data. Tags must be controller-scoped if they are used in these ways:

- Multiple programs in the project
- To produce or consume data
- In safety tag mapping

For more information, see Safety Tag Mapping on page 256.

Controller-scoped safety tags can be read, but not written to, by standard routines.

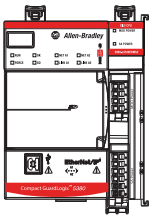
Program Parameters

For program parameters, a safety parameter cannot be connected with or bound to a standard parameter or controller-scoped tag.

For information on program parameters, see Program Parameters on page 232.

Produced/Consumed Safety Tags

Compact GuardLogix



To transfer safety data between Compact GuardLogix 5380 controllers, you use produced and consumed safety tags.

Tags that are associated with safety I/O and produced or consumed safety data must be controller-scoped safety tags. For produced/consumed safety tags, you must create a user-defined data type with the first member of the tag structure that is reserved for the status of the connection. This member is a predefined data type called CONNECTION_STATUS.

Table 27 - Produced and Consumed Connections

Tag	Connection Description
Produced	Compact GuardLogix 5380 controllers can produce (send) safety tags to other GuardLogix controllers. • Compact GuardLogix 5380 controllers only support unicast produced tags. • Compact GuardLogix 5380 controllers do support producing a tag to up to 15 consumers if all consumers are configured to consume the tag unicast. • The producing controller uses one connection for each consumer.
Consumed	Compact GuardLogix 5380 controllers can consume (receive) safety tags from other GuardLogix controllers in these configurations: • If you have a Compact GuardLogix 5380 controller (the producer) in the I/O tree of another Compact GuardLogix 5380 controller (the consumer), then the consumer can only consume a tag from the producer if the tag is unicast. • If the producer controller is a GuardLogix 5570 controller, then a Compact GuardLogix 5380 consumer controller can consume multicast or unicast tags. • Each consumed tag consumes one connection.

Produced and consumed safety tags are subject to these restrictions:

- Only controller-scoped safety tags can be shared.
- Produced and consumed safety tags are limited to 128 bytes.
- Produced/consumed tag pairs must be of the same user-defined data type.
- The first member of that user-defined data type must be the predefined CONNECTION_STATUS data type.
- The requested packet interval (RPI) of the consumed safety tag must match the safety task period of the producing Compact GuardLogix 5380 controller.

To properly configure produced and consumed safety tags to share data between peer safety controllers, you must properly configure the peer safety controllers, produce a safety tag, and consume a safety tag, as described in this section.

Configure the SNN for a Peer Safety Controller Connection

The peer safety controller is subject to the same configuration requirements as the local safety controller. The peer safety controller must also have a safety network number (SNN).

The safety application that is downloaded into the peer safety controller configures SNN values for each CIP Safety port on the controller.

Table 28 - SNN and Controller Placement

Peer Safety Controller Location	SNN
Placed in the local chassis	The user application on the peer controller generates an SNN value for the local backplane port of the controller.
Placed in another chassis	The controller must have a unique SNN.

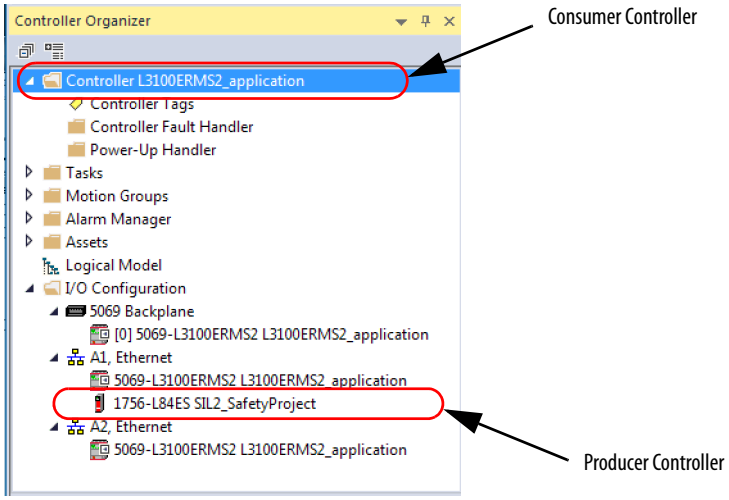
For an explanation of the Safety Network Number, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

If the automatically assigned SNN of the producer controller does not match the SNN the controller actually uses, you can follow these steps to copy and paste the SNN.

TIP When set the correct SNNs of the controller as described in Assign the Safety Network Number (SNN) on page 88, it results in the producer controller being assigned the correct SNN. In these cases, you need not perform this procedure.

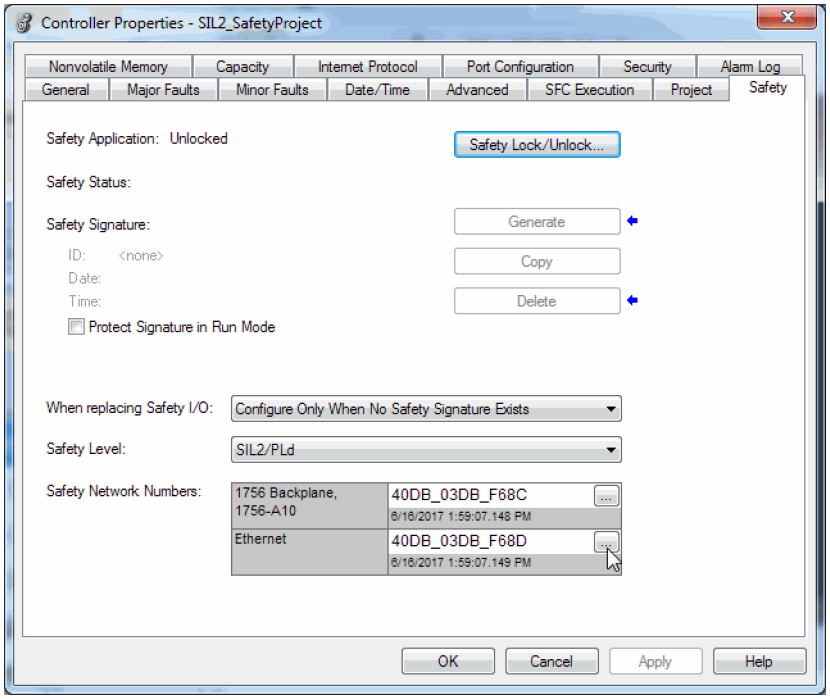
1. Add the producer controller to the I/O tree of consumer controller.

   In this example, the producer controller is accessed via an EtherNet/IP network through the A1 Ethernet port. Set the A1 port SNN to the same SNN as the Ethernet port SNN from the SIL2_SafetyProject.

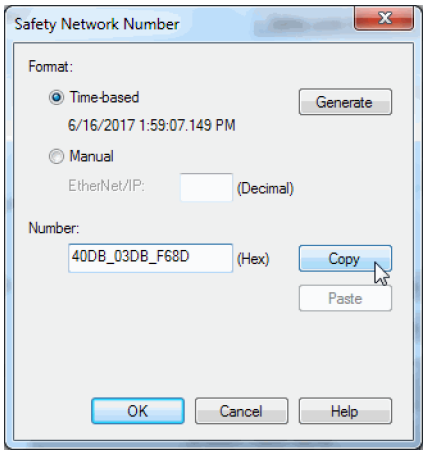


2. In the producer controller project, right-click the producer controller and choose Controller Properties.

3. On the Safety tab, click the ... next to the port (Ethernet or Backplane) that communicates with the consumer controller. This opens the Safety Network Number dialog box.

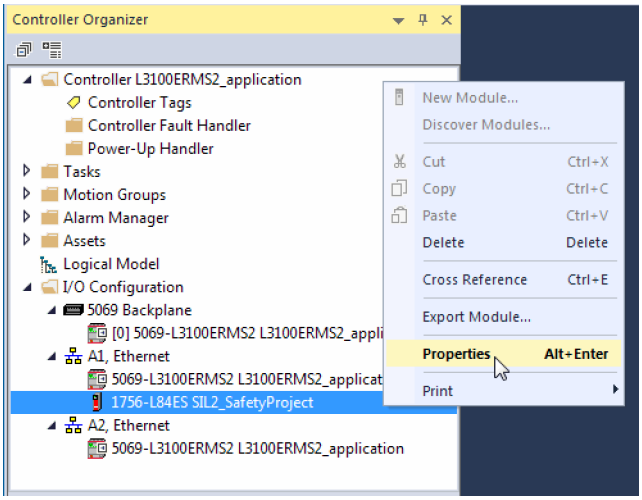


4. Copy the producer controller SNN.

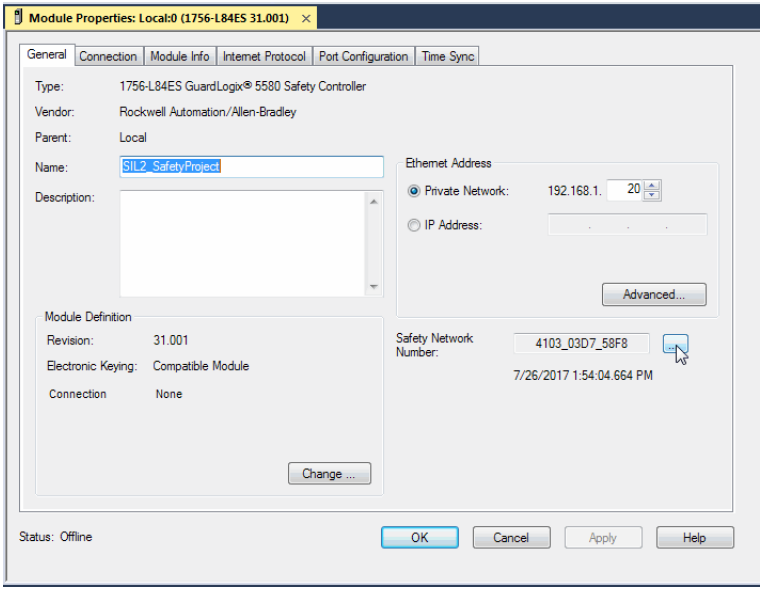


TIP You can also copy the SNN directly from the Safety Tab. On the Safety tab, select the cell with the SNN. Right-click and select Copy (or press Ctrl-C).

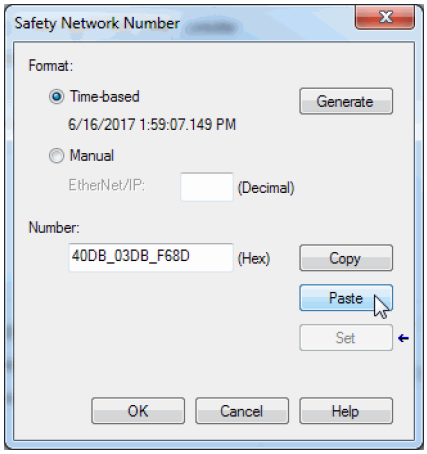
5. In the I/O tree of the consumer controller project, right-click on the module that represents the producing controller, and choose Properties.



6. On the Module Properties General tab, click ... to open the Safety Network Number dialog.

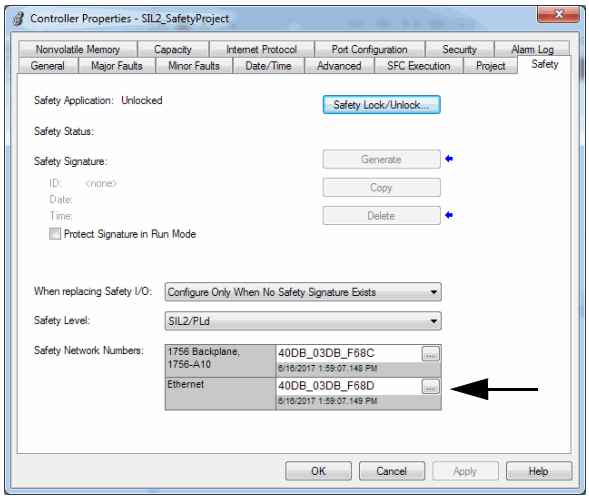


7. Paste the producer controller SNN into the SNN field and click OK.

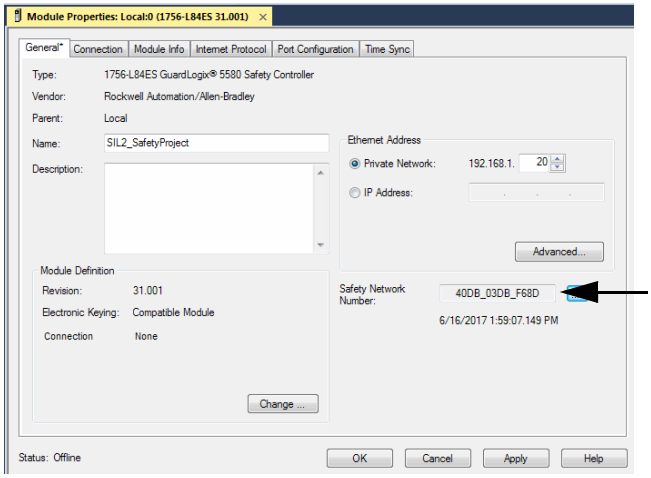


The safety network numbers match.

Producer Controller Properties Dialog Box in Producer Project



Producer Module Properties Dialog Box in Consumer Project



Produce a Safety Tag

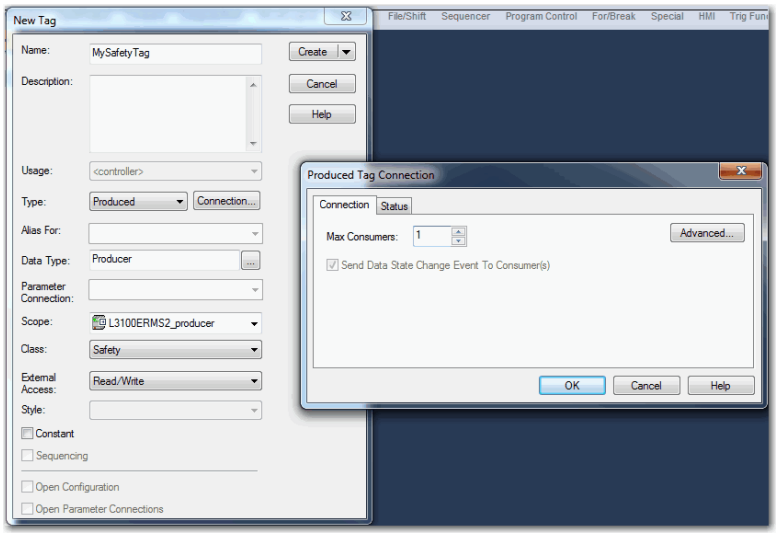
Complete these steps to produce a safety tag.

1. In the producing controller project, create a user-defined data type defining the structure of the data to be produced.

   Make sure that the first data member is of the CONNECTION_STATUS data type.

   For more information on the CONNECTION_STATUS data type, see Monitor Safety Connections on page 269

2. Right-click Controller Tags and choose New Tag.
3. Set the type as Produced, the class as Safety, and the Data Type to the user-defined data type you created in step 1.
4. Click Connection and enter the max limit on the number of consumers (1...15).



5. Click OK.
6. Click Create.

Consume Safety Tag Data

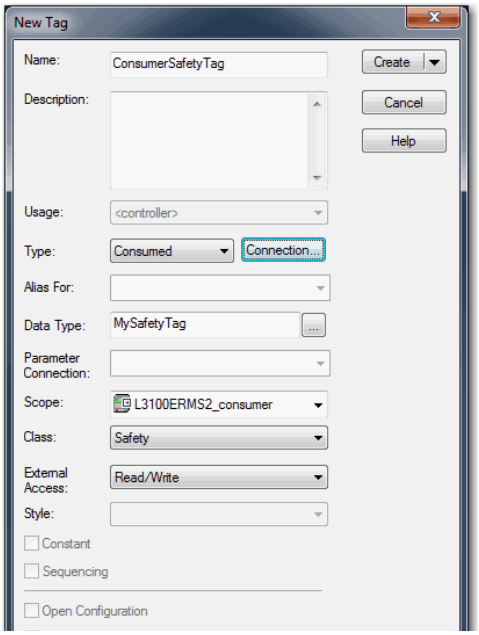
Follow these steps to consume data that is produced by another controller.

IMPORTANT Logix Designer does not download a project if you try to consume a safety tag from a remote controller that has disable keying enabled.

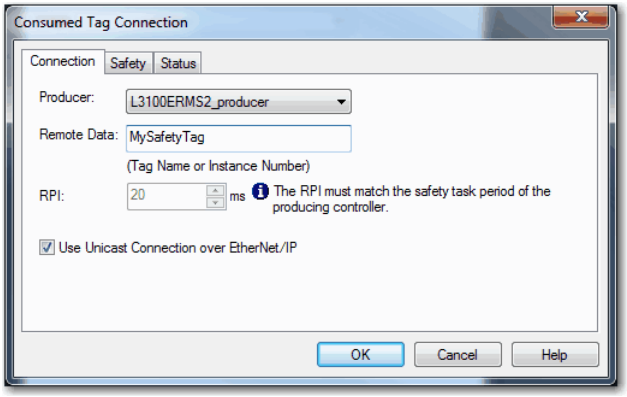
1. In the consumer controller project, create a user-defined data type identical to the one created in the producer project (the names of the user-defined data types must match).

   TIP The user-defined data type can be copied from the producer project and pasted into the consumer project.

2. Right-click Controller Tags and choose New Tag.
3. Set the Type as Consumed, the Class as Safety, and the Data Type to the user-defined data type you created in step 1.



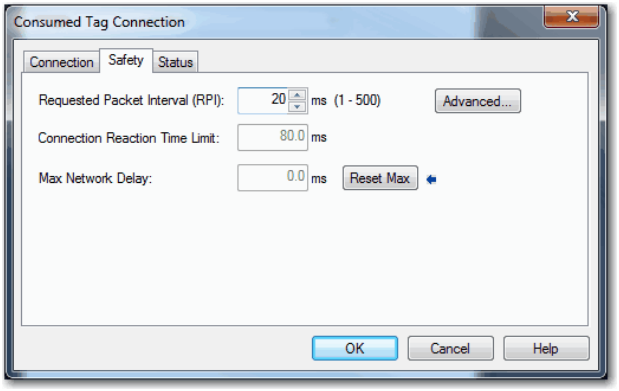
4. Click Connection to open the Consumed Tag Connection dialog box.



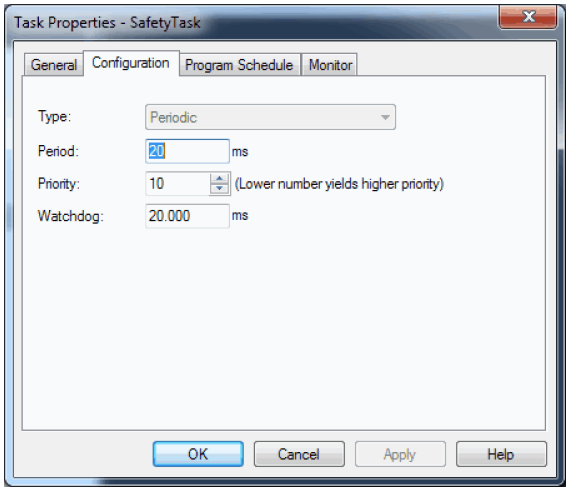
5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.
7. Click the Safety tab.
8. In the Requested Packet Interval (RPI) field, enter the RPI for the connection in 1 ms increments. The default is 20 ms.

- The RPI specifies the period when data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.

Consumer Project



Producer Project

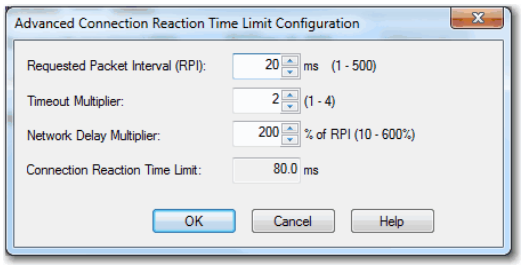


- The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, you can achieve an acceptable Connection Reaction Time Limit by adjusting the safety task period of the producing controller, which adjusts the RPI.
- The Max Network Delay is the maximum observed transport delay from the time the data was produced until the time the data was received. When online, click Reset Max to reset the Max Network Delay.

9. If the Connection Reaction time limit is acceptable, click OK.

TIP If a safety consumed tag has the error code: "16#0111 Requested Packet Interval (RPI) out of range," check that the consumed tag RPI matches the producer safety task period.

10. If your application has more complex requirements, click Advanced on the Safety tab to access the Advanced Connection Reaction Time Limit parameters.



- The Timeout Multiplier determines the number of RPIs to wait for a packet before declaring a connection timeout.

- The Network Delay Multiplier defines the message transport time that is enforced by the CIP Safety protocol. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and back to the producer.

  You can use the Network Delay Multiplier to increase or decrease the Connection Reaction Time Limit.

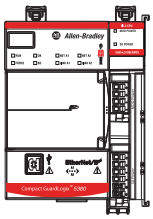
ATTENTION: If you decrease the timeout multiplier or network delay multiplier below the defaults, this could cause nuisance safety connection losses. If you use wireless networks, you may need to increase the values above the default.

Table 29 - More Resources

Resource	Description
Connection Reaction Time Limit on page 208	Provides more information on how to set the RPI and understand how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time
Monitor Safety Connections on page 269	Contains information on the CONNECTION_STATUS predefined data type
Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011	Provides detailed information on using produced and consumed tags

Safety Tag Mapping

Compact GuardLogix



A safety routine cannot directly access standard tags. To allow standard tag data to be used within safety task routines, the Compact GuardLogix 5380 controllers provide a safety tag mapping feature that lets standard tag values be copied into safety task memory.

Mapped tags are copied from the standard tags to their corresponding safety tags at the beginning of the safety task. This can increase the safety task scan time.

TIP Standard task routines can directly read safety tags.

Restrictions

Safety tag mapping is subject to these restrictions:

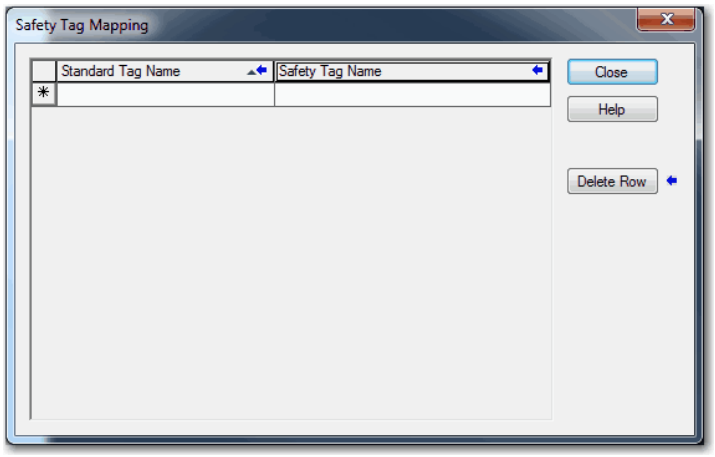
- The safety tag and standard tag pair must be controller-scoped.
- The data types of the safety and standard tag pair must match.
- Alias tags are not allowed.
- Mapping must take place at the whole tag level. For example, myTimer.pre is not allowed if myTimer is a TIMER tag.
- A mapping pair is one standard tag mapped to one safety tag.
- You cannot map a standard tag to a safety tag that has been designated as a constant.
- Tag mapping cannot be modified when the following is true:
  - The project is safety-locked.
  - A safety signature exists.
  - The key switch is in RUN position.
  - A nonrecoverable safety fault exists.

ATTENTION: When you use standard data in a safety routine, you must verify that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 2/PLd safety output with standard tag data.

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

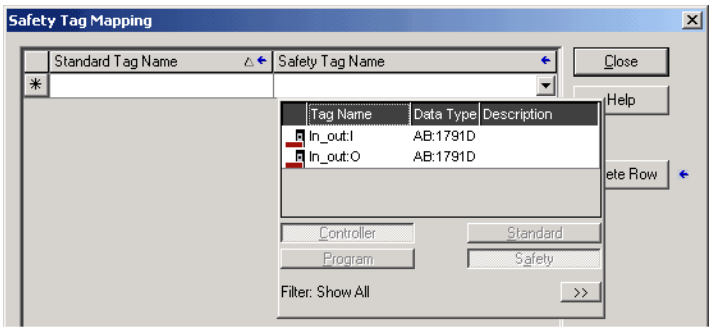
Create Tag Mapping Pairs

1. To open the Safety Tag Mapping dialog box, choose Map Safety Tags from the Logic menu.



2. Add an existing tag to the Standard Tag Name or Safety Tag Name column by typing the tag name into the cell, or choose a tag from the pull-down menu.

   Click the arrow to display a filtered tag browser dialog box. If you are in the Standard Tag Name column, the browser shows only controller-scoped standard tags. If you are in the Safety Tag Name column, the browser shows controller-scoped safety tags.



3. To add a new tag to the Standard Tag Name or Safety Tag Name column:
   a. Right-click in the empty cell and select New Tag.
   b. Type the tag name into the cell.
4. Right-click in the cell and choose New tagname, where tagname is the text you entered in the cell.

Monitor Tag Mapping Status

The leftmost column of the Safety Tag Mapping dialog box indicates the status of the mapped pair.

Table 30 - Tag Mapping Status Icons

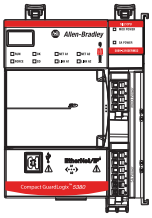
Cell Contents	Description
Empty	Tag mapping is valid.
	When offline, the X icon indicates that tag mapping is invalid. You can move to another row or close the Safety Tag Mapping dialog box.(1) When online, an invalid tag map results in an error message explaining why the mapping is invalid. You cannot move to another row or close the Safety Tag Mapping dialog box if a tag mapping error exists.
	Indicates the row that currently has the focus.
	Represents the Create New Mapped Tag row.
	Represents a pending edit.

(1) Tag mapping is also checked during project verification. Invalid tag mapping results in a project verification error.

For more information, see the tag mapping restrictions on page 256.

Safety Application Protection

Compact GuardLogix



You can help protect your application program from unauthorized changes by generating a safety signature, setting passwords, and safety-locking the controller.

Safety-lock the Compact GuardLogix 5380 Controller

ATTENTION: Safety-locking alone does not satisfy SIL 2/PLd requirements.

To help protect safety-related control components from modification, and help prevent the safety signature from being deleted accidentally, you can safety-lock the controller and set passwords to lock and unlock the controller.

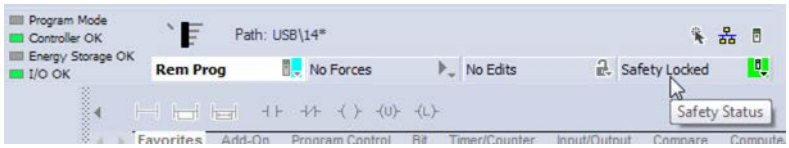
IMPORTANT If the application is configured to load from the SD card on power up, then the application in the controller is overwritten even if the controller is safety locked.

The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety Add-On Instructions, safety tags, safety I/O, and the safety signature.

You can modify all standard components while the controller is safety locked.

TIP There are multiple ways to view the safety lock status of the controller:

- The 4-character display on the controller indicates lock status.
- In the Logix Designer application, the text of the online bar Safety Status button indicates the safety-lock status.



- The Logix Designer application tray also displays the following icons to indicate the safety controller safety-lock status.

  = controller safety-locked

  = controller safety-unlocked

You can safety-lock the controller project regardless of whether you are online or offline and regardless of whether you have the original source of the program. However, no safety forces or pending online safety edits can be present.

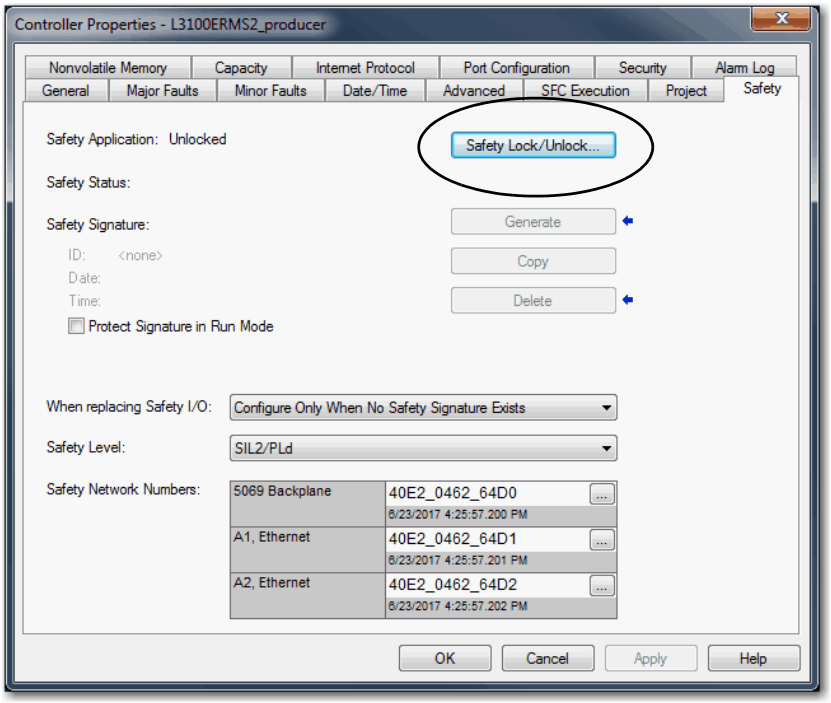
You cannot change the Safety-locked or -unlocked status when the controller mode switch is in the RUN position.

TIP Safety-lock or -unlock actions are logged in the controller log.

For more information on how to access the controller log, refer to the Logix 5000 Controllers Controller Information and Status Programming Manual, publication 1756-PM015.

You can safety-lock and -unlock the controller from the Safety tab of the Controller Properties dialog box.

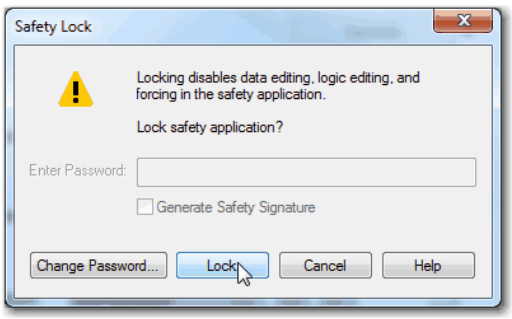
Figure 55 - Safety-locking the Controller



TIP In the Logix Designer application, you can also choose Tools > Safety > Safety Lock/Unlock.

If you set a password for the safety-lock feature, you must type it in the Enter Password field. Otherwise, click Lock.

Figure 56 - Safety-locking the Controller



You can also set or change the password from the Safety Lock dialog box. See Set Passwords for Safety-locking and Unlocking on page 261.

The safety-lock feature, described in this section, and standard security measures in the Logix Designer application are applicable to Compact GuardLogix controller projects.

See the Logix 5000 Controllers Security Programming Manual, publication 1756-PM016, for information on Logix Designer security features.

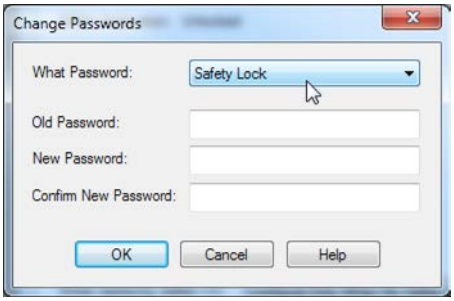
Set Passwords for Safety-locking and Unlocking

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

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

Follow these steps to set passwords.

1. On the Logix Designer menu bar, click Tools > Safety > Change Passwords.
2. From the What Password pull-down menu, choose either Safety Lock or Safety Unlock.



3. Type the old password, if one exists.
4. Type and confirm the new password.
5. Click OK.

TIP Passwords can be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols can be used: ' ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .

To clear an existing password, enter a new password of zero length.

Generate the Safety Signature

IMPORTANT To generate a signature, the controller must be in Program mode.

Before verification testing, you must generate the safety signature. You can generate the safety signature only when these conditions exist:

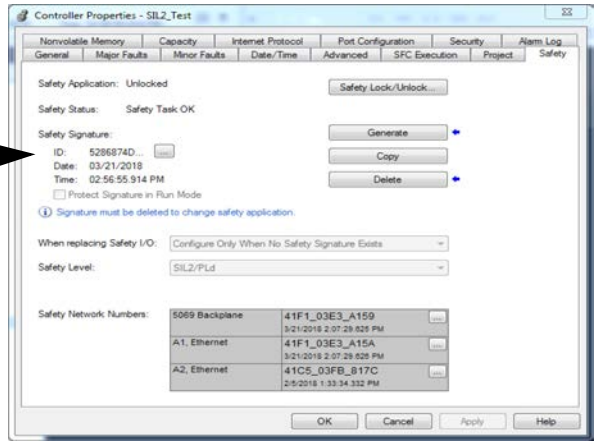
- The safety-unlocked Compact GuardLogix 5380 controller project is online.
- There are no safety forces, pending online safety edits, or safety faults.
- The safety status must be Safety Task OK.

TIP You can view the safety status via the safety status button on the online bar on the Safety tab of the Controller Properties dialog box.

To generate the safety signature from the Safety tab of the Controller Properties dialog box, click Generate.

Figure 57 - Generate Safety Signature

For the safety signature, Compact GuardLogix 5380 controllers have a 32 byte ID. Only the first 4 bytes of the ID display on the tab. To view and copy the entire 32 byte ID, click ... to open the Safety Signature ID dialog box.



TIP In the Logix Designer application, you can also choose Tools > Safety > Generate Signature.

If a previous signature exists, you are prompted to overwrite it.

TIP Safety signature creation and deletion is logged in the controller log.

For more information on how to access the controller log, refer to Logix 5000 Controllers Controller Information and Status Programming Manual, publication 1756-PM015.

When a safety signature exists, these actions are not permitted in the safety portion of the application:

- Online/offline programming or editing (including safety Add-On Instructions).
- Force safety I/O.
- Change the inhibit state of safety I/O modules or producer controllers.
- Manipulate safety data (except by safety routine logic).
- Download a new safety application only if the controller is locked.

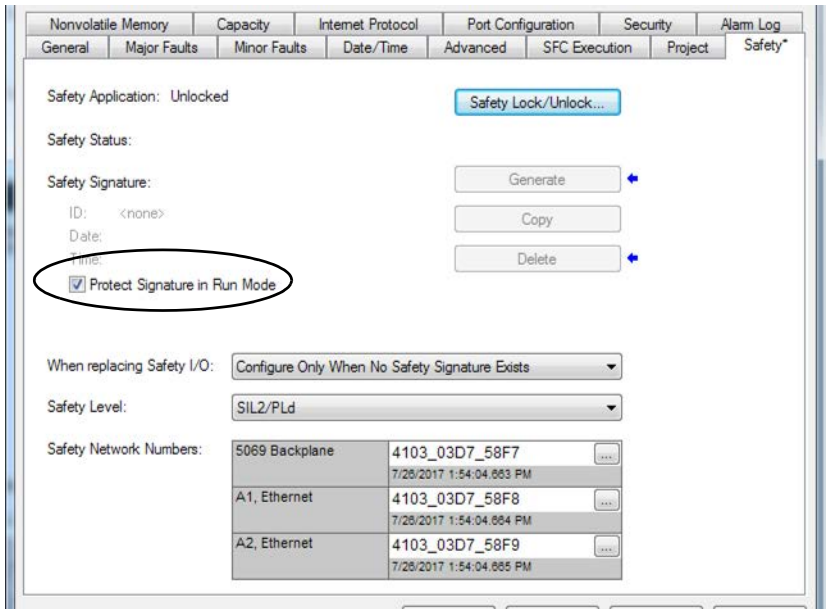
Protect the Safety Signature in Run Mode

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

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

Follow these steps to protect the safety signature:

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



Copy the Safety Signature

You can use the Copy button to create a record of the safety signature for use in safety project documentation, comparison, and validation.

Click Copy to copy the ID, Date, and Time components to the Windows clipboard.

Delete the Safety Signature

Click Delete to delete the safety signature. The safety signature cannot be deleted when these are true:

- The controller is safety-locked.
- The controller is in Run mode with the mode switch in RUN.
- The controller is in Run or Remote Run mode with Protect Signature in Run Mode enabled.

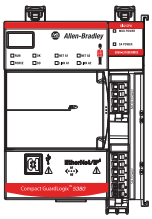
ATTENTION: If you delete and then generate a new safety signature, you must retest and revalidate your system to meet SIL 2/PLd requirements.

Without a safety signature, the controller is not SIL2/PLd capable.

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

Programming Restrictions

Compact GuardLogix



The Logix Designer application imposes restrictions that limit the availability of some menu items and features (such as cut, paste, delete, search and replace). These restrictions help protect safety components from being modified whenever at least one of these are true:

- The controller is safety-locked.
- A safety signature exists.
- Safety faults are present.

IMPORTANT The maximum and last scan times of the safety task and safety programs can be reset when online.

If even one of these conditions apply, you cannot do the following:

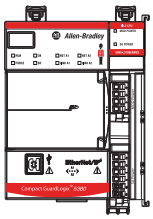
- Create or modify safety objects, including safety programs, safety routines, safety tags, safety Add-On Instructions, and safety I/O devices.
- Apply forces to safety tags.
- Create new safety tag mappings.
- Modify or delete tag mappings.
- Modify or delete user-defined data types that are used by safety tags.
- Modify the controller name, description, chassis type, slot, and safety network number.
- Create, modify, or delete a safety connection.

When the controller is safety-locked, you cannot modify or delete the safety signature.

For a program parameter, a safety parameter cannot be connected with, or bound to, a standard parameter or controller-scoped tag.

Monitor Safety Status

Compact GuardLogix



You can use the following to monitor the controller status:

- Online bar in the Logix Designer application
- Safety tab in the Controller Properties dialog box

View Status Via the Online Bar

The online bar displays project and controller information, including the controller status, force status, online edit status, and safety status.

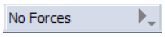
Figure 58 - Status Buttons

Controller Status

When the Controller Status button  is selected as shown above, the online bar shows the controller mode (Remote Program) and status (OK). The Energy Storage OK indicator combines the status of the primary controller and the safety partner.

If either or both have an energy storage fault, the status indicator illuminates. The I/O indicator combines the status of standard and safety I/O. The I/O with the most significant error status is displayed next to the status indicator.

Forces Status

The Forces Status button  indicates Forces or No Forces. When the button is selected, the online bar shows whether I/O or SFC forces is enabled or disabled and installed or not installed. The ForcesStatus menu contains commands to remove, enable, or disable all forces.

Online Edit Status

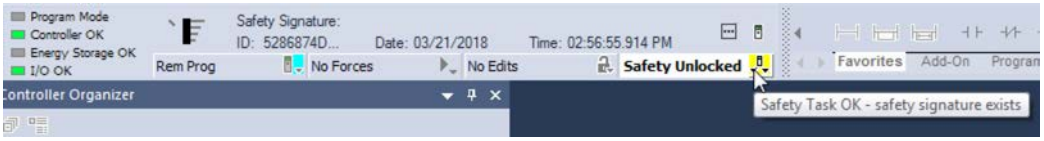
The Online Edit Status button  indicates whether edits or no edits exist in the online ladder routine or Function Block Diagram. When the button is selected, the online bar shows the edit state of the controller. If edits are made by another user, this area shows a textual description of the edits.

Safety Status

When you click the Safety Status button 

, the online bar displays the safety signature.

Figure 59 - Safety Signature Online Display



The Safety Status button itself indicates whether the controller is safety-locked or -unlocked, or faulted. It also displays an icon that shows the safety status.

When a safety signature exists, the icon includes a small check mark. 

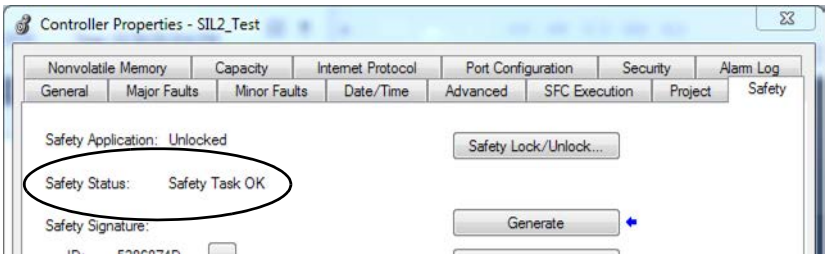
Table 31 - Safety Status Icons in a SIL 2/PLd Application, Both Online and Offline

If the safety status is	This icon appears
Safety Unlocked	 The controller is not safety locked.
Safety Locked	 The controller is safety locked.
Safety Faulted	 There is a safety fault.
Safety Task Inoperable	 The controller is not safety locked and the safety task is inoperable.  The controller is safety locked and the safety task is inoperable.  There is a safety fault and the safety task is inoperable.

View Status Via the Safety Tab

View controller safety status information on the safety status button on the online bar and on the Safety tab of the Controller Properties dialog box.

Figure 60 - Safety Status



- Safety task inoperable.
- Safety Task OK.

Except for Safety Task OK, the descriptions indicate that nonrecoverable safety faults exist.

See Major Safety Faults (Type 14) on page 274 for fault codes and corrective actions.

Monitor Safety Connections

For tags associated with consumed safety data, you can monitor the status of safety connections by using the CONNECTION_STATUS member. For monitoring input and output connections, safety I/O tags have a connection status member called SafetyStatus. Both data types contain two bits: ConnectionFaulted and RunMode.

The ConnectionFaulted value indicates whether the safety connection between the safety producer and the safety consumer is Valid (0) or Faulted (1). If ConnectionFaulted is set to Faulted (1) for any reason, the safety data is reset to zero and the RunMode value is set to Idle State (0).

The RunMode value indicates if consumed data is actively being updated by a device that is in the Run Mode (1) or Idle State (0). Idle state is indicated if the connection is closed, the safety task is faulted, or the remote controller or device is in Program mode or Test mode. For safety I/O connections, the RunMode is always inverse the ConnectionFaulted status. It does not provide unique data.

The following table describes the combinations of the ConnectionFaulted and RunMode states.

Table 32 - Safety Connection Status

ConnectionFaulted Status	RunMode Status	Safety Connection Operation
0 = Valid	1 = Run	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Valid	0 = Idle	The connection is active and the producing device is in the Idle state. The safety data is reset to zero. This applies to consumed connections only.
1 = Faulted	0 = Idle	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero and the RunMode value is set to Idle State (0).
1 = Faulted	1 = Run	Invalid state.

If a device is inhibited, the ConnectionFaulted bit is set to Faulted (1) and the RunMode bit is set to Idle (0) for each connection that is associated with the device. As a result, safety consumed data is reset to zero.

Utilize Status

Connection Status(.ConnectionFaulted) is the status of the safety connection between the safety controller and safety I/O module. When the connection is operating properly, this bit is LO (0). When the connection is NOT operating properly, this bit is HI (1). When the connection status is HI (connection not operating properly), all other module defined tags are LO, and should be considered 'invalid' data.

Point Status is available for both safety inputs (.PtxxInputStatus) and safety outputs (.PtxxOutputStatus). When a point status tag is HI (1), it indicates that individual channel is functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which this channel resides is operating properly.

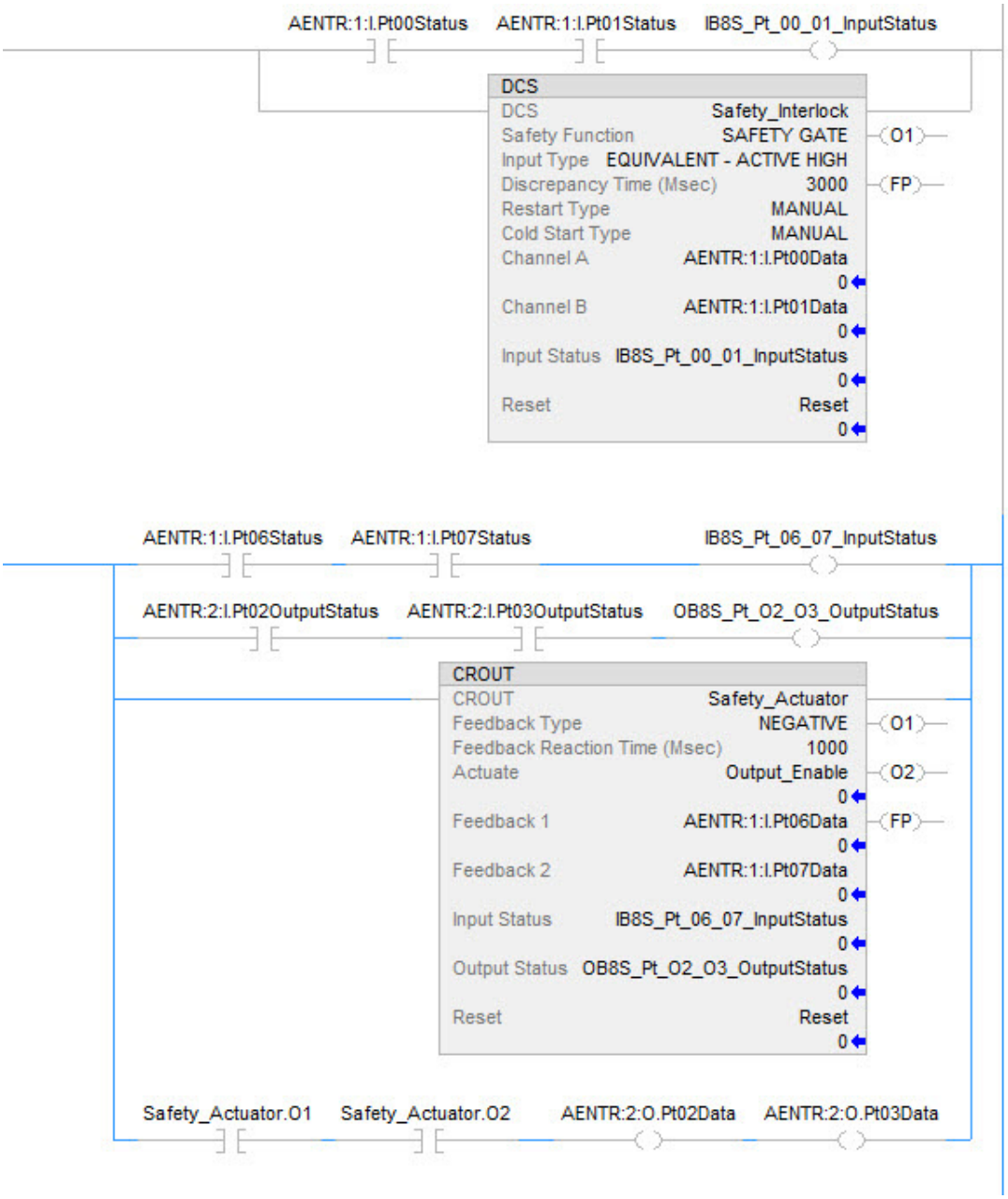
Combined Status is also available for both safety inputs (.CombinedInputStatus) and safety outputs (.CombinedOutputStatus). When the combined status tag is HI (1), it indicates that all input or output channels on the module are functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which these channels reside is operating properly.

Whether combined status or point status is used is application dependent. Point status simply provides more granular status.

The dual-channel safety instructions have built in safety I/O status monitoring. Input status and Output status are parameters for the safety input and output instructions. The DCS instruction (and other dual-channel safety instructions) has input status for input channels A and B. The CROUT instruction has input status for Feedbacks 1 and 2, and has output status for the output channels that are driven by the CROUT outputs O1 and O2. The status tags used in these instructions must be HI (1) for the safety instruction output tag(s) (O1 for input instructions and O1/O2 for CROUT) to be energized.

For proper safety instruction operation, it is important to drive the input status and output status tags BEFORE/ABOVE the safety instruction as shown in Figure 61.

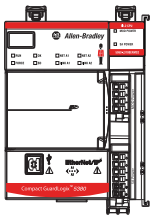
Figure 61 - Instruction Examples



Safety I/O status should be interrogated when using instructions such as XIC and OTE. The responsibility for this falls to the user. You should verify that safety input channel status is HI (1) before using a safety input channel as an interlock. You should verify that safety output channel status is HI (1) before energizing a safety output channel.

Safety Faults

Compact GuardLogix



Faults in the Compact GuardLogix 5380 system can be:

- Recoverable controller faults
- Nonrecoverable controller faults
- Nonrecoverable safety faults in the safety application
- Recoverable safety faults in the safety application

Nonrecoverable Controller Faults

Nonrecoverable controller faults occur when the controller internal diagnostics fail. If a nonrecoverable controller fault occurs, standard and safety task execution stops and outgoing connections stop. Safety I/O devices respond to the loss of output data by transitioning to the safe state. Recovery requires that you download the application program again.

If a fault occurs, diagnostic data is automatically written to the SD card. Rockwell Automation can then use the data to help investigate the cause of the fault. Contact Technical Support.

Nonrecoverable Safety Faults in the Safety Application

If a nonrecoverable safety fault occurs in the safety application, safety logic and the safety protocol are terminated. Safety task watchdog and control partnership faults fall into this category.

When the safety task encounters a nonrecoverable safety fault, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

ATTENTION: If you override a safety fault, it does not clear the fault. If you override a safety fault, it is your responsibility to prove that operation of your system is still safe.

You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

If a safety signature exists, you can clear the fault to enable the safety task to run. If no safety signature exists, the safety task cannot run again until the entire application is downloaded again.

- If you use the Clear Majors button or Clear Faults menu item in Logix Designer to clear the fault, the standard application should continue to run while the safety application is recovered from the snapshot.
- If you use the mode switch method (turn the mode switch to Program, then back to Run), the safety application is recovered from the snapshot, but the standard application briefly transitions out of Run mode.

Recoverable Faults in the Safety Application

If a recoverable fault occurs in the safety application, the system can halt the execution of the safety task, depending upon whether or not the fault is handled by the Program Fault Handler in the safety application.

When a recoverable fault is cleared programmatically, the safety task continues without interruption.

When a recoverable fault in the safety application is not cleared programmatically, a Type 14, Code 2 recoverable safety fault occurs. The safety program execution is stopped, and safety protocol connections are closed and reopened to reinitialize them. Safety outputs are placed in the safe state and the producer of safety-consumed tags commands the consumers to place them in a safe state, as well.

If the recoverable safety fault is not handled, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to eliminate these faults, rather than handling them at run-time.

ATTENTION: If you override a safety fault, it does not clear the fault. If you override a safety fault, it is your responsibility to prove that operation of your system is still safe.

You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

View Faults

The Recent Faults dialog box on the Major Faults tab of the Controller Properties dialog box contains two subtabs, one for standard faults and one for safety faults.

The status display on the controller also shows fault codes with a brief status message. See Status Indicators on page 307.

Fault Codes

Table 33 shows the fault codes specific to Compact GuardLogix 5380 controllers. The type and code correspond to the type and code that is displayed on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

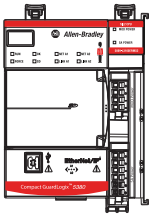
Table 33 - Major Safety Faults (Type 14)

Code	Cause	Status	Corrective Action
01	Task watchdog expired. User task has not completed in a specified period of time. A program error caused an infinite loop, the program is too complex to execute as quickly as specified, or a higher priority task is keeping this task from finishing.	Nonrecoverable	Clear the fault. If a safety signature exists, safety memory is reinitialized and the safety task begins executing. If a safety signature does not exist, you must redownload the program so the safety task can run.
02	An error exists in a routine of the safety task.	Recoverable	Correct the error in the user-program logic.
07	Safety task is inoperable. This fault occurs when the safety logic is invalid.	Nonrecoverable	Clear the fault. If a safety signature exists, safety memory is reinitialized via the safety signature and the safety task begins executing. If a safety signature does not exist, you must download the program again so the safety task can run.

The Logix 5000 Controllers Major and Minor Faults Programming Manual, publication 1756-PM014, contains descriptions of the fault codes common to Logix controllers.

Develop a Fault Routine for Safety Applications

Compact GuardLogix



If a fault condition occurs that is severe enough for the controller to shut down, the controller generates a major fault and stops the execution of logic.

Some applications do not want all safety faults to shut down the entire system. In those situations, use a fault routine to clear a specific fault and let the standard control portion of your system continue to operate or configure some outputs to remain ON.

ATTENTION: You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to eliminate these faults, rather than handling them at run-time.

The controller supports two levels for handling major faults in a safety application:

- Safety Program Fault Routine
- Controller Fault Handler

Both routines can use the GSV and SSV instructions as described on page 276.

Each safety program can have its own fault routine. The controller executes the program fault routine when an instruction fault occurs. If the program fault routine does not clear the fault, or if a program fault routine does not exist, the safety task faults and shuts down.

When the safety task faults, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

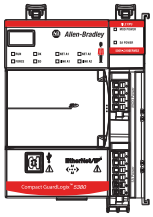
The controller fault handler is an optional component that executes when the program fault routine cannot clear the fault or does not exist.

You can create one program for the controller fault handler. After you create that program, you must configure a routine as the main routine.

The Logix 5000 Controllers Major and Minor Faults Programming Manual, publication 1756-PM014, provides details on creating and testing a fault routine.

Use GSV/SSV Instructions in a Safety Application

Compact GuardLogix



For standard tasks, you can use the GSV instruction to get values for the available attributes. When using the SSV instruction, the software displays only the attributes that you can set.

For the safety task, the GSV and SSV instructions are more restricted. SSV instructions in safety and standard tasks cannot set bit 0 (major fault on error) in the mode attribute of a safety I/O device.

ATTENTION: Use the SSV instruction carefully. Making changes to objects can cause unexpected controller operation or injury to personnel.

Access FaultRecord Attributes

Create a user-defined structure to simplify access to the MajorFaultRecord and SafetyTaskFaultRecord attributes.

Table 34 - Parameters for Accessing FaultRecord Attributes

Name	Data Type	Style	Description
TimeLow	DINT	Decimal	Lower 32 bits of the fault timestamp value
TimeHigh	DINT	Decimal	Upper 32 bits of the fault timestamp value
Type	INT	Decimal	Fault type (program, I/O, or other)
Code	INT	Decimal	Unique code for this fault (dependent on fault type)
Info	DINT[8]	Hexadecimal	Fault-specific information (dependent on fault type and code)

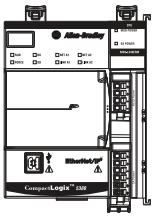
Capture Fault Information

The SafetyStatus and SafetyTaskFaultRecord attributes can capture information about non-recoverable faults. Use a GSV instruction in the controller fault handler to capture and store fault information. The GSV instruction can be used in a standard task in conjunction with a controller fault handler routine that clears the fault and lets the standard tasks continue executing.

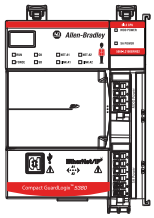
For more information on using the GSV and SSV instructions in safety applications, refer to the Input/Output Instructions chapter of the Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003.

Develop Motion Applications

CompactLogix



Compact GuardLogix



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	4
5069-L320ERM	8
5069-L330ERM	16
5069-L340ERM	20
5069-L350ERM	24
5069-L380ERM	28
5069-L3100ERM	32

Compact GuardLogix 5380 Controllers	
5069-L306ERMS2	2
5069-L310ERMS2	4
5069-L320ERMS2, 5069-L320ERMS2K	8
5069-L330ERMS2, 5069-L330ERMS2K	16
5069-L340ERMS2	20
5069-L350ERMS2, 5069-L350ERMS2K	24
5069-L380ERMS2	28
5069-L3100ERMS2	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.
- All CompactLogix 5380 and Compact GuardLogix 5380 controllers support single-axis motor control with PowerFlex variable frequency drives over an EtherNet/IP network.

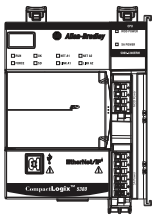
  This functionality is available on CompactLogix 5380 and Compact GuardLogix 5380 controllers that do not support other aspects of Integrated Motion over an EtherNet/IP network.

For more information, see the following:

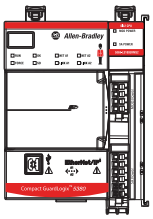
- Integrated Motion on the EtherNet/IP network Configuration and Startup User Manual, publication MOTION-UM003.
- Integrated Motion on the EtherNet/IP network Reference Manual, Publication MOTION-RM003.

Motion Overview

CompactLogix



Compact GuardLogix



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.

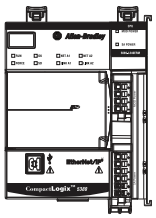
The controllers do not support Analog or SERCOS motion.

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

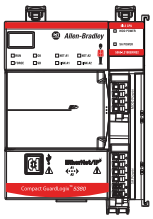
1. Create a controller project.
2. Select the type of drive.
3. Create axis tags as needed.
4. Configure the drive.
5. Create axes as needed.

Program Motion Control

CompactLogix



Compact GuardLogix



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.

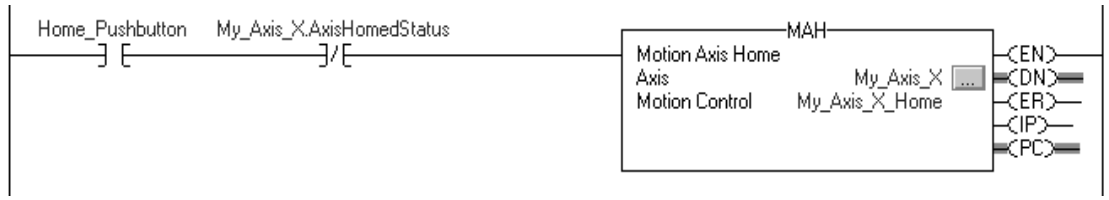
For more information, see the Logix 5000 Controller Motion Instructions Reference Manual, publication MOTION-RM002.

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.

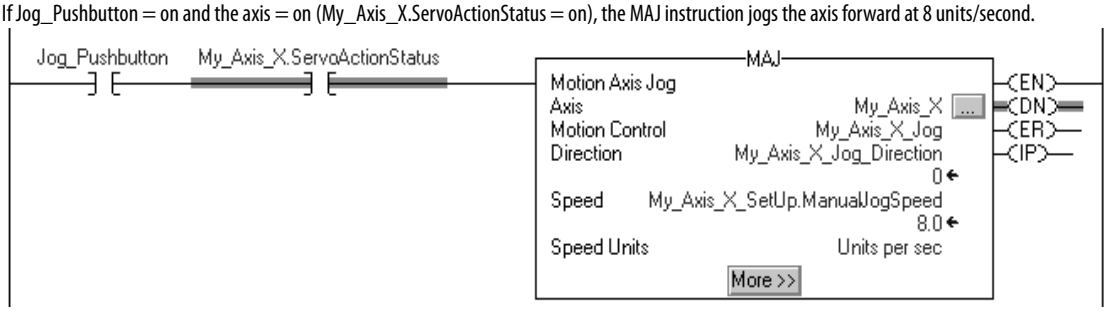
In this example, a simple ladder diagram that homes, jogs, and moves an axis.

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

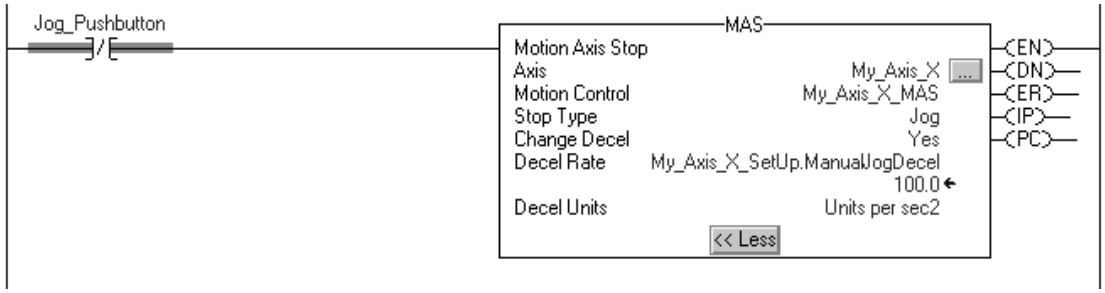
If Home_Pushbutton = on and the axis hasn't been homed (My_Axis_X.AxisHomedStatus = off), the MAH instruction homes the axis.



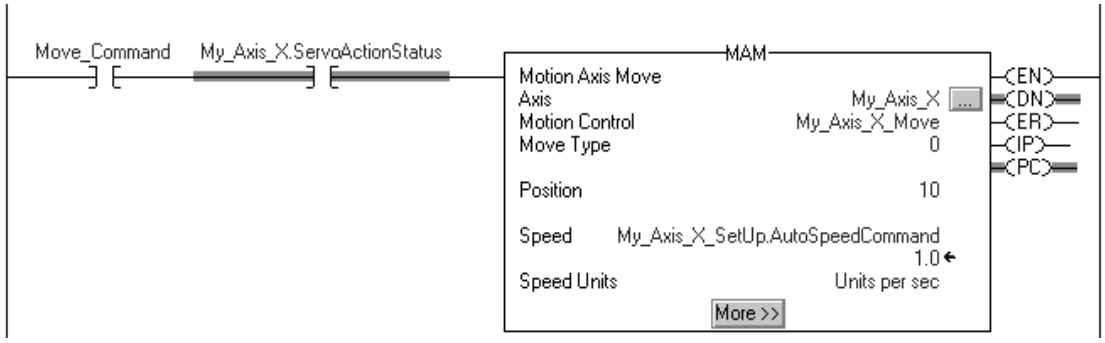
If Jog_Pushbutton = on and the axis = on (My_Axis_X.ServoActionStatus = on), the MAJ instruction jogs the axis forward at 8 units/second.



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.

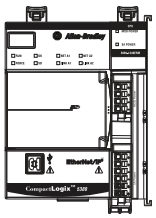


If Move_Command = on and the axis = on (My_Axis_X.ServoActionStatus = on), the MAM instruction moves the axis. The axis moves to the position of 10 units at 1 unit/second.

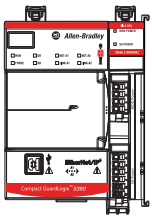


Obtain Axis Information

CompactLogix



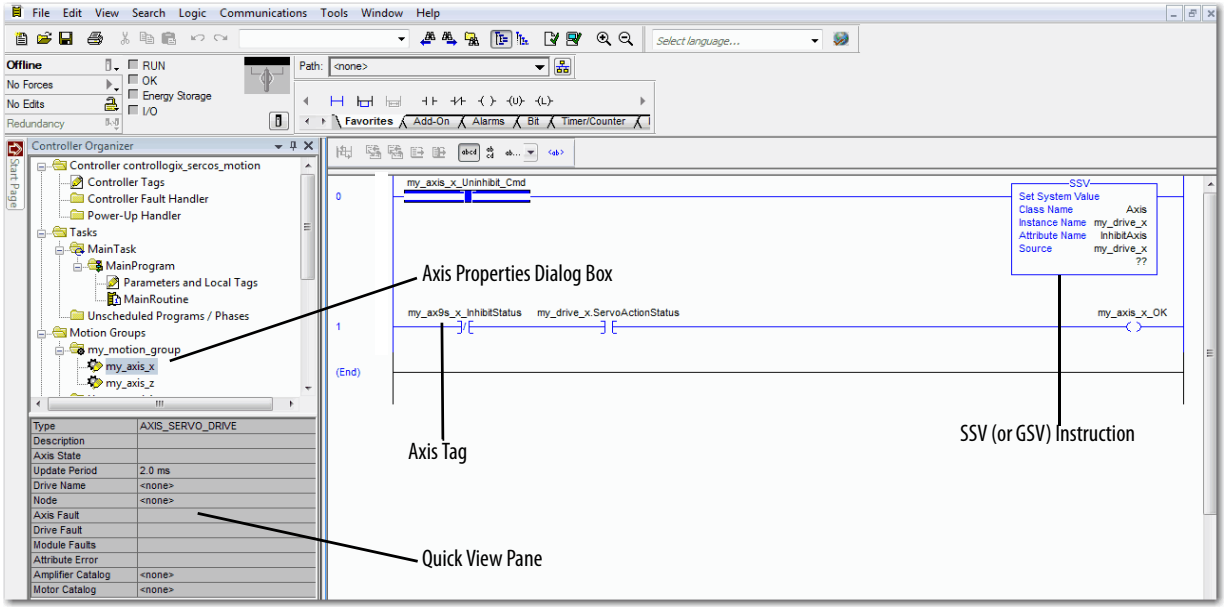
Compact GuardLogix



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 62 - Obtain Axis Information



Notes:

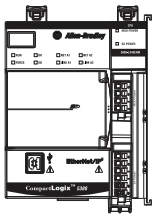
Troubleshoot the Controller

This chapter describes how to troubleshoot the controller if issues occur during normal operation.

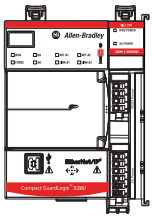
You can use messages on the 4-character display to troubleshoot the controller. For more information, see Appendix A, Status Indicators on page 307.

Controller Diagnostics with Logix Designer

CompactLogix



Compact GuardLogix



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

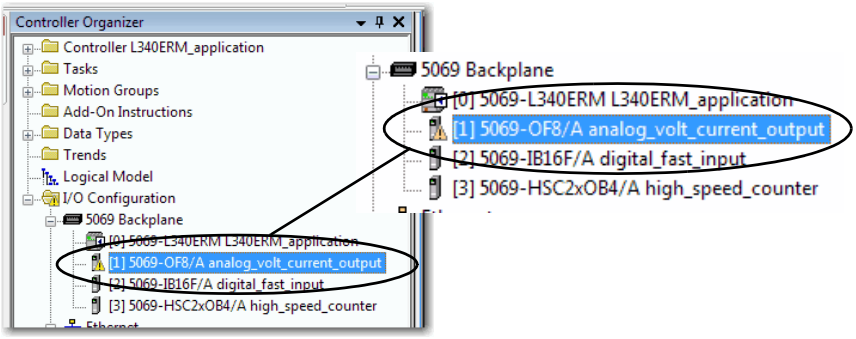
Warning Symbol in the I/O Configuration Tree

IMPORTANT **Safety Consideration**

You cannot configure safety connections to automatically fault the controller.

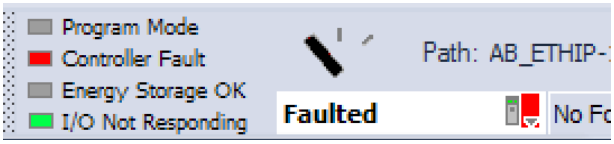
A warning symbol appears in the controller organizer next to the I/O module. This occurs when there are faults or other conditions in the I/O module, or if the connection to the I/O module fails while in run mode.

Figure 63 - Warning Symbol on I/O Module



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.

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:

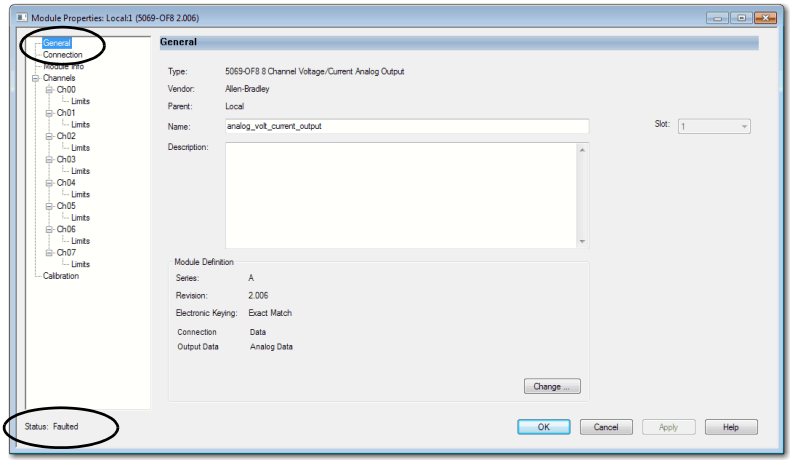
- Module Status on General Category
- Module Fault Descriptions on Connection Category
- Module Fault Descriptions on Module Info Category
- Diagnostics Option on Module Info Category

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 64.

Module Status on General Category

The General category displays the module status.

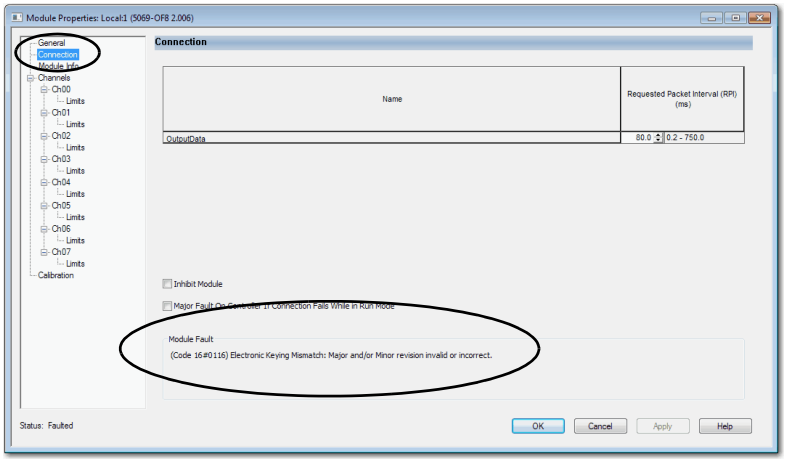
Figure 64 - Module Status in Fault Message Line



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 65 - Fault Description with Error Code



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.

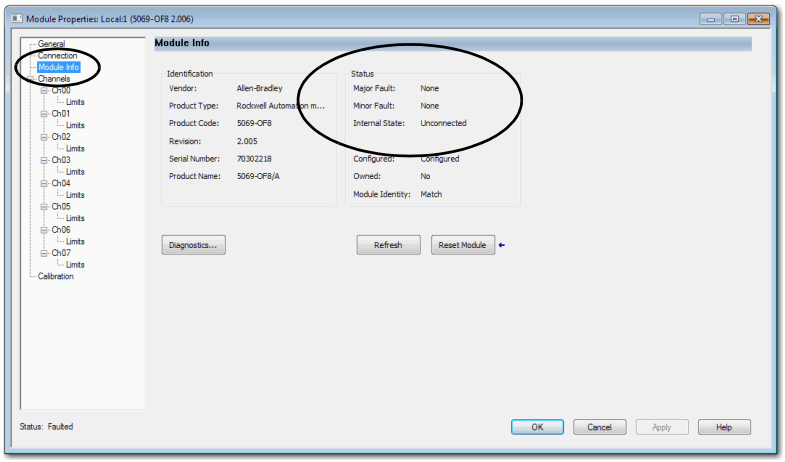
TIP The Module Info tab requires successful communications to help you troubleshoot the fault effectively. Consider the following:

- 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

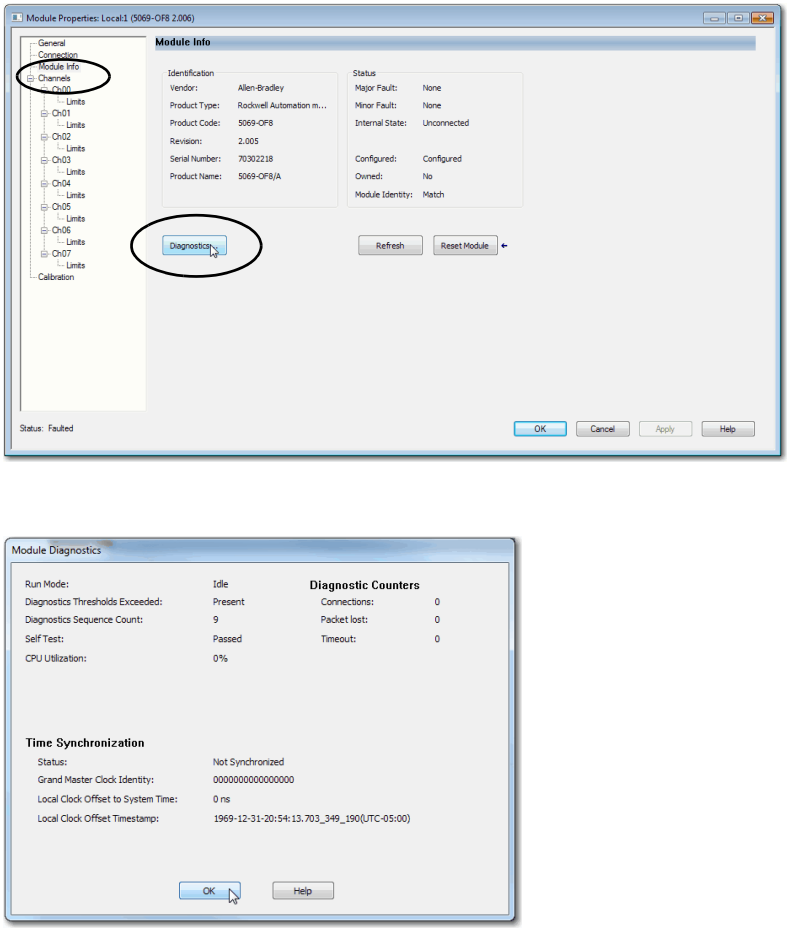
Figure 66 - Major and Minor Fault Information



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.

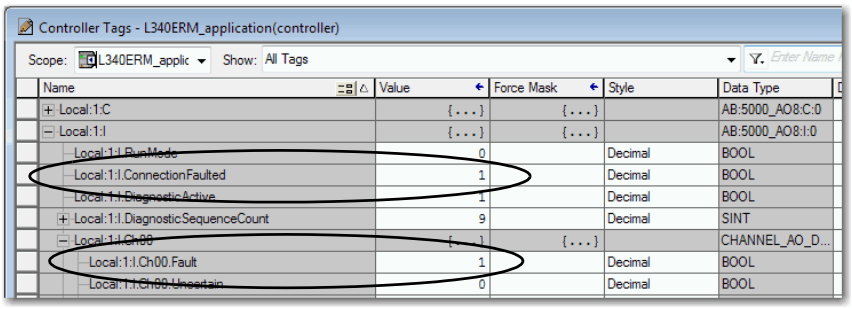
Figure 67 - Module Diagnostics



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.



Fault Information in the Controller Properties Dialog Box

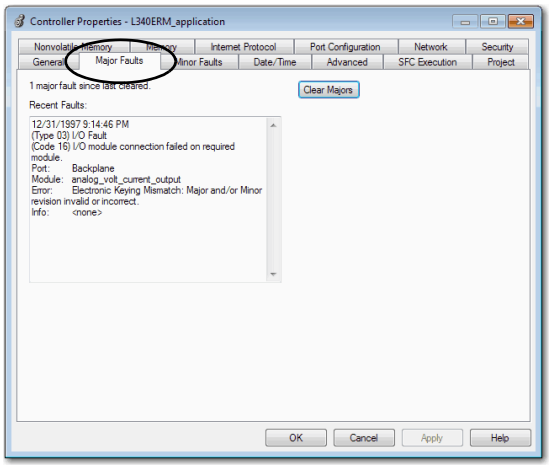
You can use these tabs on the Controller Properties dialog box to troubleshooting the controller:

- 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.

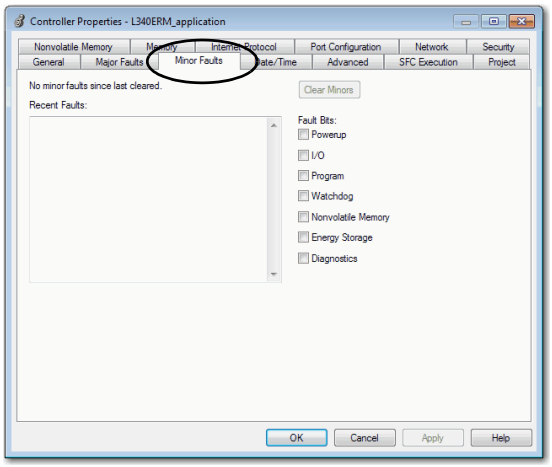
Figure 68 - Major Faults Tab in Controller Properties Dialog Box



Minor Faults

You can monitor information about recent minor faults and also clear minor faults on the Minor Faults tab.

Figure 69 - Minor Faults Tab in Controller Properties Dialog Box

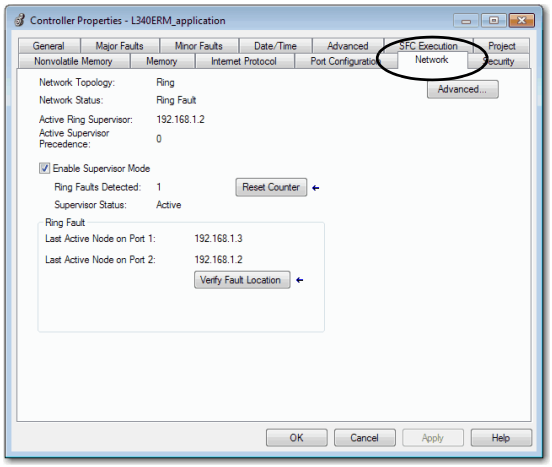


Network

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.

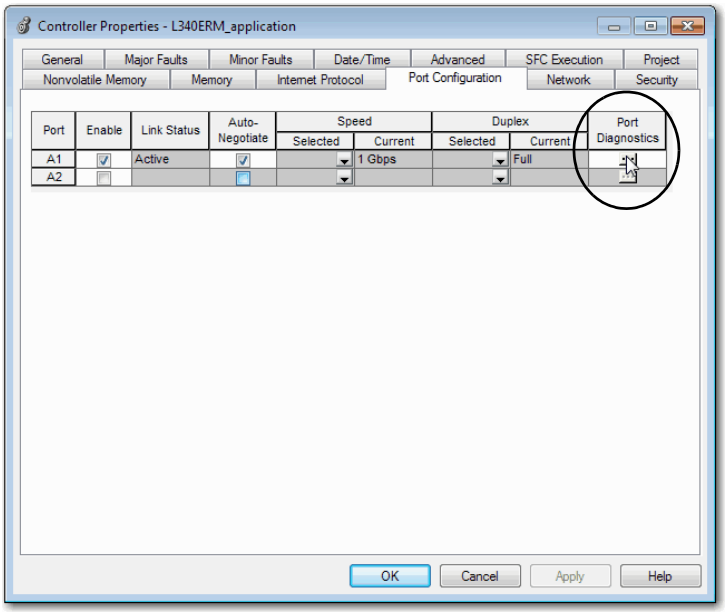
Figure 70 - Network Tab in Controller Properties Dialog Box



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.



The Port Diagnostics page, displays information for the port. See Table 35 on page 292 for parameter descriptions.

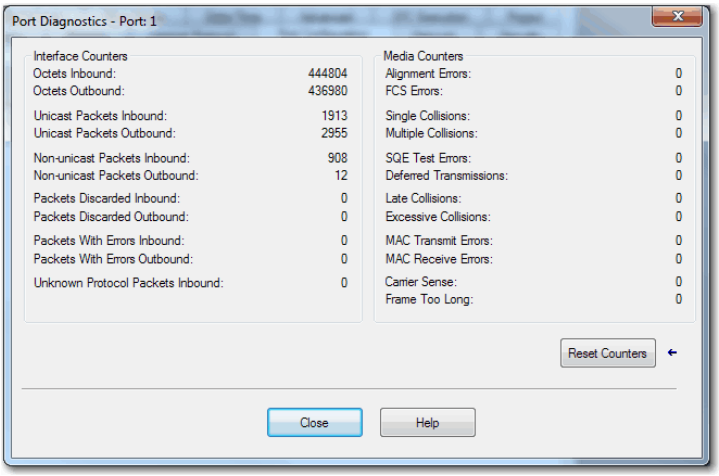


Table 35 - Port Diagnostics Parameters - Logix Designer

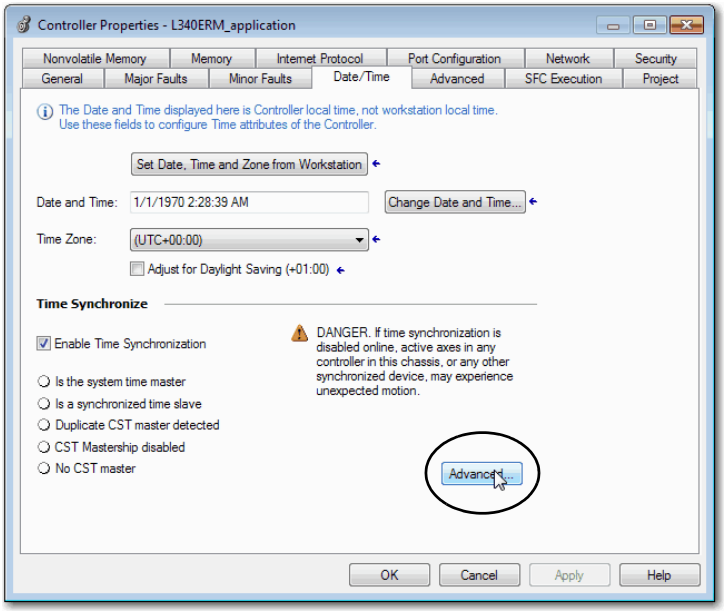
Parameter	Description
Interface Counters	The Interface Counters values have no value when you cannot communicate out of the port.
Octets Inbound	Displays the number of octets that are received on the interface.
Octets Outbound	Displays the number of octets that are transmitted to the interface.
Unicast 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.
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.

IMPORTANT The information appears only if the project is online and Time Synchronization is enabled on the Date/Time tab. Also, when the controller operates in Dual-IP mode, the Advanced Time Sync tab provides data for each port.

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



The Advanced Time Sync dialog box opens. See Table 36 on page 294 for parameter descriptions.

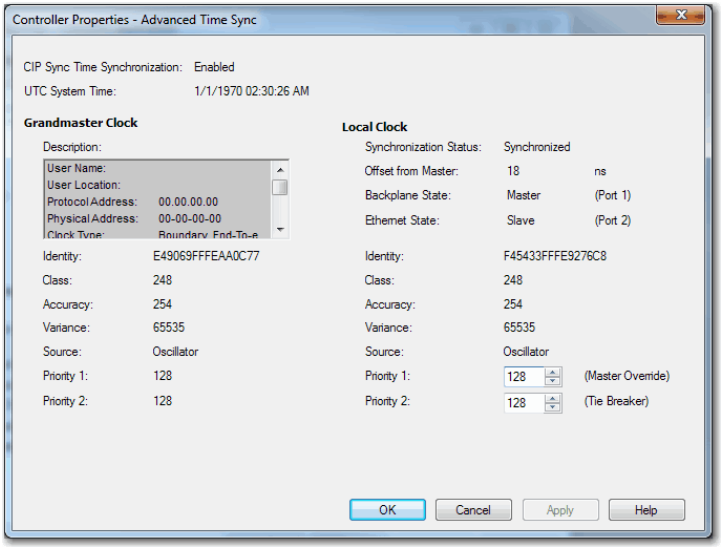


Table 36 - Time Sync Parameters

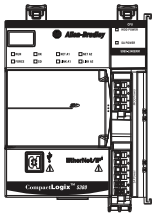
Grandmaster Clock	
Description	Displays information about the Grandmaster clock. The vendor of the Grandmaster device controls this information. The following information is specified: • User Name • User Location • Protocol Address • Physical Address • Clock Type • Manufacturer Name • Model • Serial 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 36 - Time Sync Parameters (continued)

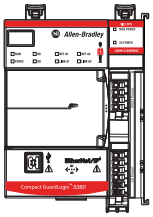
Local Clock	
Synchronization Status	Displays whether the local clock is synchronized or not synchronized with the Grandmaster reference clock. A clock is synchronized if it has one port in the slave state and is receiving updates from the time master.
Offset to Master	Displays the amount of deviation 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

CompactLogix

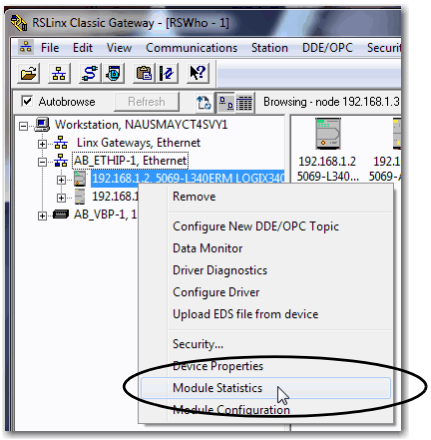


Compact GuardLogix



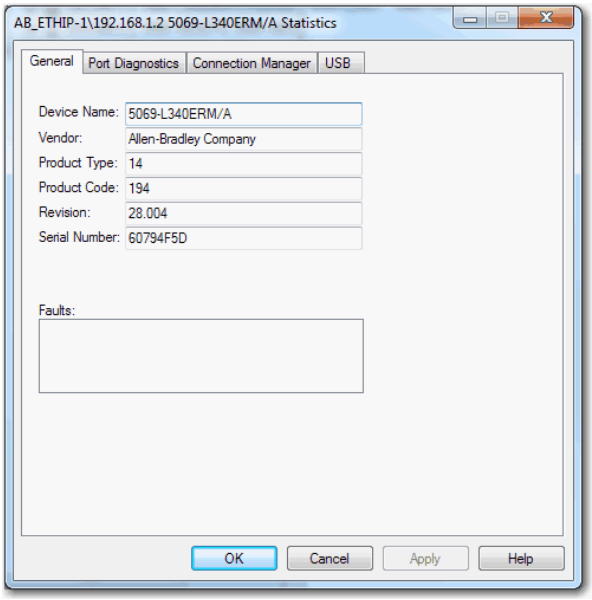
You can also view diagnostic information in Linx-based software.

1. Use the RSWho button to browse.
2. Navigate to the Ethernet network.
3. Right-click the controller and choose Module Statistics.



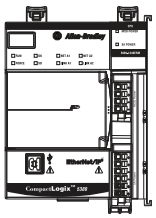
The Module Statistics dialog provides this information:

- 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.

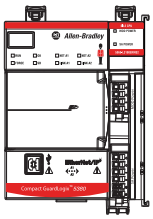


Controller Web Pages

CompactLogix



Compact GuardLogix



The controller provides diagnostic web pages that track controller performance, network performance, and backplane performance.

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.

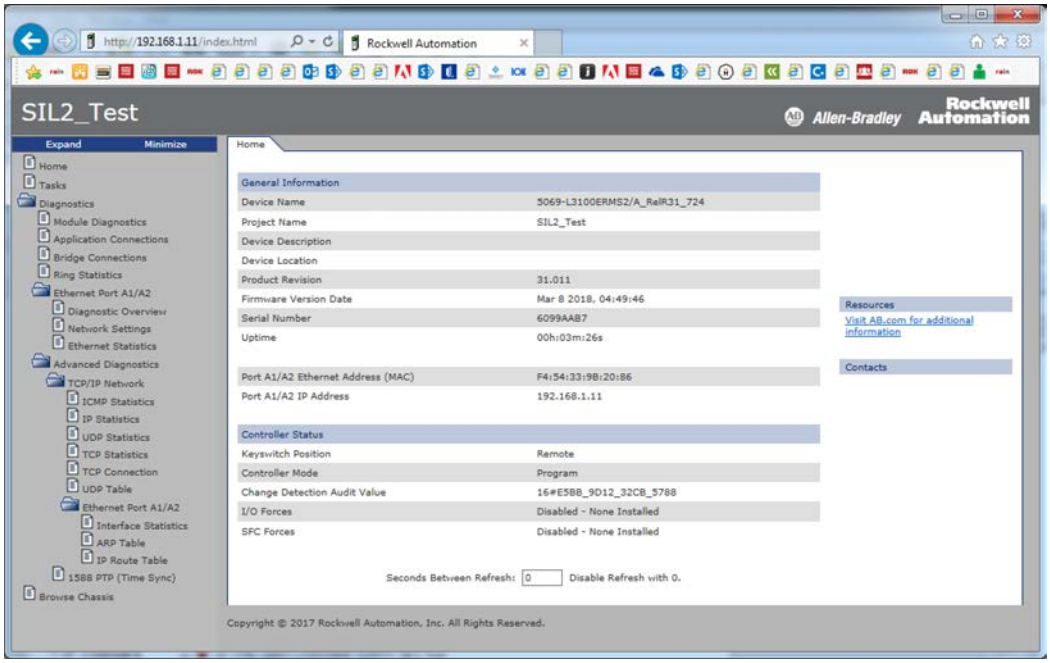
  There is one Ethernet Port web page for both ports, and the controller web pages provide one set of Ethernet data.
- When the controller operates in Dual-IP mode, the left-side navigation bar displays an Ethernet Port A1 folder and an Ethernet Port A2 folder. Each folder has three tabs.

  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.

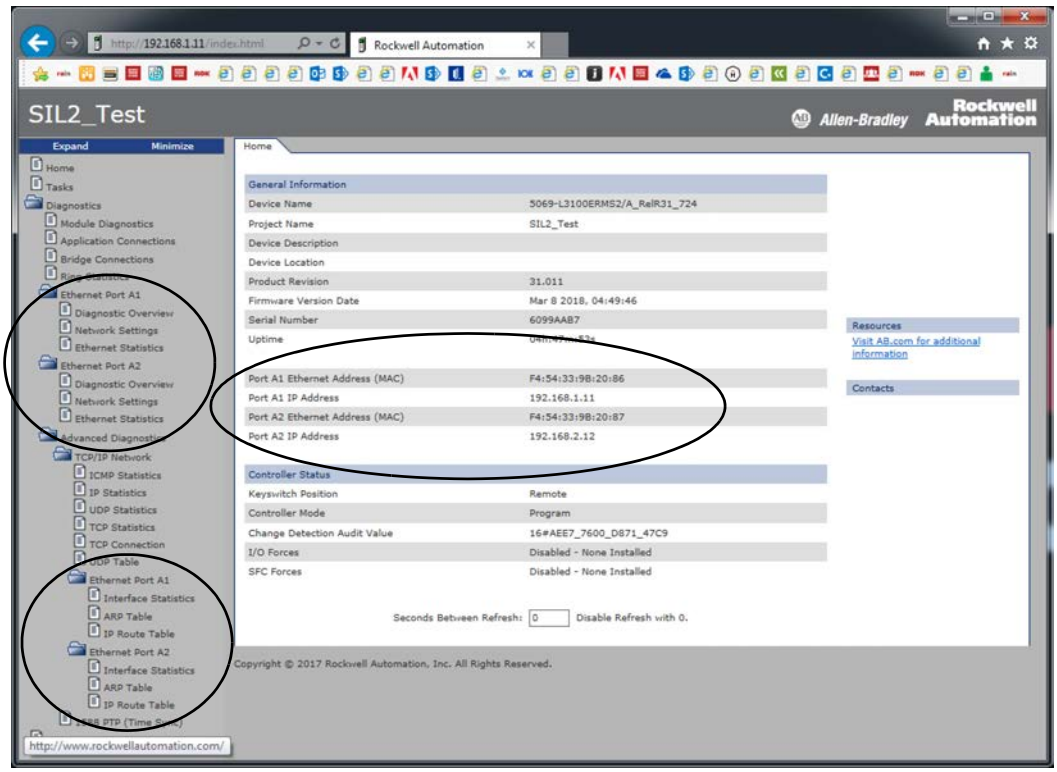
Home Web Page

The Home web page provides device information and controller status.

Linear/DLR Mode



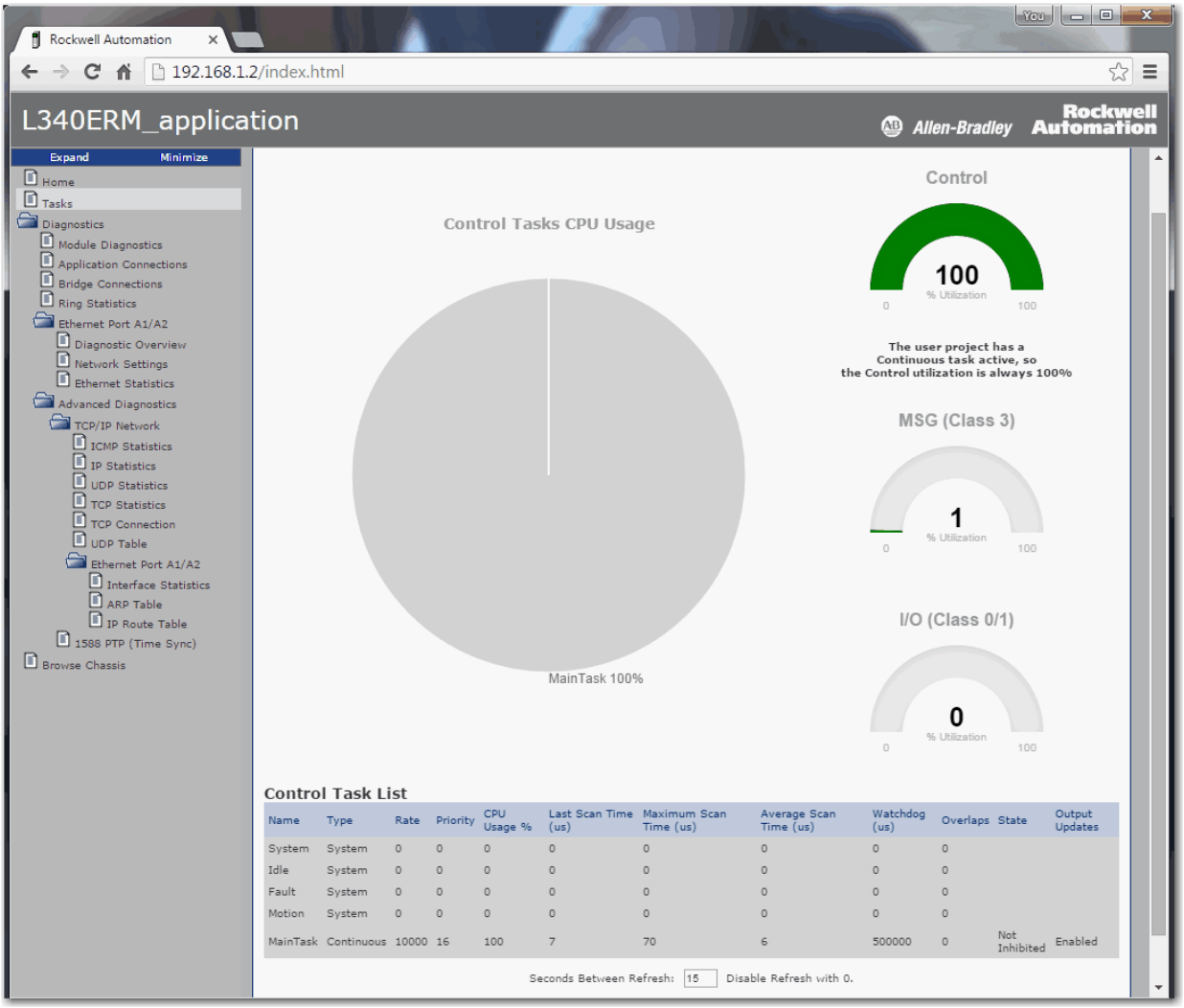
Dual-IP Mode



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.

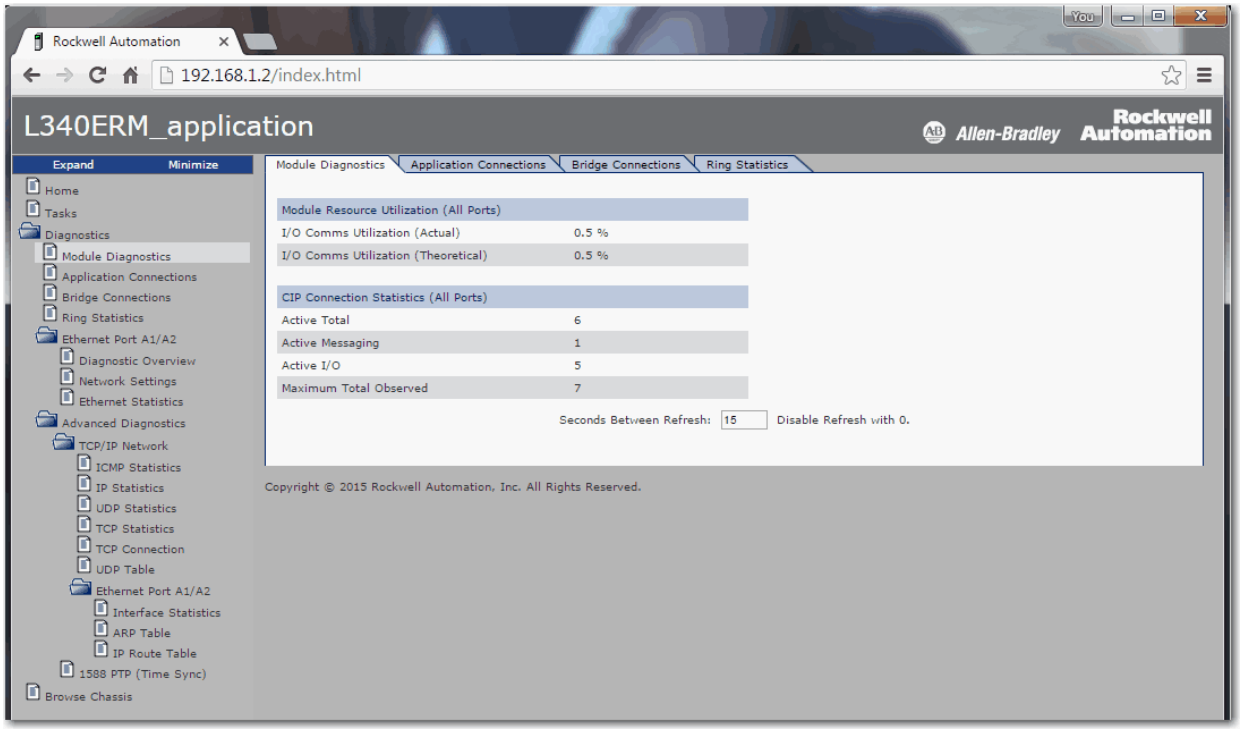
The table shows the tasks that are running on the Control core (all system tasks are summarized as one task).



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

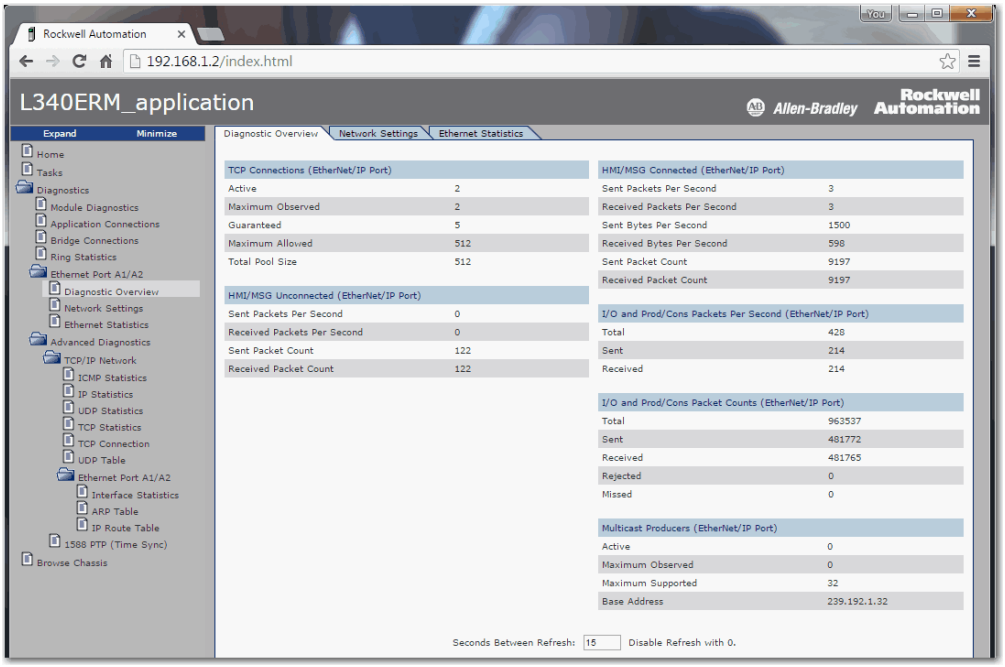


Ethernet Port Web Pages

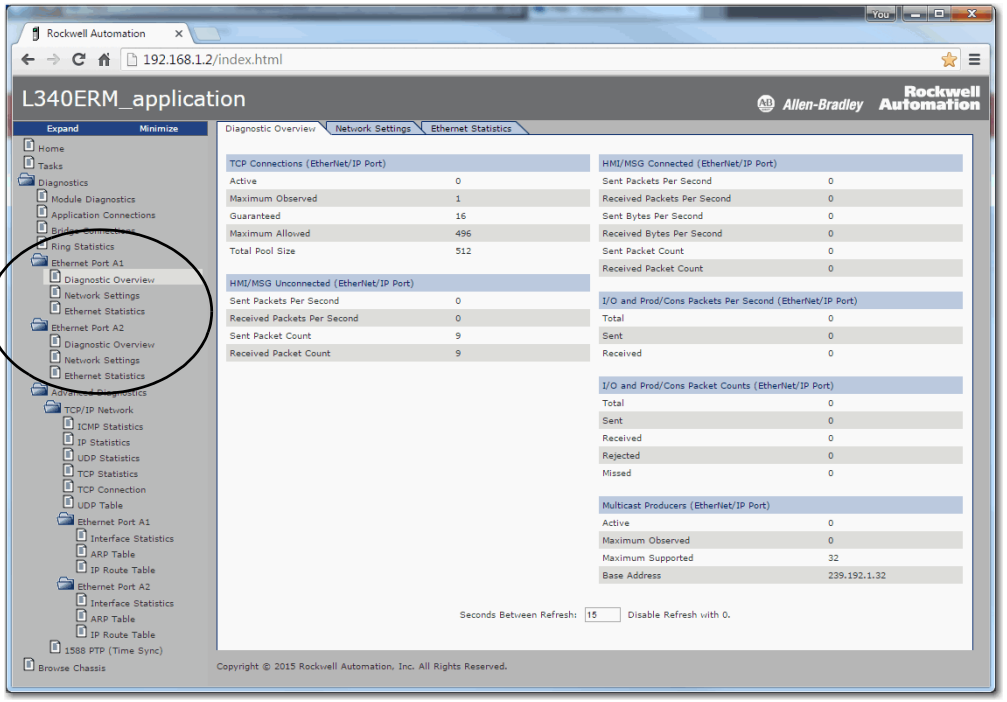
The Ethernet Port web pages use a series of tabs to provide information about the following:

- Diagnostic Overview
- Network Settings
- Ethernet Statistics

Linear/DLR Mode



Dual-IP Mode



Advanced Diagnostics Web Pages

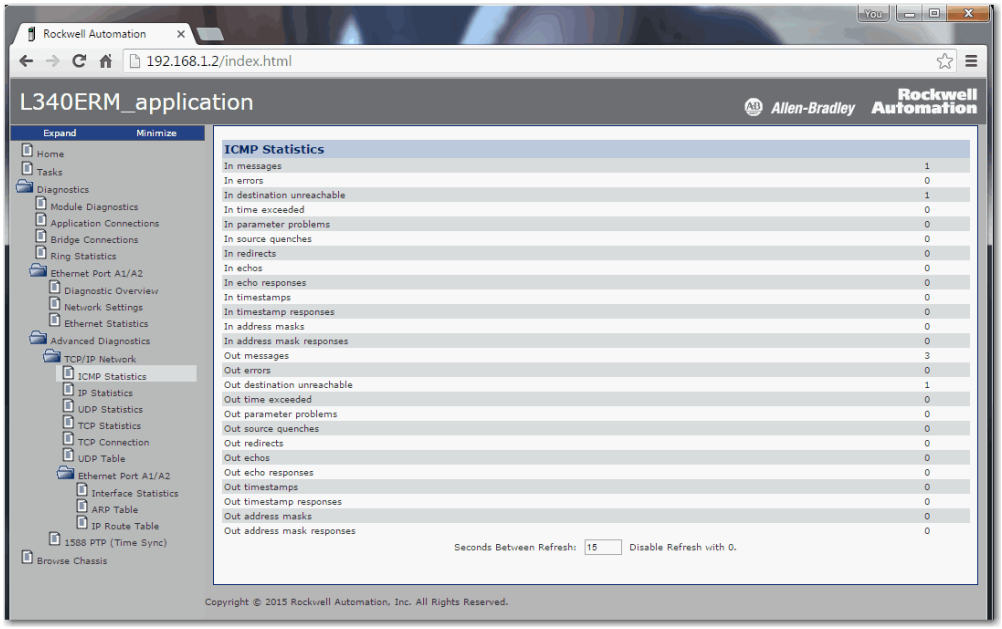
The Advanced Diagnostics web pages provide information about the following:

- 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

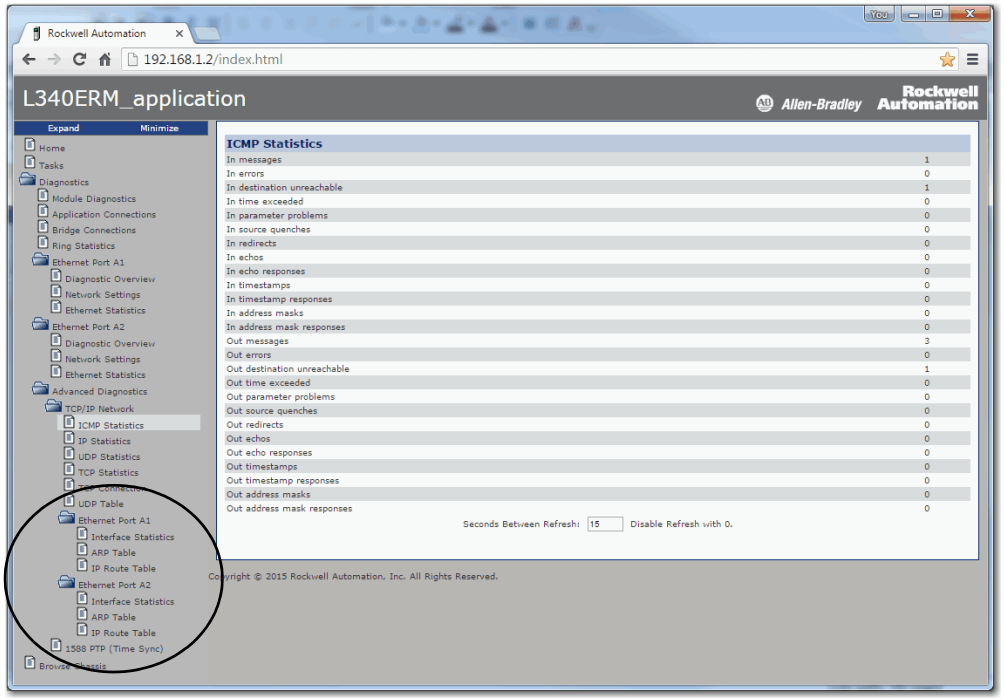
IMPORTANT This information is listed separately for, and is unique to, each port when the controller operates in Dual-IP mode.

- 1588 PTP (Time Sync)

Linear/DLR Mode

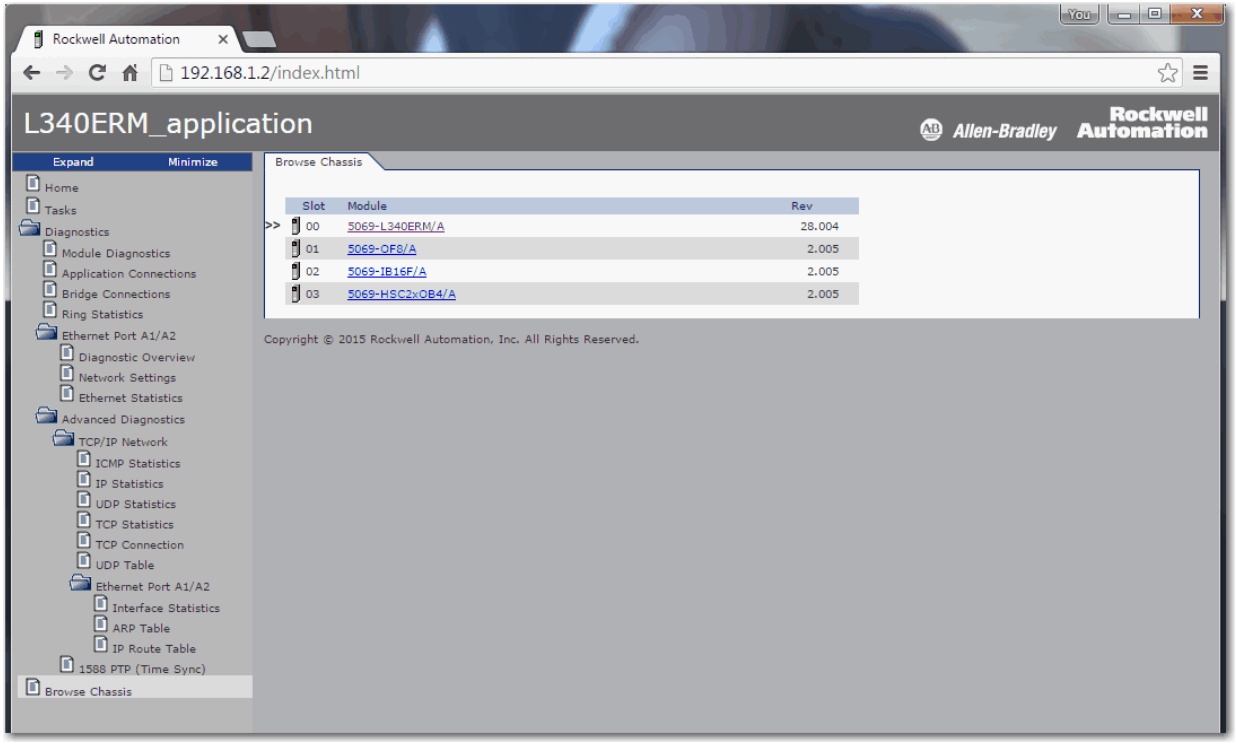


Dual-IP Mode



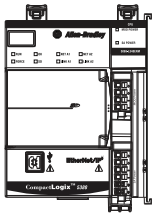
Browse Chassis Web Page

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.

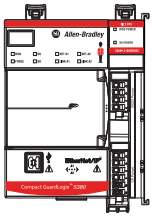


Other Potential Issues to Troubleshoot

CompactLogix



Compact GuardLogix



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 137.

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.

Notes:

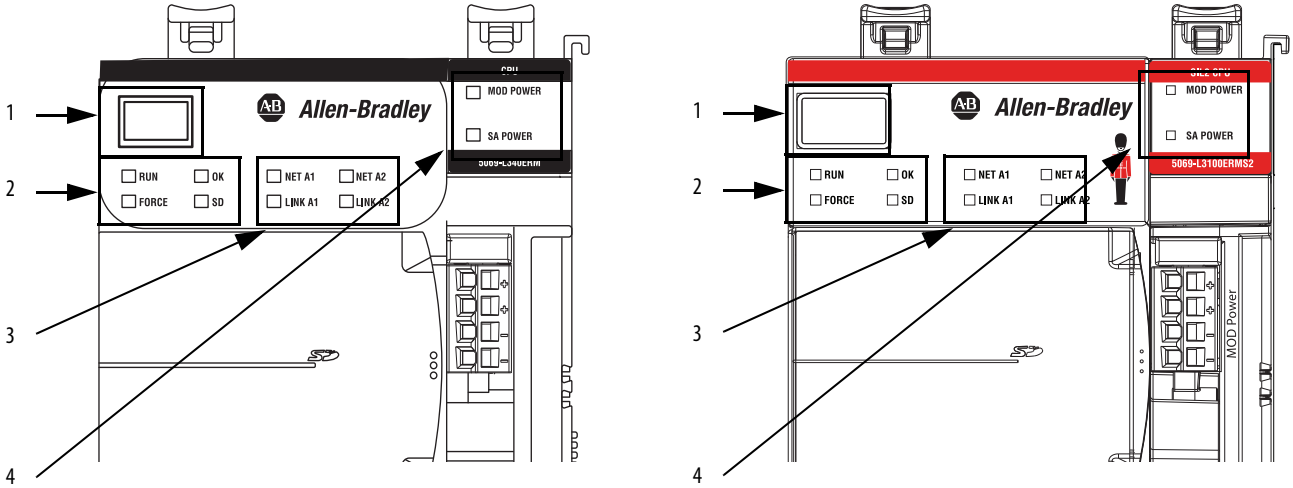
Status Indicators

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 71 shows the status display and indicators on CompactLogix 5380 and Compact GuardLogix 5380 controllers.

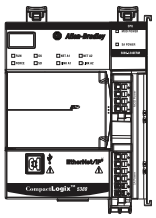
Figure 71 - Status Display and Indicators



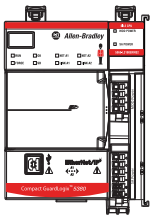
Item	Description
1	4-Character Scrolling Status Display, see page 309
2	Controller Status Indicators, see page 317
3	EtherNet/IP Status Indicators, see page 319
4	Power Status Indicators, see page 320

General Status Messages

CompactLogix



Compact GuardLogix



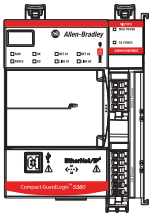
The scrolling messages that are described in this table are typically indicated upon powerup, powerdown, and while the controller is running to show the status of the controller.

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.
TEST	The controller is conducting power-up tests.
CHRG	The embedded energy storage circuit is charging.
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 318. 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 318. 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 318. 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.

Message	Interpretation
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.
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 utilities 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.
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

Compact GuardLogix



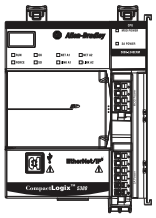
The Compact GuardLogix 5380 controller display can show these scrolling messages.

Table 37 - Safety Status Messages

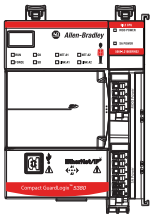
Message	Interpretation
No Safety Signature	Safety Task is in Run mode without a safety signature. Generate a safety signature.
Safety Task Inoperable	The safety logic is invalid. For example, a watchdog timeout occurred or memory is corrupt.
Safety Unlocked	The controller is in Run mode with a safety signature, but is not safety-locked. Safety lock the controller.

Fault Messages

CompactLogix



Compact GuardLogix



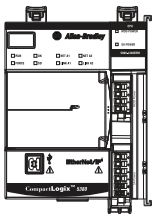
If the controller displays a fault, these messages can appear on the status display.

Table 38 - Fault Messages

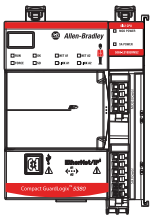
Message	Interpretation
Major Fault T*XX*:C*XX message*	A major fault of Type *XX* and Code *XX* has been detected. For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, a JMP instruction is programmed to jump to an invalid LBL instruction. For details about major recoverable faults, see the Logix 5000™ Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
I/O Fault Local:*X #XXXX message*	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
I/O Fault *ModuleName #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module is indicated with the fault code and brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named My_Module is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
I/O Fault *ModuleParent:X #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The parent name of the module is indicated because no module name is configured in the I/O Configuration tree of Logix Designer application. In addition, the fault code is indicated with a brief description of the fault. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
X I/O Faults	I/O faults are present and *X* = the number of I/O faults present. If there are multiple I/O faults, the controller indicates 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 each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

Major Fault Messages

CompactLogix



Compact GuardLogix



The Major Fault T*XX*:C*XX message* on the controller status display indicates major faults. Table 39 lists fault types, codes, and the associated messages as they are shown on the status display.

For detailed descriptions and suggested recovery methods for major faults, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

Table 39 - Major Fault Status Messages

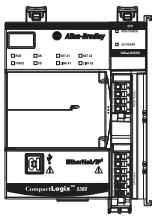
Type	Code	Message
1	1	Run Mode Powerup
1	60	Nonrecoverable
1	61	Nonrecoverable – Diagnostics Saved on SD Card
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	User-defined
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	

Table 39 - Major Fault Status Messages (continued)

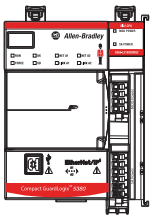
Type	Code	Message
6	1	Task Watchdog Expired
7	40	Save Failure
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
7	44	Failed to Restore Processor Memory
8	1	Mode switch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	DriveGuard® Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
14	1	Safety Task Watchdog Expired
14	2	Error In Routine of Safety Task
14	7	Safety Task Inoperable
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

I/O Fault Codes

CompactLogix



Compact GuardLogix



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. For details about each I/O fault code, see the Logix 5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

Table 40 - I/O Fault Messages

Code	Message
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Settable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size

Table 40 - I/O Fault Messages (continued)

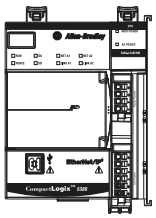
Code	Message
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD0A	Axis Attribute Reject
#FD1F	Safety I/O
#FD20	No Safety Task
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate

Table 40 - I/O Fault Messages (continued)

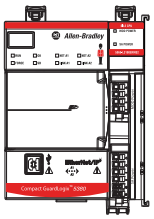
Code	Message
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled Personal Computer Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed - Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed

Controller Status Indicators

CompactLogix



Compact GuardLogix



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 41 - 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 42 - 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 43 - SD Indicator

State	Description
Off	No activity is occurring with the SD card.
Flashing green Solid 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.
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.

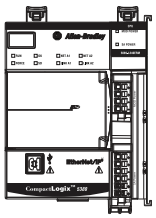
Table 44 - OK Indicator

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 105. • 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 105. • 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 309. – 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.

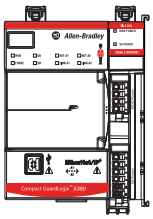
EtherNet/IP Status Indicators

The EtherNet/IP indicators show the state of the controller Ethernet ports and network communication activity.

CompactLogix



Compact GuardLogix



NET A1 and NET A2 Indicators

The NET A1 and NET A2 indicators show the state of the Ethernet port.

Table 45 - 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

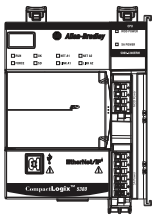
The LINK A1 and LINK A2 indicators show the state of the EtherNet/IP links.

Table 46 - LINK A1 and LINK A2 Indicators

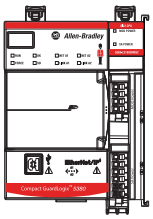
State	Description
Off	The link is down. One or more of these conditions exists: • Ethernet cables are not properly connected at both ends. That is, the cables are not properly connected the controller Ethernet port and to the connected device. • No link exists on the port. For example, the connected device is not powered. • The port is administratively disabled. • LINK A2 only: – The controller is the active ring supervisor in a DLR network, and the ring is not broken. This is normal operation. – 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. • There is **no activity** on the port.

Power Status Indicators

CompactLogix



Compact GuardLogix



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 47 describes the MOD Power indicator on a CompactLogix 5380 and Compact GuardLogix 5380 controller.

Table 47 - 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 48 describes the SA Power indicator on a CompactLogix 5380 and Compact GuardLogix 5380 controller.

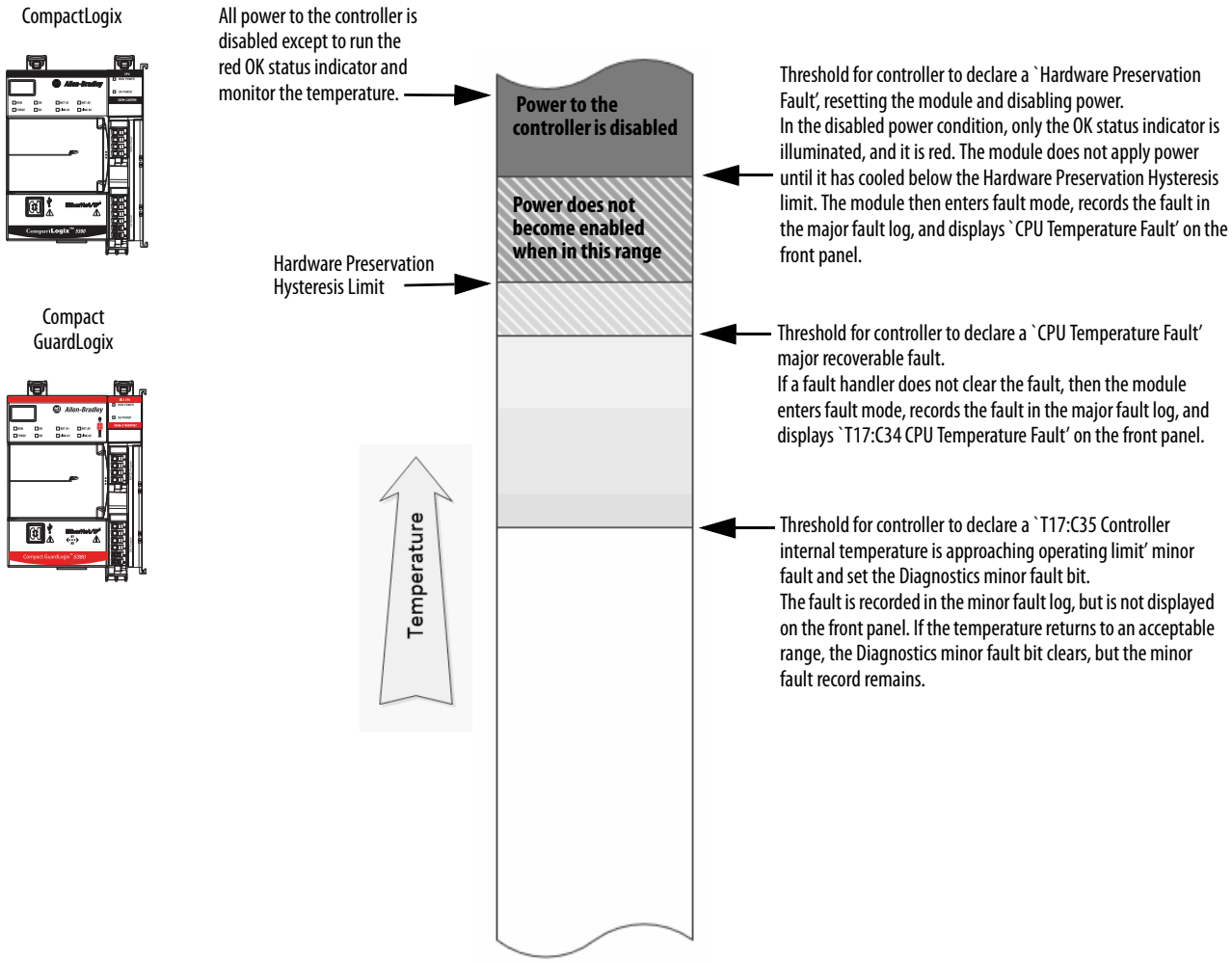
Table 48 - SA Power Indicator

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.



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.

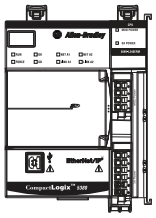
Notes:

Security Options

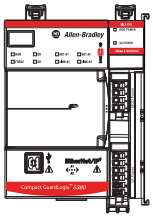
For enhanced security, you can disable functionality on your controller.

Disable an Ethernet Port

CompactLogix



Compact GuardLogix



You can disable the controller Ethernet ports with the Studio 5000 Logix Designer® application, version 28.00.00 or later.

IMPORTANT Remember the following:

- When you use the Logix Designer application, version 29.00.00 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.

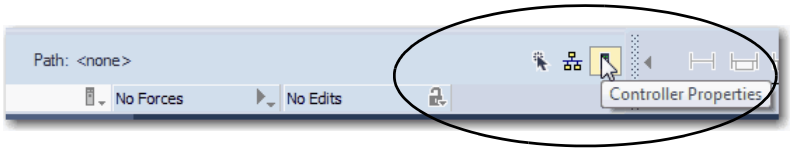
There are two ways to disable the Ethernet port:

- Disable the Ethernet Port on the Port Configuration Tab on page 324
- Disable the Ethernet Port with a MSG Instruction on page 325

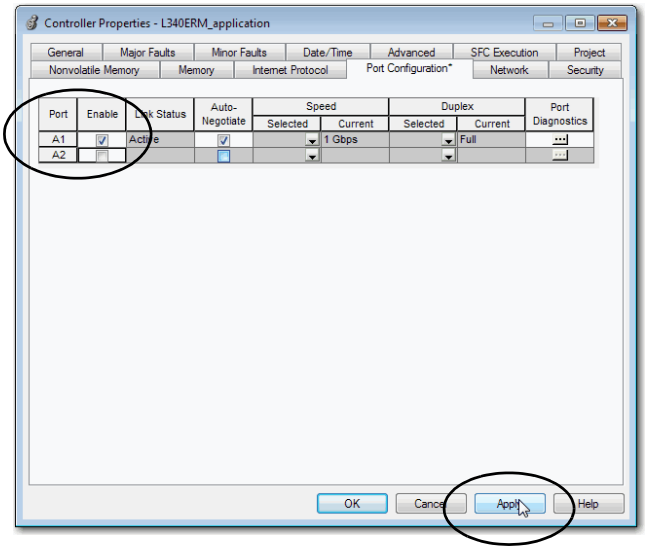
Disable the Ethernet Port on the Port Configuration Tab

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.

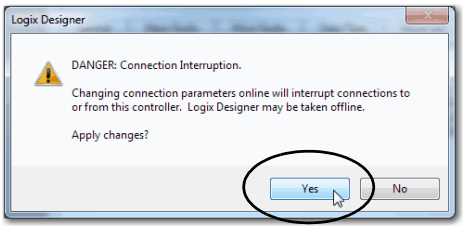
1. On the Online toolbar, click the Controller Properties button.



2. On the Controller Properties dialog box, click the Port Configuration tab.
3. On the Port Configuration tab, clear the Enable checkbox for the port that you want to disable and click Apply.



4. If you are online when you make this change, click Yes on the Alert dialog box.



- The change takes effect immediately.
- If you are offline, 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.

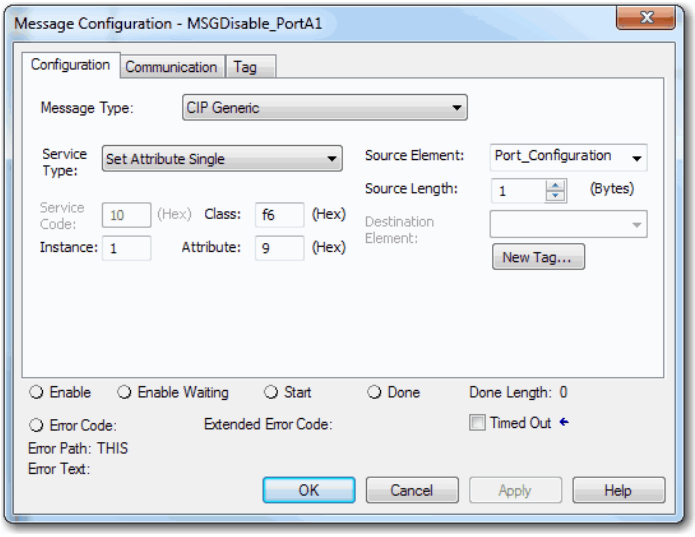
2. Configure the Configuration tab on the Message Configuration dialog box as follows:

   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.

   - 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

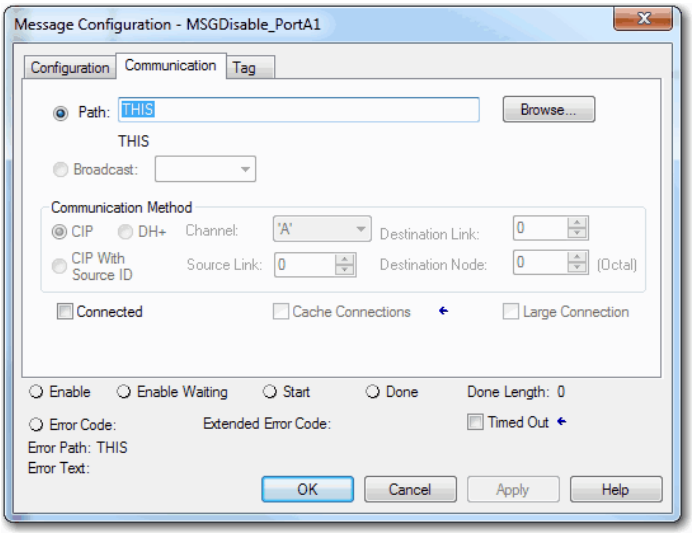
     In this example, the controller tag is named Port_Configuration.

   - Source Length - 1



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

IMPORTANT Messages to THIS must be unconnected messages.



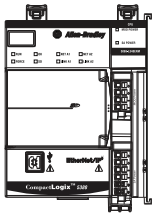
4. Before you enable the MSG instruction, make sure that the Source Element tag value is 2.

IMPORTANT You can re-enable an Ethernet port after it is disabled.

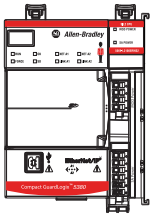
To re-enable the port, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 1.

Disable the 4-character Status Display

CompactLogix



Compact GuardLogix



With the Studio 5000 Logix Designer application, version 29.00.00 or later, you can disable certain categories of messages on the 4-character status display:

- Disable All Categories of Messages on page 328
- Disable Individual Categories of Messages on page 330

You use a CIP Generic MSG to execute each option.

IMPORTANT These system messages are always displayed and cannot be disabled:

- Powerup messages (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 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:
  - 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.

Disable All Categories of Messages

When you disable the 4-character display entirely, this information is no longer shown:

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

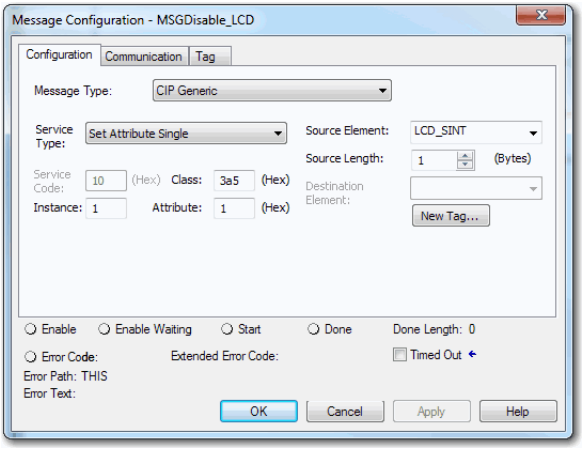
Complete these steps.

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.

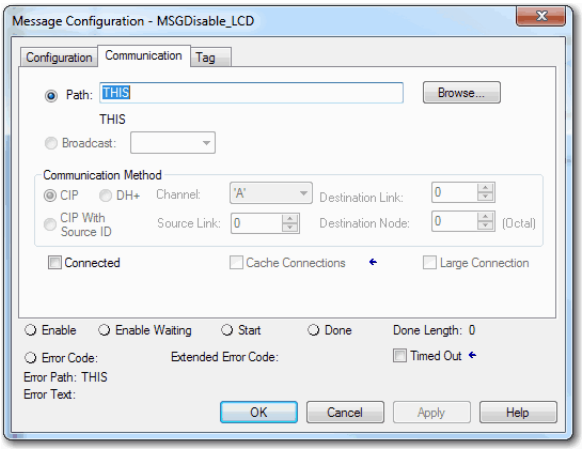
2. Configure the Configuration tab on the Message Configuration dialog box as follows:
   - Message Type - CIP Generic
   - Service Type - Set Attribute Single
   - Instance - 1
   - Class - 3a5
   - Attribute - 1
   - Source Element - Controller tag of SINT data type

     In this example, the controller tag is named LCD_SINT.
   - Source Length - 1



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

IMPORTANT Messages to THIS must be unconnected messages.



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

IMPORTANT You can re-enable the 4-character display after it is disabled.

To re-enable the 4-character display, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure that the Source Element tag value is 0.

Disable Individual Categories of Messages

You can disable a subset of the information that scrolls across the controller. You can disable these subsets:

- Project name and link status
- Port status and IP address

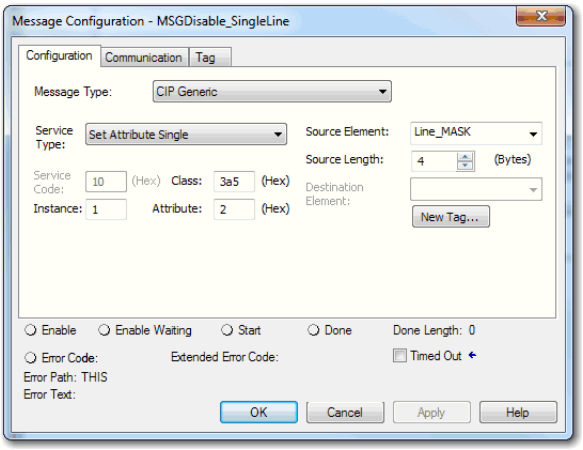
Complete these steps.

1. Add a MSG instruction to your program

   This message only needs to execute once, it does not need to execute with every program scan.

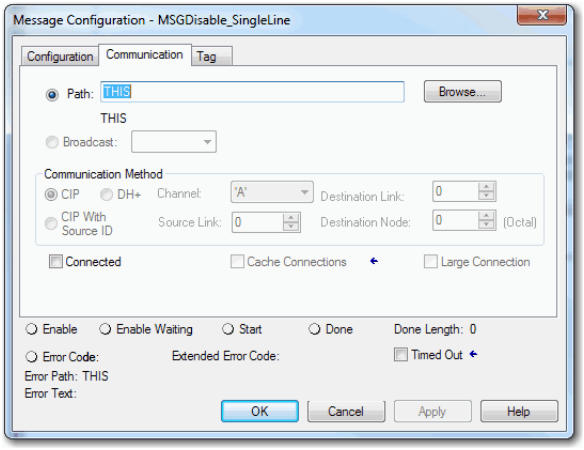
   IMPORTANT You cannot add a MSG instruction to your program if the controller is in Run mode or if the FactoryTalk Security settings deny this editing option.

2. Configure the Configuration tab on the Message Configuration dialog box as follows:
   - Message Type - CIP Generic
   - Service Type - Set Attribute Single
   - Instance - 1
   - Class - 3a5
   - Attribute - 2
   - Source Element - Controller tag of DINT data type - In this example, the controller tag is named Line_MASK.
   - Source Length - 4



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

IMPORTANT Messages to THIS must be unconnected messages.



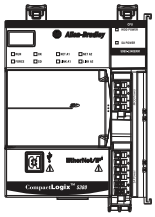
4. Before you enable the MSG instruction, set the bits in the Source Element tag to these values, based on what information that you want to disable:
   - Project name and link status - Bit 0 of the Source Element = 1
   - Port status and IP address - Bit 1 of the Source Element = 1

IMPORTANT You can re-enable the subsets of information on the 4-character display after they are disabled.

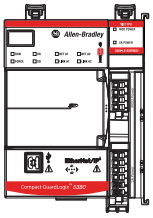
To re-enable the subsets, complete the steps that are described in this section. Before you enable the MSG instructions, however, make sure the appropriate bit in the Source Element tag value is 0.

Disable the Controller Web Pages

CompactLogix



Compact GuardLogix



You can disable the controller web pages with Studio 5000 Logix Designer® application, version 28.00.00 or later.

You use a CIP Generic MSG to execute this option.

Controller web pages 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 the controller web page after it returns to its default settings.

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

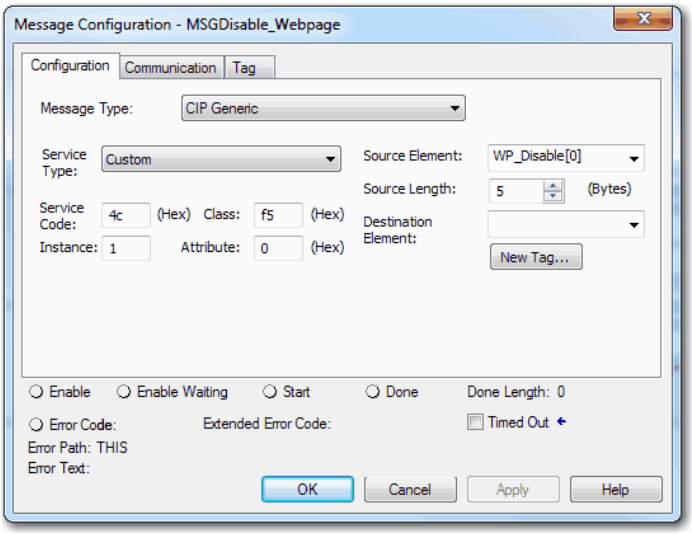
In this example, the controller tag is named WP_Disable and must match this graphic.

IMPORTANT The Source Element tag in your Logix Designer application project must match the values that are shown in the graphic.

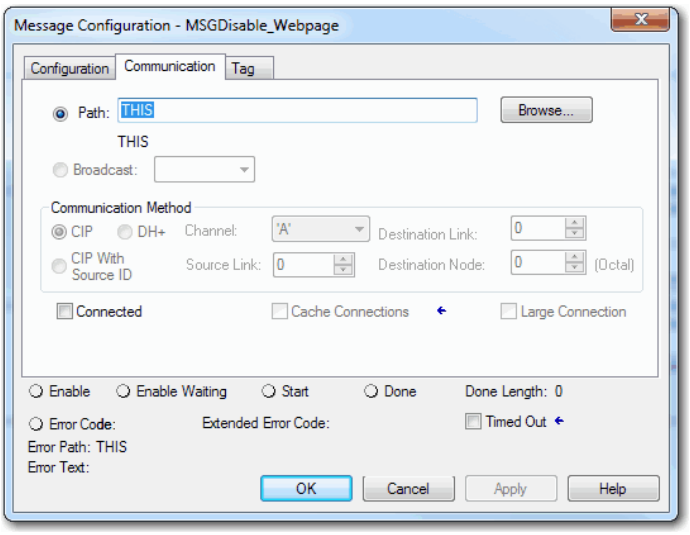
If you use values that are different than the ones shown, the controller web pages are not disabled.

◢ WP_Disable	{...}	{...}	Hex	SINT[5]
▷ WP_Disable[0]	16#00		Hex	SINT
▷ WP_Disable[1]	16#50		Hex	SINT
▷ WP_Disable[2]	16#00		Hex	SINT
▷ WP_Disable[3]	16#06		Hex	SINT
▷ WP_Disable[4]	16#00		Hex	SINT

– Source Length - 5



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



4. Before you enable the MSG instruction, consider the following:
   - To disable the controller web page, the last element in the SINT array for the Source Element must be 0.

WP_Disable	{...}	{...}	Hex	SINT[5]
WP_Disable[0]	16#00		Hex	SINT
WP_Disable[1]	16#50		Hex	SINT
WP_Disable[2]	16#00		Hex	SINT
WP_Disable[3]	16#06		Hex	SINT
WP_Disable[4]	16#00		Hex	SINT

   - To enable the controller web page, the last element in the SINT array for the Source Element must be 1.

WP_Disable	{...}	{...}	Hex	SINT[5]
WP_Disable[0]	16#00		Hex	SINT
WP_Disable[1]	16#50		Hex	SINT
WP_Disable[2]	16#00		Hex	SINT
WP_Disable[3]	16#06		Hex	SINT
WP_Disable[4]	16#01		Hex	SINT

Change Controller Type

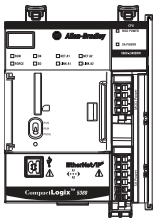
Safety controllers have special requirements and do not support certain standard features. You must understand the behavior of the system when changing the controller type from standard to safety, or from safety to standard, in your controller project.

Changing controller type affects the following:

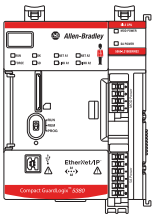
- Supported features
- Physical configuration of the project
- Controller properties
- Project components such as tasks, programs, routines, and tags
- Safety Add-On Instructions

Change from a Standard to a Safety Controller

CompactLogix



Compact GuardLogix



You can change from a CompactLogix™ 5380 controller to a Compact GuardLogix® 5380 controller in SIL 2/PLd 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:

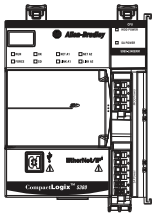
- The safety task is created only if the maximum number of downloadable tasks has not been reached. The safety task is initialized with its default values.

  TIP 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.

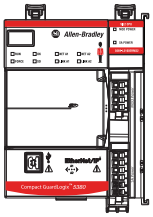
- Safety components are created (safety task, safety program, and so forth).
- A time-based safety network number (SNN) is generated for the local chassis.
- A time-based safety network number (SNN) is also generated for each embedded EtherNet/IP port.
- Standard controller features that are not supported 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

CompactLogix



Compact GuardLogix



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.

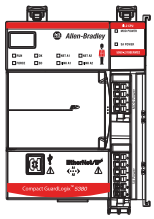
  TIP Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

If the safety controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

Change Safety Controller Types

Compact GuardLogix



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 controller, the application changes to SIL 2/PLd.

Safety Network Numbers are also preserved when you change to a Compact GuardLogix 5380 controller.

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Notes:

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

Publication 5069-UM001D-EN-P - April 2018
Supersedes Publication 5069-UM001C-EN-P - December 2016