Compact GuardLogix 5370 Controllers

Catalog Number(s) 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS, 1769-L37ERMS, 1769-L38ERMOS, 1769-L38ERMS

Allen-Bradley
by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 4

Communicate Over Networks

Chapter 5

Add and Configure Standard I/O Modules

Chapter 6

Add, Configure, Monitor, and Replace CIP Safety I/O Devices

Chapter 7

Elements of a Control Application

Chapter 8

Develop Safety Applications

Chapter 9

Develop Integrated Motion over an EtherNet/IP Network Application

Chapter 10

Go Online with the Controller

Chapter 11

Monitor Status and Handle Faults

Chapter 12

Appendix A

Appendix B

Notes:

About This Publication

This manual describes the necessary tasks to install, configure, program, and operate a Compact GuardLogix® 5370 controller. This manual is intended for automation engineers and control system developers.

Compact GuardLogix 5370 controllers are designed to provide solutions for small and medium-sized applications.

Download Firmware, AOP, EDS, and Other Files

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

Summary of Changes

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

Topic	Page
Removed installation information, see the Compact GuardLogix 5370 Controllers Installation Instructions, publication 1769-IN024	N/A

Terminology

This table defines terms that are used in this manual.

Abbreviation	Full Term	Definition
1oo2	One Out of Two	Refers to the behavioral design of a multi-processor safety system.
CIP™	Common Industrial Protocol	A communication protocol that is designed for industrial automation applications.
CIP Safety™	Common Industrial Protocol – Safety Certified	SIL 3/PLe-rated version of CIP.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
DLR	Device Level Ring	A communication protocol that allows multi-port EtherNet/IP™ devices to operate in ring topologies.
EN	European Norm	The official European standard.
GSV	Get System Value	An instruction that retrieves specified controller-status information and places it in a destination tag.
–	Multicast	The transmission of information from one sender to multiple receivers.
NAT	Network Address Translation	The translation of an Internet Protocol (IP) address to another IP address on another network.
PFD	Probability of a dangerous failure on demand	The average probability of a system to fail to perform its design function on demand.
PFH	Average frequency of a dangerous failure per hour	The average frequency of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
RPI	Requested Packet Interval	The expected rate in time for production of data when communicated over a network.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	An instruction that sets controller system data.
–	Standard	An object, task, tag, program, or component in your project that is not a safety-related item.
–	Unicast	The transmission of information from one sender to one receiver.

Additional Resources

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

Resource	Description
Compact GuardLogix 5370 Controllers Installation Instructions, publication 1769-IN024	Provides information on how to install, mount, and connect Compact GuardLogix controllers to a network.
CompactLogix System Selection Guide, publication 1769-SG001	Describes information about products that are used in a CompactLogix™ control system to assist you in the design of a control solution.
CompactLogix Controllers Specifications Technical Data, publication 1769-TD005	Provides controller specifications for all CompactLogix controllers.
GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099	Provides information on safety application requirements for GuardLogix 5570 and Compact GuardLogix 5370 controllers in Studio 5000 Logix Designer® applications.
CompactLogix 5370 L1 Controllers Installation Instructions, publication 1769-IN029	Provides information on how to install, mount, and connect CompactLogix 5370 L1 controllers to a network.
CompactLogix 5370 L2 Controllers Installation Instructions, publication 1769-IN090	Provides information on how to install, mount, and connect CompactLogix 5370 L2 controllers to a network.
CompactLogix 5370 L3 Controllers Installation Instructions, publication 1769-IN023	Provides information on how to install, mount, and connect CompactLogix 5370 L3 controllers to a network.
Armor Compact GuardLogix Controllers Installation Instructions, publication 1769-IN022	Provides information on how to install, mount, and connect Armor™ Compact GuardLogix controllers to a network.
Compact I/O Modules Installation Instructions, publication 1769-IN088	Describes how to install 1769 Compact I/O™ modules with any Compact GuardLogix controller.
Compact I/O Modules Specifications, publication 1769-TD006	Provides specifications for Compact I/O modules.
Compact I/O Expansion Power Supplies Installation Instructions, publication 1769-IN028	Describes how to wire the 1769 Compact I/O power supply.
Compact I/O DeviceNet Scanner Module Installation Instructions, publication 1769-IN060	Describes how to install the Compact I/O DeviceNet™ Scanner module.
1769-SDN DeviceNet Scanner Module User Manual, publication 1769-UM009	Describes how to use the 1769-SDN scanner module with Compact GuardLogix controllers.
Compact High-speed Counter Module User Manual, publication 1769-UM006	Describes high-speed counter operation for standalone 1769-HSC module when used with Compact GuardLogix controllers.
Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides advanced users with guidelines for system optimization and with system information to guide system design choices.
Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Guides all user levels in projects development for Logix 5000™ controllers and provides links to individual guides for information on topics, such as import/export, messages, security, and programming in different languages.
Logix Controllers Instructions Reference Manual, publication 1756-RM009	Provides information on the Logix 5000 instruction set that includes general, motion, and process instructions.
Logix 5000 Controllers Process Control/Drives Instruction Set Reference Manual, publication 1756-RM006	Details how to program the controller for process applications.
Execution Time and Memory Use for Logix 5000 Controller Instructions Reference Manual, publication 1756-RM087	Explains how to estimate the memory use and execution time of programmed logic, and how to select from different programming options.
Logix 5000 Controllers Motion Instructions Reference Manual, publication MOTION-RM002	Details how to program the controllers for motion applications.
Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003	Describes how to configure an Integrated Motion over an EtherNet/IP motion application and to start up that motion solution in a Logix 5000 control system.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Describes the following concepts that you must consider when you design a control system that includes an EtherNet/IP™ network: • EtherNet/IP overview • Ethernet infrastructure • EtherNet/IP protocol
EtherNet/IP Embedded Switch Technology Application Guide, publication ENET-AP005	Describes how to use a DLR network topology.
EtherNet/IP Socket Interface Application Technique, publication ENET-AT002	Describes socket interface applications.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

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

System Overview

The Compact GuardLogix® 5370 controllers offer state-of-the-art control, communication, and I/O elements in a distributed control package. This product family includes the following Compact GuardLogix controllers:

- 1769-L30ERMS
- 1769-L33ERMS
- 1769-L33ERMSK
- 1769-L36ERMS
- 1769-L37ERMS
- 1769-L38ERMS

The Armor™ Compact GuardLogix controller (1769-L33ERMOS, 1769-L36ERMOS, 1769-L37ERMOS(1), and 1769-L38ERMOS(1)) combines a Compact GuardLogix controller with a power supply in an IP67-rated housing for mounting on a machine. For information on how to install the Armor Compact GuardLogix controller, see the Armor Compact GuardLogix Controllers Installation Instructions, publication 1769-IN022.

For a complete description of the Compact GuardLogix® 5370 control system components and functionality, see page 14.

Safety Application Requirements

The Compact GuardLogix 5370 controller system is certified for use in safety applications up to and including Safety Integrity Level (SIL) 3 and Performance Level (PL)e, in which the de-energized state is the safe state. Safety application requirements include evaluating probability of failure rates (PFD and PFH), system reaction time settings, and functional-verification tests that fulfill SIL 3/PLe criteria.

For SIL 3 and PLe safety system requirements, including functional validation test intervals, system reaction time, and PFD/PFH calculations, refer to the GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099. You must read, understand, and fulfill these requirements before operating a Compact GuardLogix SIL 3, PLe safety system.

(1) Available at firmware revision 31.

Compact GuardLogix-based SIL 3/PLe safety applications require the use of at least one safety network number (SNN) and a safety task signature. Both affect controller and I/O configuration and network communication.

For more information, see the GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099.

Safety Network Number

The safety network number (SNN) must be a unique number that identifies safety subnets. Each safety subnet that the controller uses for safety communication must have a unique SNN. Each CIP Safety™ device must also be configured with the safety subnet's SNN. The SNN can be assigned automatically or manually.

For information on SNN assignment, see Manage the Safety Network Number (SNN) on page 46.

Safety Task Signature

The safety task signature consists of an ID number, date, and time that uniquely identifies the safety portion of a project. This includes safety logic, data, and configuration. The Compact GuardLogix system uses the safety task signature to determine the project's integrity and to let you verify that the correct project is downloaded to the target controller. Creation, recording, and verification of the safety task signature is a mandatory part of the safety-application development process.

See Generate a Safety Task Signature on page 131 for more information.

Distinguish Between Standard and Safety Components

Slots in the Compact GuardLogix backplane that are not used by the safety function can be populated with other CompactLogix™ modules that are certified to the Low Voltage and EMC Directives.

See the product certifications at rok.auto/certifications to find the CE certificate for the Programmable Control–CompactLogix Product Family and determine which modules are certified.

You must create and document a clear, logical, and visible distinction between the safety and standard portions of the controller project. To aid in the creation of this distinction, the Logix Designer application features safety identification icons to identify the safety task, safety programs, safety routines, and safety components. In addition, the Logix Designer application uses a safety class attribute that is visible whenever safety task, safety programs, safety routine, safety tag, or safety Add-On Instruction properties are displayed.

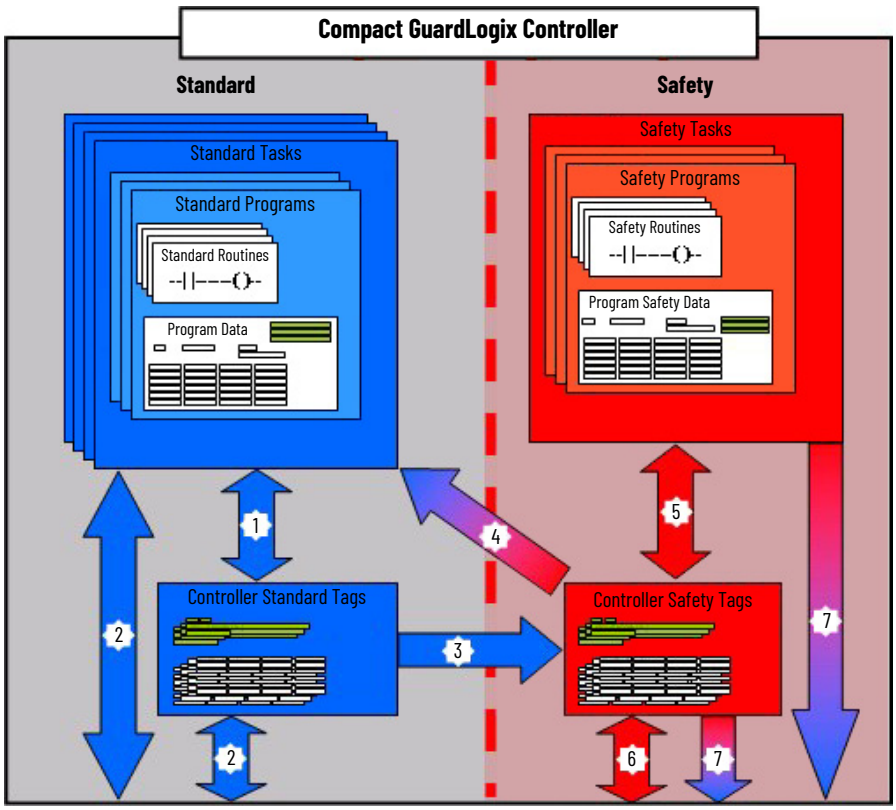
The controller does not allow writes to safety tag data from external human-machine interface (HMI) devices or via message instructions from peer controllers. The Logix Designer application can write safety tags when the Compact GuardLogix controller is safety-unlocked, does not have a safety task signature, and is operating without safety faults.

HMI Devices

HMI devices can be used with Compact GuardLogix controllers. HMI devices can access standard tags like a standard controller does. However, HMI devices cannot write to safety tags; safety tags are read-only for HMI devices.

Controller Data Flow Capabilities

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



No.	Description
1	Standard tags and logic behave the same way that they do in the standard Logix platform.
2	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.
3	Compact GuardLogix controllers are integrated controllers with the ability to move (map) standard tag data into safety tags for use within the safety task.
	ATTENTION: This data must not be used to control a SIL 3/PLe output directly.
4	Standard logic can directly read controller-scoped safety tags.
5	Safety logic can read or write Safety tags.
6	GuardLogix 5570 and Compact GuardLogix 5370 controllers can exchange Safety tags over an Ethernet network.
7	External devices (such as HMI devices, personal computers, or other standard controllers) can read Safety tag data, program- or controller-scoped.
	IMPORTANT Once this data is read, it is considered standard data, not SIL 3/PLe data.

System Components

This table describes components that are used in a typical Compact GuardLogix 5370 controller system.

System Component	Description
Controller	One of the controllers that is documented in this publication
Power supply	One of the following 1769 Compact I/O™ power supplies: • 1769-PA2 • 1769-PB2(1) • 1769-PA4 • 1769-PB4
Communication networks components	Any of the following: • EtherNet/IP™ network via built-in EtherNet/IP network ports (safety and standard communication) • DeviceNet™ network via a 1769-SDN module (only for standard communication)(2) • USB connection only for programming and firmware updates
Software	• Logix Designer application, version 28.00.00 or later • RSLinx® Classic software, version 3.80.xx or later • RSNetWorx™ for DeviceNet software, version 25.00.00 or later
Secure Digital (SD) card for external nonvolatile memory	• 1784-SD1 card - Ships with the Compact GuardLogix 5370 controller and offers 1 GB of memory • 1784-SD2 card - Available for separate purchase and offers 2 GB of memory
I/O modules(3)	• Local expansion modules- 1769 Compact I/O modules • Distributed I/O - Multiple I/O module product lines over DeviceNet and EtherNet/IP networks
Reset button	If pressed and held in when the controller power-ups, this button clears the user program from the internal memory of the controller and from the internal safety partner.

(1) Armor Compact GuardLogix controller systems have this power supply inside their IP67-rated housings.
(2) For safety communication, a bridge is required that goes from Ethernet to DeviceNet; see page 79.
(3) Armor Compact GuardLogix controller systems do not support I/O inside their IP67-rated housings. To get I/O, you must connect via EtherNet/IP to distributed I/O.

Controller Functionality

The following table describes the functionality available with Compact GuardLogix 5370 controllers.

Cat. No.	Controller Tasks Supported	Programs Supported Per Task	Internal Energy Storage Solution	EtherNet/IP Network Topology Support	Power Supply Distance Rating	Onboard User Memory Size (MB)		Local Compact I/O Module Support	Motion Axes
						Standard	Safety		
1769-L30ERMS	32(1)	100	Yes - No battery needed	Support the following topologies: • Device Level Ring (DLR) • Linear • Traditional star	4	1	0.5	As many as 8	4
1769-L33ERMS 1769-L33ERMSK						2	1	As many as 16	8
1769-L33ERMOS								—	
1769-L36ERMS						3	1.5	As many as 30	16
1769-L36ERMOS								—	
1769-L37ERMOS(2)						4			
1769-L37ERMS(2)								As many as 30	
1769-L38ERMOS(2)						5		—	
1769-L38ERMS(2)								As many as 30	

(1) Includes one safety task.
(2) Available at firmware revision 31.

Programming Requirement

Use the following table to identify the programming tool and the versions for use with your Compact GuardLogix 5370 controllers.

Software Versions

Cat. No.	Studio 5000® Environment	RSLinx® Classic Software Version
1769-L30ERMS 1769-L33ERMS 1769-L33ERMSK 1769-L33ERMOS 1769-L36ERMS 1769-L36ERMOS	28.00.00 or later	3.80 or later
1769-L37ERMOS 1769-L37ERMS 1769-L38ERMOS 1769-L38ERMS	31.00.00 or later	4.00 or later

Safety routines include safety instructions, which are a subset of the standard ladder logic instruction set, and safety application instructions. Programs that are scheduled under the safety task support only ladder logic.

Supported Versions

Feature	Studio 5000 Logix Designer® Application	
	Safety Task	Standard Task
Add-On Instructions	X	X
Alarms and events		
Controller logging	X	
Data access control		
Equipment phase routines		
Event tasks		
Firmware Supervisor	X	
Function block diagrams (FBD)		
Integrated motion		
Ladder logic	X	
Language switching		
Memory card		
Network Address Translation (NAT)		
Online import and export of program components		
Safety and standard connections	X	
Sequential function chart (SFC) routines		
Structured text		
Unicast connections for produced and consumed safety tags	X	
Unicast connections for safety I/O devices on EtherNet/IP networks		

For information on how to use these features, refer to the Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001, the publications that are listed in Additional Resources on page 10, and online help.

Notes:

Complete the Controller Setup

To complete the tasks that are described in this chapter, you must have the following software on your computer.

- RSLinx™ Classic software
- Studio 5000™ environment
- BOOTP-DHCP server (installed with RSLinx Classic)
- ControlFLASH™ (installed with Studio 5000 environment)

Compact GuardLogix® 5370 controllers require a network Internet Protocol (IP) address to operate on an EtherNet/IP™ network.

Set the IP Address

The IP address uniquely identifies the controller. The IP address is in the form *xxx.xxx.xxx.xxx* where each *xxx* is a number from 000...254 with some exceptions for reserved values. These numbers are **examples** of reserved values that you cannot use:

- 000.*xxx.xxx.xxx*
- 127.*xxx.xxx.xxx*
- 224 to 255.*xxx.xxx.xxx*

Some other values are reserved based on an application-by-application basis.

You can complete one of these tasks dependent on system conditions:

- **Set** the IP address for a controller that does not have one assigned.
- **Change** the IP address for a controller that has an IP address that is assigned to it.

IMPORTANT	Compact GuardLogix 5370 controllers have two EtherNet/IP ports to connect to an EtherNet/IP network; you cannot install any additional ports to these controllers. The EtherNet/IP ports carry the same network traffic as part of the embedded switch of the controller. However, the controllers use only one IP address.

You must set the IP address of a Compact GuardLogix 5370 controller when the controller powers up for the first time, that is, when commissioning the controller for the first time. You are not required to set an IP address each time that power is cycled to the controller.

You can use these tools to **set** the IP address of a Compact GuardLogix 5370 controller:

- Bootstrap Protocol (BOOTP) server
- Dynamic Host Configuration Protocol (DHCP) server
- RSLinx Classic software
- Logix Designer application
- SD card

Use the BOOTP Server to Set the IP Address

Bootstrap Protocol (BOOTP) is a protocol that enables the controller to communicate with a BOOTP server. The server can be used to assign an IP address. You can use the BOOTP server to set an IP address for your Compact GuardLogix 5370 controller.

Consider these points when using the BOOTP server:

- The BOOTP server is installed automatically when you install RSLinx Classic or the Studio 5000 environment on your computer. The BOOTP server sets an IP address and other Transmission Control Protocol (TCP) parameters.
- The controller ships from the factory without an IP address and BOOTP-enabled.
- This section describes how to use a Rockwell Automation BOOTP/DHCP server. If you use another BOOTP/DHCP server, contact your network administrator to verify that you are using it correctly.
- To use the BOOTP server, your computer and the controller must be connected to the same EtherNet/IP network.
- If the controller is BOOTP-disabled, you cannot use the BOOTP server to set the IP address.

There are two conditions in which the Compact GuardLogix 5370 controllers use the BOOTP servers to set the IP address of the controller:

- **Initial power-up** - Because the Compact GuardLogix 5370 controller ships with BOOTP-enabled, when it is first powered up, the controller sends a request for an IP address on the EtherNet/IP network. You can use the BOOTP server to set the IP address, as described later in this section.
- **Power-up after controller operation has begun** - When controller power is cycled after operation has begun, the BOOTP/DHCP server sets the IP address if one of these conditions exists:
  - Controller is BOOTP-enabled - You set the IP address manually with the BOOTP server.
  - Controller is DHCP-enabled - The IP address is set automatically via the DHCP server.

Access the BOOTP/DHCP utility from one of these locations:

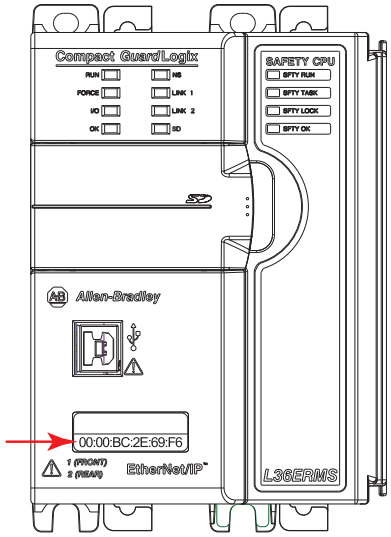
- Start>Programs>Rockwell Software>BOOTP-DHCP Server

  If you have not installed the utility, you can download and install it from rok.auto/pcdc.
- Tools directory on the programming software installation CD

IMPORTANT

Before you start the BOOTP/DHCP utility, make sure that you have the hardware (MAC) address of the controller. The hardware address is on the front of the controller and uses an address in a format similar to the following:

00:00:BC:2E:69:F6



Use the DHCP Server to Set the IP Address

Dynamic Host Configuration Protocol (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. The main difference is that BOOTP manual configuration (static), while DHCP enables static and dynamic allocation of network addresses and configurations to newly attached controllers.

Be cautious when you use the DHCP server to configure a controller. A BOOTP client, such as the CompactLogix™ controllers, can start from a DHCP server only if the DHCP server is written to handle BOOTP queries. This requirement is specific to the DHCP server used. Consult your system administrator to see if a DHCP server supports BOOTP commands and manual IP allocation.

ATTENTION:
Assign a fixed network address to the Compact GuardLogix 5370 controllers. The IP address of this controller is not to be dynamically provided. Failure to observe this precaution can result in unintended machine motion or loss of process control.

If you use the Rockwell Automation BOOTP or DHCP server in an up-linked subnet where a DHCP server exists, a controller can procure an address from the enterprise server before the Rockwell Automation utility even sees the controller. Disconnect from the up-link to set the address and configure the controller to retain its static address before reconnecting to the up-link, if necessary.

Use the RSLinx Classic Software to Set the IP Address

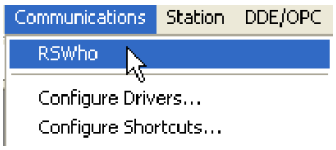
You can use RSLinx software to set the IP address of the Compact GuardLogix 5370 controller.

IMPORTANT This section explains how to assign an IP address to a Compact GuardLogix controller that does not have one already.
To assign an IP address to a Compact GuardLogix controller via RSLinx software, you must be first connected to your controller via the USB port.

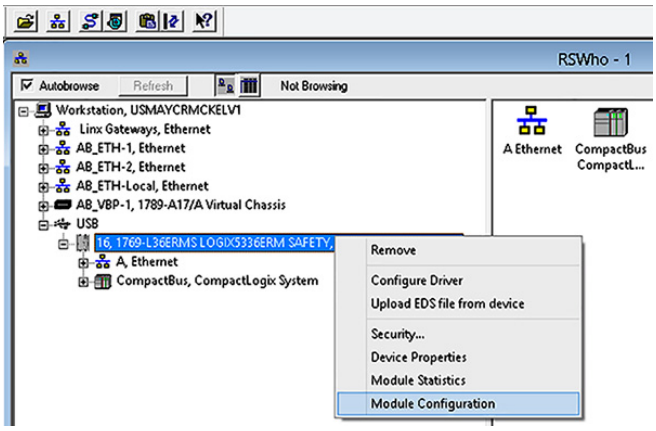
Complete these steps to set the IP address of the controller with RSLinx software.

IMPORTANT These steps show a 1769-L36ERMS controller. The same steps would also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

1. Make sure that a USB cable is connected to your computer and the controller.
2. Start RSLinx software.
   After several seconds, an RSWho dialog box appears.
3. If no RSWho dialog box appears, from the Communications pull-down menu, choose RSWho.

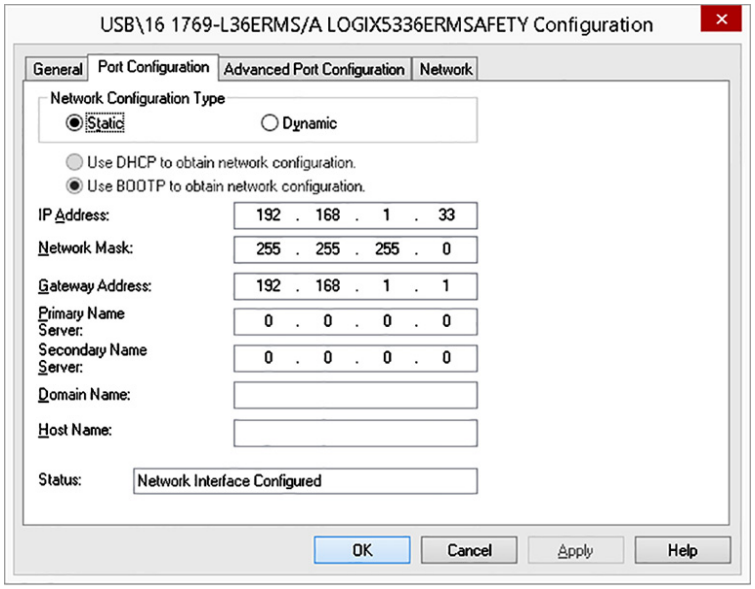


   The RSWho dialog box appears and includes the USB driver.
4. Right-click the EtherNet/IP module and choose Module Configuration.



   The Module Configuration dialog box appears.

5. Click the Port Configuration tab.



6. For Network Configuration Type, select Static to assign this configuration to the port.

IMPORTANT If you click Dynamic on a power cycle, the controller clears the current IP configuration and starts to send BOOTP requests.

7. Type the new IP address and Network Mask.
8. Click OK.

As with all configuration changes, make sure that you are using the SD card in a way that does not overwrite the IP address at the next controller power cycle.

For more information about the SD card, see Store and Load Programs with a Secure Digital Card on page 155.

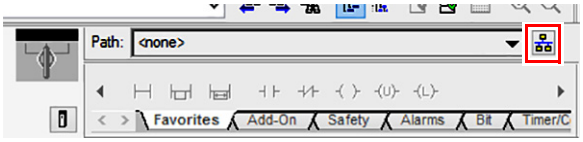
Use the Studio 5000 Environment to Set the IP Address

You can use the Logix Designer application to set the IP address of a Compact GuardLogix 5370 controller. To set the IP address via the application, you must be connected to your controller via the USB port.

Complete these steps to set the IP address of the controller.

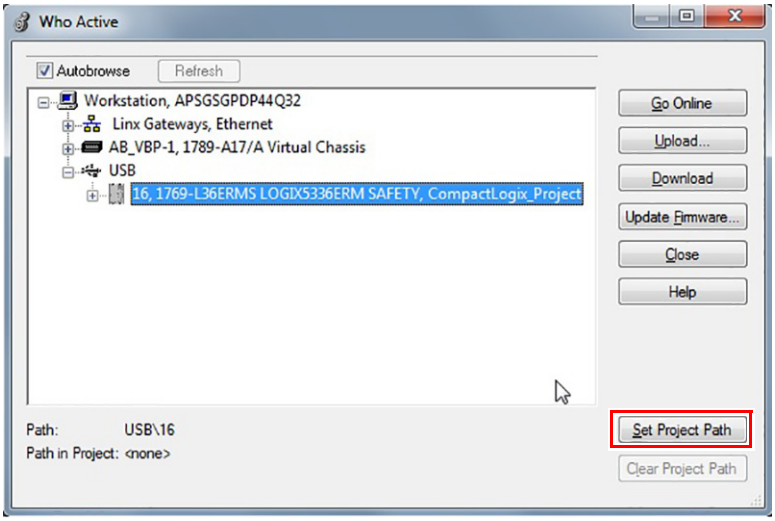
IMPORTANT These steps show a 1769-L36ERMS controller. The same steps also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

1. Start the Logix Designer application.
2. To specify the project path, click RSWho .

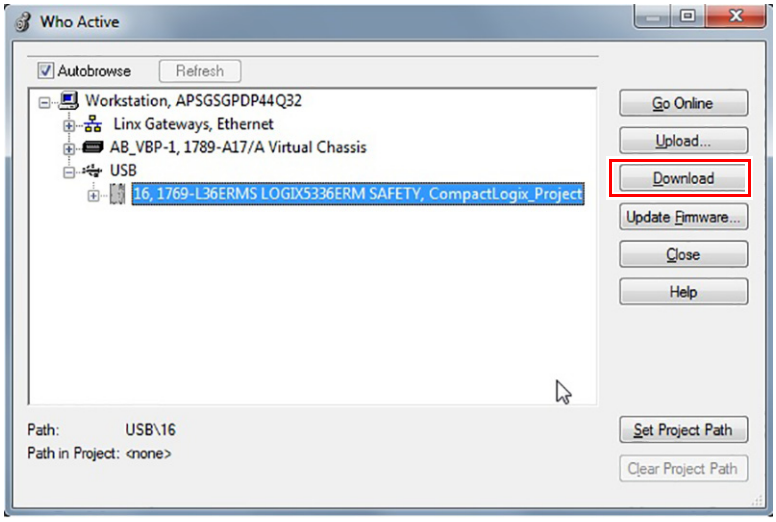


The RSWho Active dialog box appears.

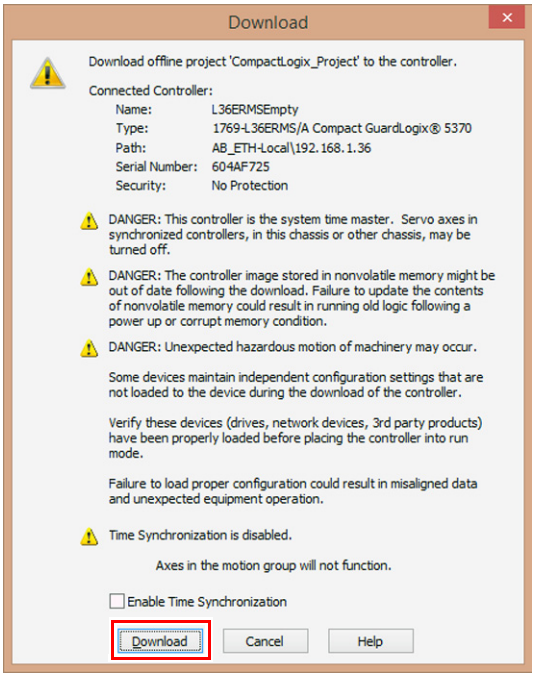
3. Navigate over the USB network and select the Compact GuardLogix controller.
4. Click Set Project Path.



5. Click Download.

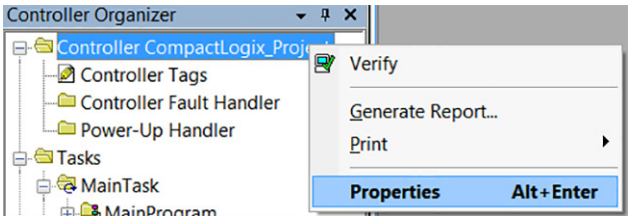


6. Click Download again.



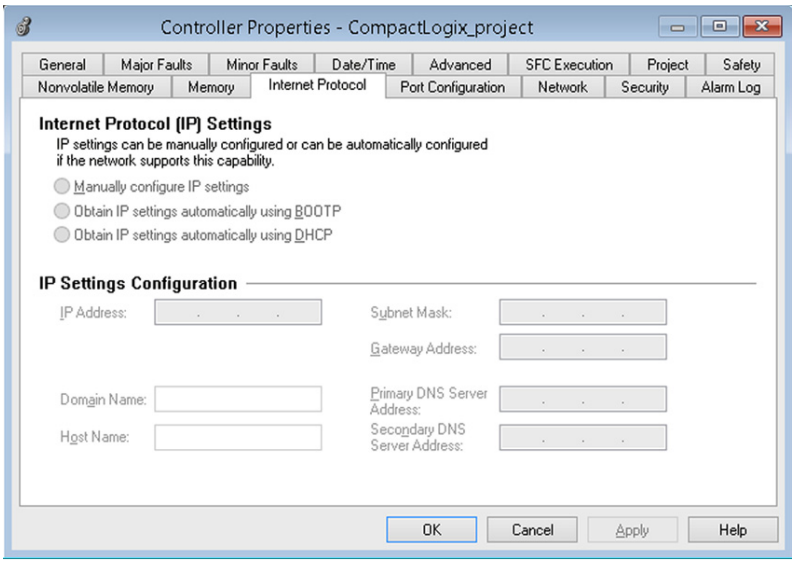
The new project is downloaded to the controller and the project goes online, in Remote Program or Program mode.

7. Right-click the controller name and choose Properties.

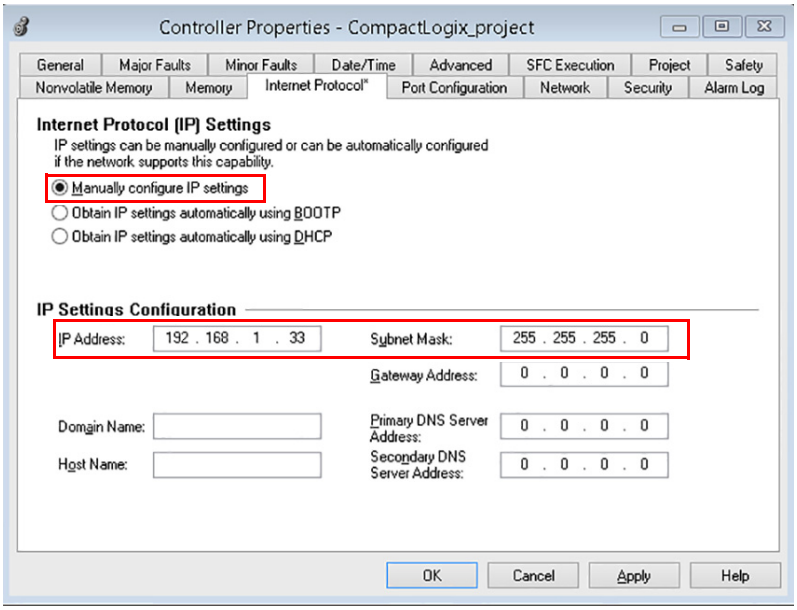


8. On the Controller Properties dialog box, click the Internet Protocol tab.

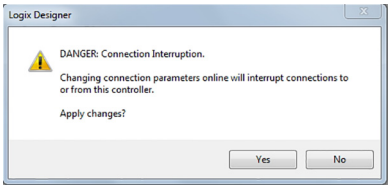
   The IP Settings Configuration values show that the controller has no IP address that is assigned to it.



9. Click Manually configure IP settings.
10. Enter desired IP address and other configuration information, and click OK.



11. When prompted to confirm the IP address setting, click Yes.



The controller now uses the newly set IP address.

Use the SD Card to Set the IP Address

You can use an SD card to set the IP address for a Compact GuardLogix 5370 controller. If you use the SD card to set the IP address, then it removes the need for software to complete this task.

IMPORTANT	To set the IP address from an SD card, software is not required during the power-up process. However, you must have previously saved the project to the SD card. The IP address of the Compact GuardLogix 5370 controller is automatically configured at power-up as long as you have configured an IP address, stored the program onto a controller, and set the SD card to the Load Image parameter set to On Power Up. The option to set the IP address of a Compact GuardLogix 5370 controller via an SD card at power-up is only one part of the process to load an entire project to the controller from the SD card. Use this option carefully. For example, the SD card can contain a desirable IP address as part of an undesirable project, for example, a project that is older than the project currently used on the controller.

These requirements apply when using the SD card to set the IP address on a Compact GuardLogix 5370 controller:

- A project must be stored on the SD card.
- The project that is stored on the SD card is configured with the Load Image parameter set to On Power Up.

Additional requirements apply for safety projects. See Chapter 12 and the GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual, publication 1756-RM099.

Change the IP Address

You can change the IP address of a Compact GuardLogix 5370 controller after system operation has begun. In this case, the controller has an IP address that is assigned to it, but you must change that IP address.

You can use these tools to change the IP address of a controller:

- RSLinx Classic software
- Studio 5000 Logix Designer® application
- SD card

IMPORTANT	You **cannot** use either of these tools to **change** the IP address of a controller: • Bootstrap Protocol (BOOTP) server • Dynamic Host Configuration Protocol (DHCP) server

Consider these factors when you determine how to change the IP address of a controller:

- Network isolation from, or integration into, the plant/enterprise network
- Network size - For large, isolated networks, it can be more convenient and safer to use a BOOTP/DHCP server rather than the Studio 5000 environment or RSLinx Classic software. A BOOTP/DHCP server limits the possibility of duplicate IP address assignment.

However, you can only use the BOOTP/DHCP server to **set** the IP address of the controller and not to change it. If you decide to change the IP address of the controller and want to use a BOOTP/DHCP server to limit the possibility of duplicate IP address assignment, you must first clear the IP address.

After clearing the IP address, use the steps that are described at Use the BOOTP Server to Set the IP Address on page 18 or Use the DHCP Server to Set the IP Address on page 19 to set the IP address of the controller.

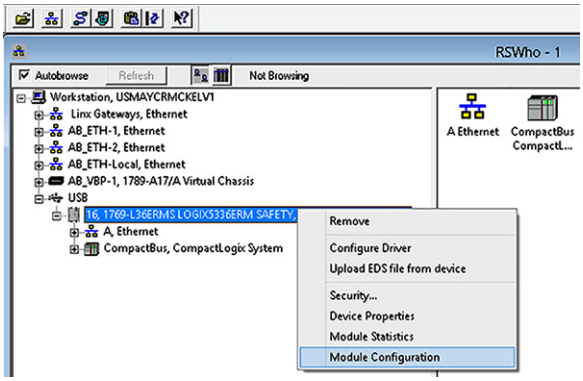
- Company policies and procedures that deal with plant floor network installation and maintenance
- Level of involvement by IT personnel in plant-floor network installation and maintenance
- Type of training that is offered to control engineers and maintenance personnel

Change the IP Address with RSLinx Software

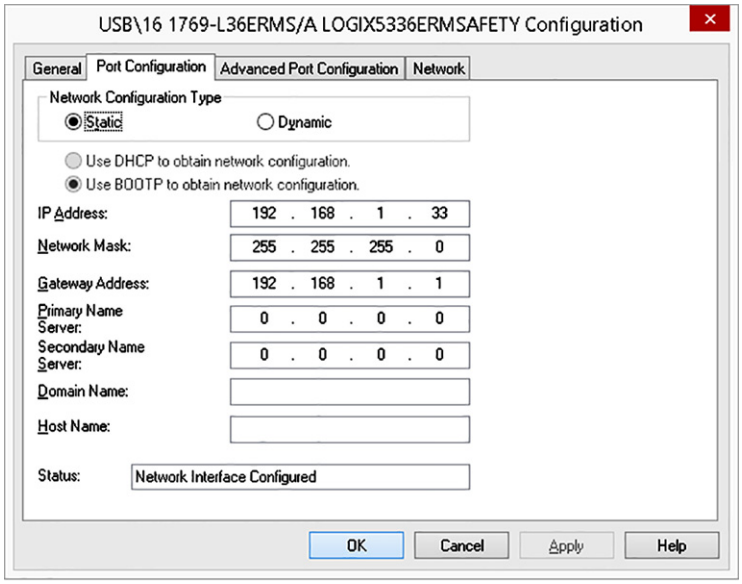
Complete these steps to change the IP address of the controller.

IMPORTANT These steps show a 1769-L36ERMS controller. The same steps also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

1. Verify that a USB cable is connected to your computer and the controller.
2. Right-click the controller and choose Module Configuration.



3. Click the Port Configuration tab.



The controller has an IP address and Network Configuration Type.

4. Type the new IP address and Network Mask.
5. For Network Configuration Type, select Static to assign this configuration to the port.

IMPORTANT If you click Dynamic on a power cycle, the controller clears the current IP configuration and starts to send BOOTP requests.

6. Click OK.

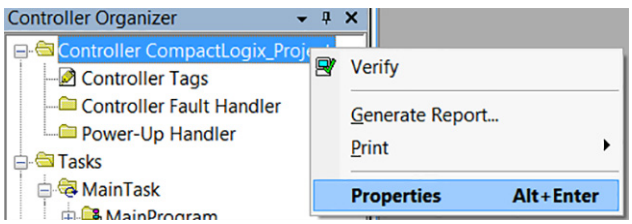
Change the IP Address with Logix Designer Application

You can change the IP address of a Compact GuardLogix 5370 controller via the Logix Designer application over a USB or EtherNet/IP network connection.

Complete these steps to change the IP address of the controller.

IMPORTANT These steps show a 1769-L36ERMS controller. The same steps also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

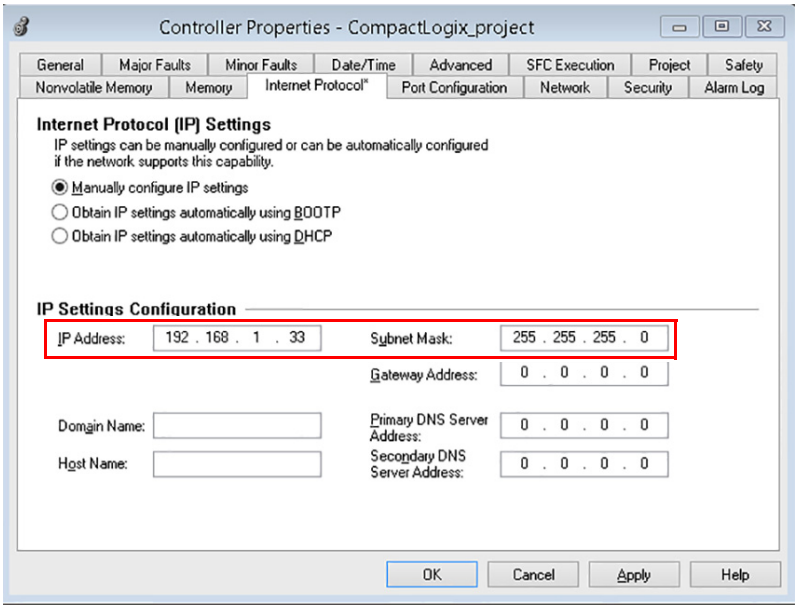
1. Verify that your computer is connected to the controller.
2. Verify that your project is online.
3. Right-click the controller name and choose Properties.



You can also right-click the Ethernet node in the I/O Configuration section and choose Properties.

The Controller Properties dialog box appears on the Internet Protocol tab.

4. Change the IP address of the controller.
5. Make other changes where necessary.



6. Click OK.

Change the IP Address with an SD Card

You can use an SD card to change the IP address for a Compact GuardLogix 5370 controller when the controller power is cycled. If you use the SD card to change the IP address, then you do not need software to complete this task.

IMPORTANT To set the IP address from an SD card, software is not required during the power-up process. However, you must have previously saved the project to the SD card.

These requirements apply when using the SD card to change the IP address on a Compact GuardLogix 5370 controller:

- A project is stored on the SD card.
- The project that is stored on the SD card includes another IP address for the Compact GuardLogix 5370 controller than the IP address currently in use on the physical controller that houses the SD card.
- The project that is stored on the SD card is configured with the Load Image parameter set to On Power Up.
- Power is cycled to the controller with the SD card installed.

Additional requirements apply for safety projects. See Chapter 12 and the GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual, publication 1756-RM099.

Load Controller Firmware

You must download the current firmware before you can use the Compact GuardLogix 5370 controller.

IMPORTANT Do not interrupt a firmware update while it is in process. Firmware update interruption can cause the firmware revision of the Compact GuardLogix controller to revert to its out-of-the-box revision level, that is, 1.*xxx*.

To load firmware, you can use any of the following:

- ControlFLASH software that installs with Logix Designer application
- The AutoFlash feature that launches through the application when you download a project and the controller does not have the matching firmware revision
- SD card (catalog numbers 1784-SD1 or 1784-SD2) with an image that is stored on the card

If you use ControlFLASH software or the AutoFlash feature, you need an EtherNet/IP network or USB connection to the controller.

IMPORTANT The controller firmware revision, which is loaded via ControlFLASH software or the AutoFlash feature, can be overwritten after future controller power cycles if conditions exist that are described in Use the Secure Digital Card to Load Firmware on page 34.

The firmware is available with the application or you can download it from the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at rok.auto/pcdc.

Use the ControlFLASH Software to Load Firmware

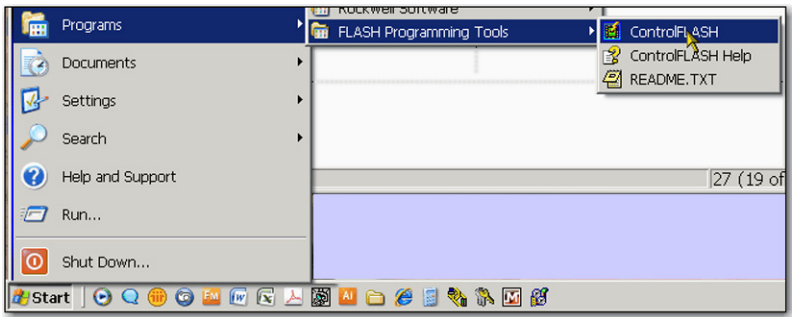
You can use the ControlFLASH software to load firmware through a USB or EtherNet/IP network connection. We recommend the following when you load firmware via the ControlFLASH software:

- Use a USB connection to load the firmware.
- If one is installed in the controller, remove the SD card.

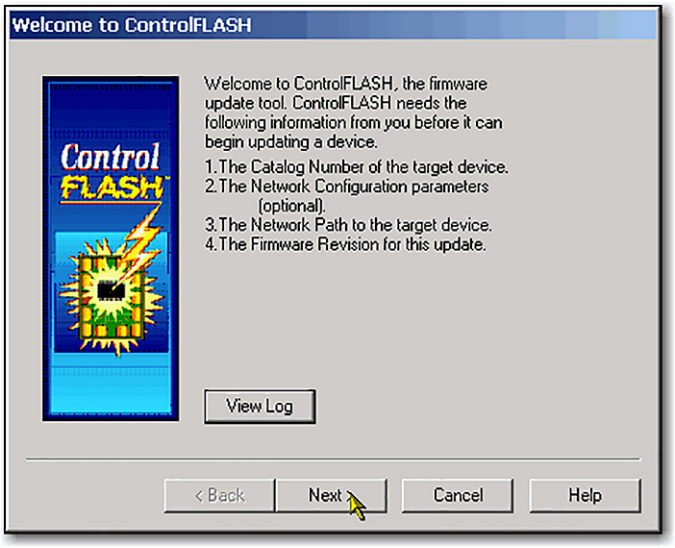
Complete these steps to use the ControlFLASH software to load firmware.

IMPORTANT These steps show a 1769-L36ERMS controller. The same steps would also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

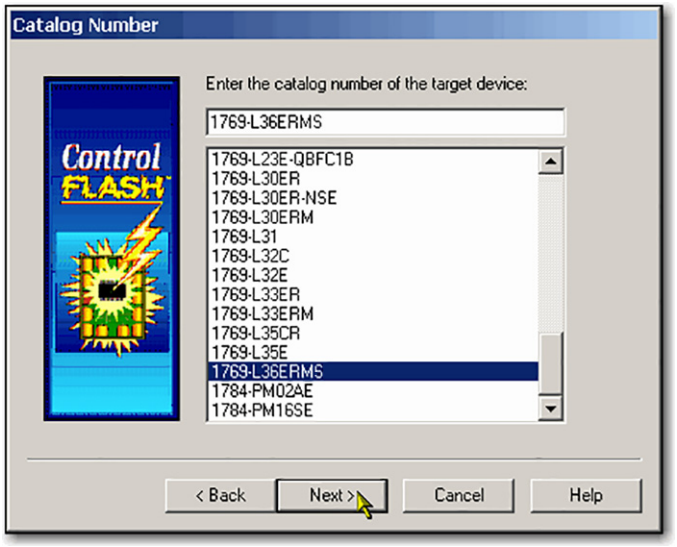
1. Verify that a connection exists between your computer and the Compact GuardLogix 5370 controller.
2. Choose Start>Programs>FLASH Programming Tools>ControlFLASH.



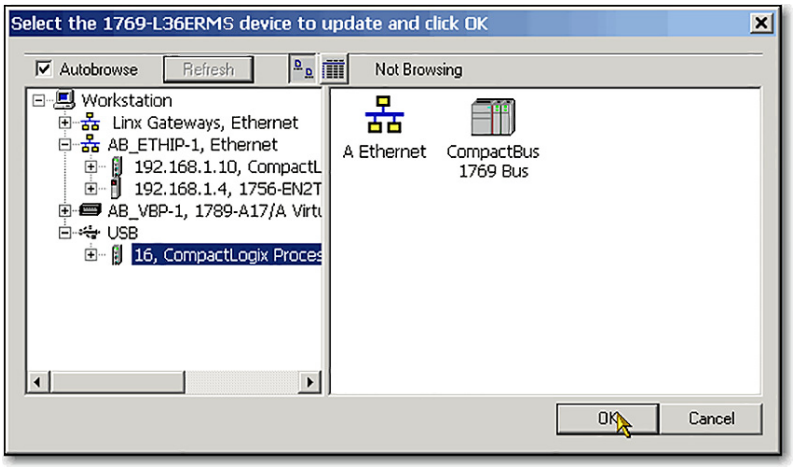
3. When the Welcome dialog box appears, click Next.



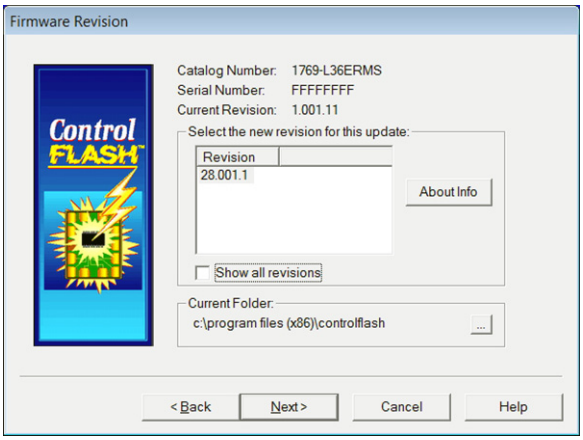
4. Choose the controller catalog number and click Next.



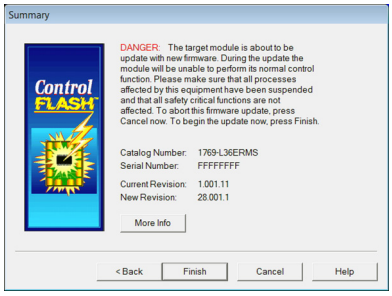
5. Expand the network until you see the controller.
6. Choose the controller at the first instance in which it appears, as shown in the following graphic, and click OK.

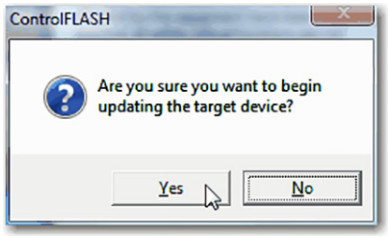


7. Choose the revision level to which you want to update the controller and click Next.

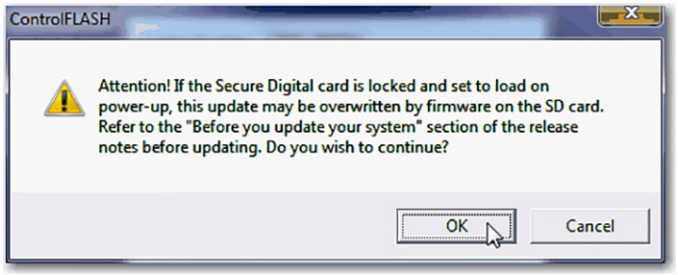


8. To start the update of the controller, click Finish and click Yes.

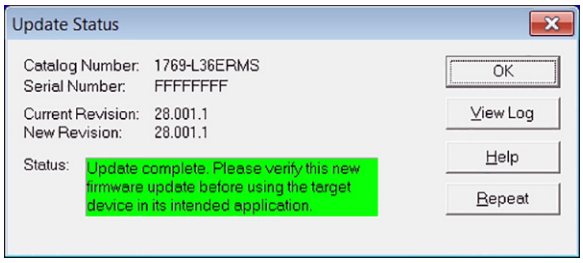




Before the firmware update begins, you see the following dialog box. Take the required action for your application. In this example, the upgrade continues when OK is clicked.



After the controller is updated, the status dialog box displays that the update is complete.



9. Click OK.
10. To close the ControlFLASH software, click Cancel and click Yes.

Use the AutoFlash Feature to Load Firmware

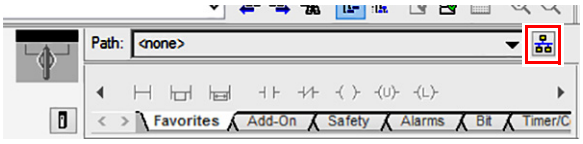
You can use the AutoFlash feature to load firmware through a USB or EtherNet/IP network connection.

Let the upgrade complete without interruption. If you interrupt a firmware update that is in process, you are alerted that an error has occurred. In this case, cycle power to the controller. The firmware revision level reverts to the 1.*xxx* revision level and you can begin the upgrade process again.

Complete these steps to use the AutoFlash feature to load firmware.

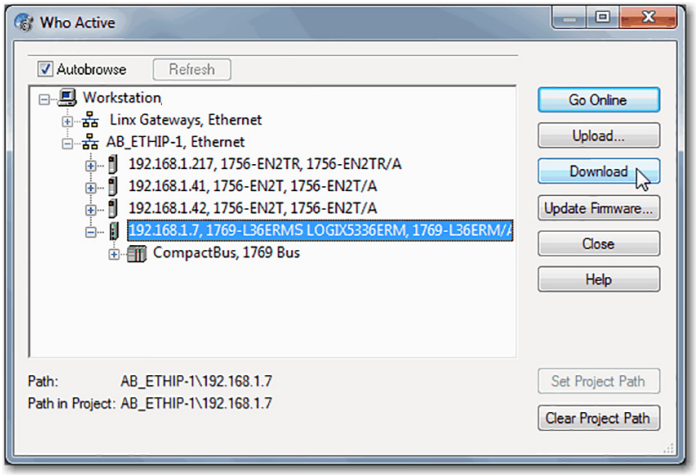
IMPORTANT These steps show a 1769-L36ERMS controller. The same steps would also apply to all Compact GuardLogix 5370 controllers with slight variations in screens.

1. Make sure that the network connection is made and your network driver is configured in RSLinx Classic software.
2. Create a controller project.
3. To specify the controller path, Click RSWho .



The RSWho Active dialog box appears

4. Navigate over the Ethernet network and select the Compact GuardLogix controller.

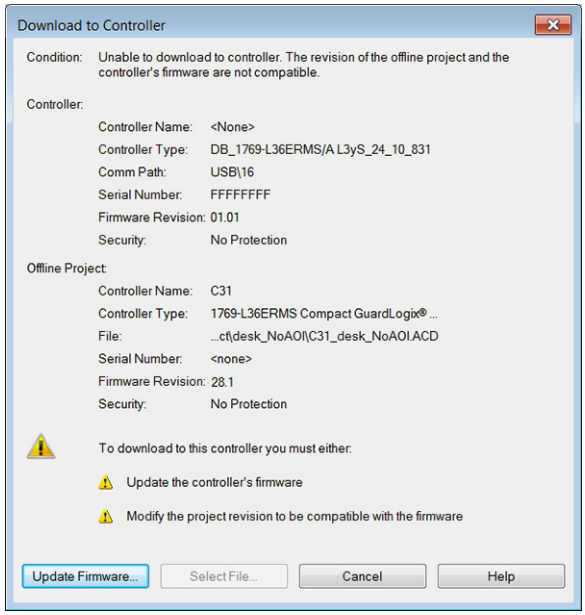


5. Click Download.

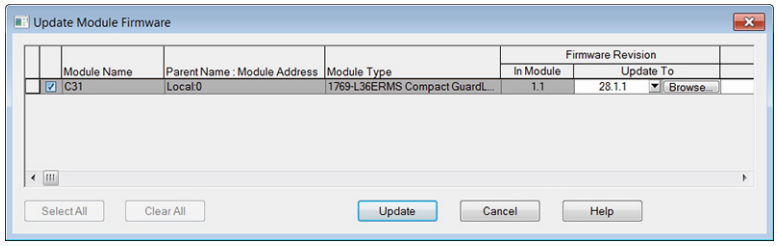
You can click Update Firmware instead of Download to complete this process. If you do so, skip to step 6.

A dialog box appears to indicate that the project revision and controller firmware revision are different.

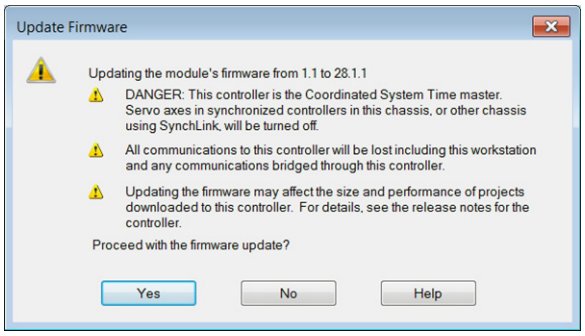
6. Click Update Firmware.



7. Use the checkbox and pull-down menu to choose your controller and firmware revision.
8. Click Update.



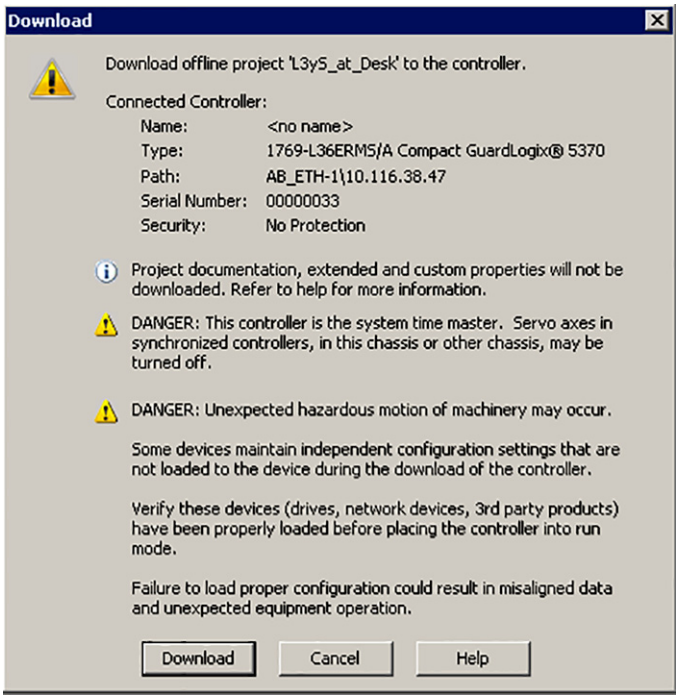
9. When the Update Firmware dialog box appears, click Yes.



Before the firmware update begins, you may be warned that your controller missing the SD card. Take the required action (typically click OK).

The firmware update begins.

10. When the firmware update is complete, a Download dialog box appears. In this example, the project download to the controller continues when Download is clicked.



Use the Secure Digital Card to Load Firmware

You can use an installed SD card to load firmware on a Compact GuardLogix 5370 controller. If you use the SD card to load firmware, then it removes the need for software to complete this task.

IMPORTANT	An installed SD card automatically updates the firmware of the Compact GuardLogix 5370 controller, if the SD card was configured with the Load Image parameter set to On Power Up.

Your application requires the following to load firmware from an SD card at power-up:

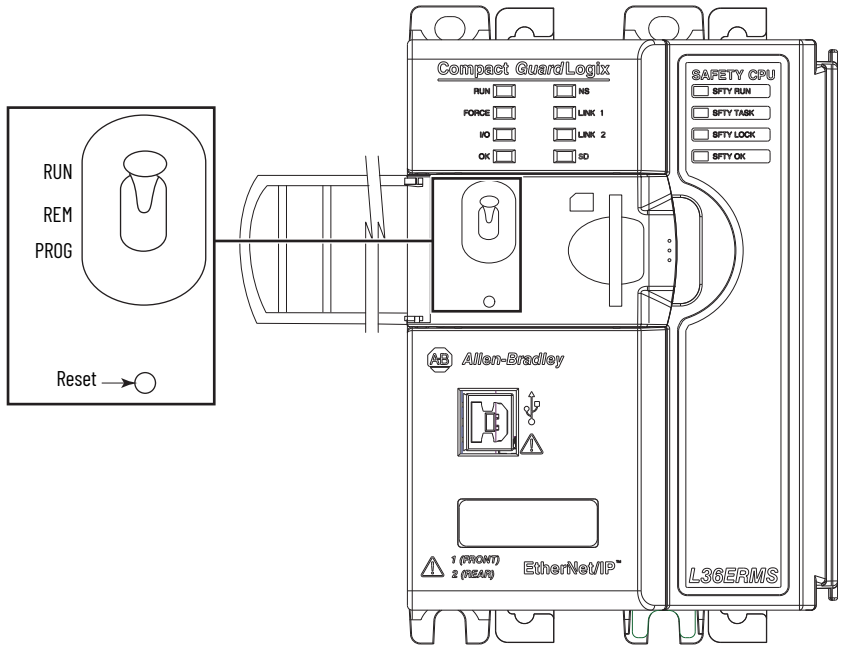
- You must have saved the project to the SD card before the power cycle.
- The firmware revision in the project that is stored on the SD card differs from the firmware revision on the Compact GuardLogix 5370 controller.

Additional requirements apply for safety projects. See Chapter 12 and the GuardLogix 5570 and Compact GuardLogix 5370 Controllers Safety Reference Manual, publication 1756-RM099.

Select the Controller Mode

WARNING: When you change switch settings 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 you proceed.

The following graphic shows the mode switch on a Compact GuardLogix 5370 controller. Use the mode switch on the controller to set the operating mode.



IMPORTANT Restrictions apply for safety applications. See Chapter 8, Develop Safety Applications, and the GuardLogix 5570 and Compact GuardLogix 5370 Safety Reference Manual, publication 1756-RM099, for detailed information on programming restrictions.

Controller Mode Descriptions

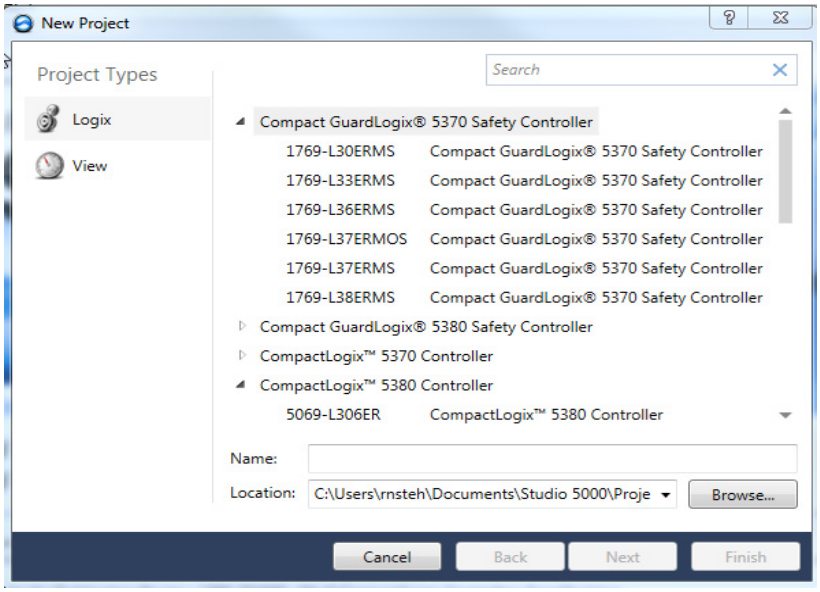
Mode Switch Position	Description	
Run	You can perform these tasks: • Upload projects. • Run the program and enable outputs. You cannot perform these tasks: • Update controller firmware. • Create or delete tasks, programs, or routines. • Create or delete tags or edit online. • Import a program to the controller. • Change the port configuration of the controller, advanced port configuration, nor network configuration settings. • Change controller configuration parameters that are directly set for operation on a Device Level Ring (DLR) network topology.	
Prog	You can perform these tasks: • Update controller firmware. • Disable outputs. • Upload/download projects. • Create, modify, and delete tasks, programs, or routines. • Change the port configuration of the controller, advanced port configuration, nor network configuration settings. You cannot perform these tasks: • Use the controller to execute (scan) tasks.	
Rem	You can perform these tasks: • Upload/download projects. • Change the port configuration of the controller, advanced port configuration, nor network configuration settings. • Change between Remote Program, Remote Test, and Remote Run modes through the application.	
	Remote Run	• The controller executes (scans) tasks. • Enable outputs. • Edit online.
	Remote Program	• Update controller firmware. • Disable outputs. • Create, modify, and delete tasks, programs, or routines. • Download projects. • Edit online. • The controller does not execute (scan) tasks.
	Remote Test	• Execute tasks with outputs disabled. • Edit online.

Configure the Controller

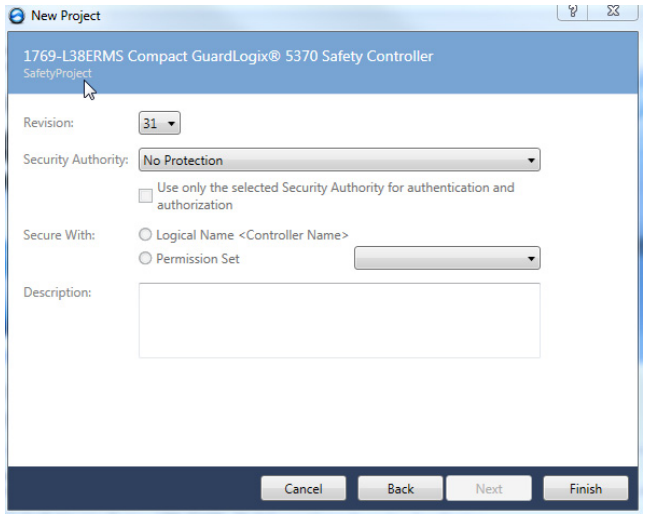
Create a Controller Project

To configure and program your controller, follow these steps to create and manage a project for the controller with the Logix Designer application.

1. To create a project, click the New button on the main toolbar.
2. To expand the list of controller options, double-click Compact GuardLogix® 5370 controller.
3. Choose a Compact GuardLogix 5370 controller:
   - 1769-L30ERMS
   - 1769-L33ERMS
   - 1769-L36ERMS
   - 1769-L37ERMS
   - 1769-L38ERMS



4. In the Name field, type the name of the project.
5. Click Browse to specify the folder for storing the safety controller project.
6. Click Next.
7. From the Revision pull-down menu, choose the major revision of firmware for the controller.

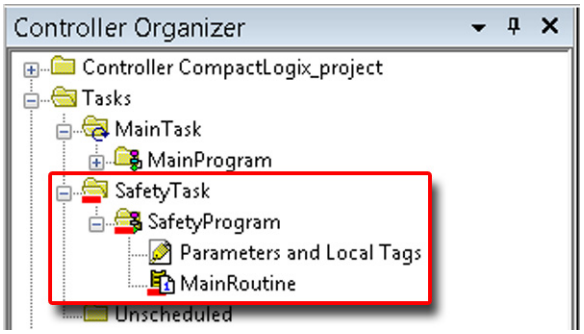


8. From the Security Authority pull-down menu, choose a security authority option.

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

9. To use only the selected security authority for authentication and authorization, select the checkbox under the chosen option.
10. In the Description field, enter a description of the project.
11. Click Finish.

    The Logix Designer application creates a safety task and a safety program. A main ladder logic safety routine that is called MainRoutine is also created within the safety program.

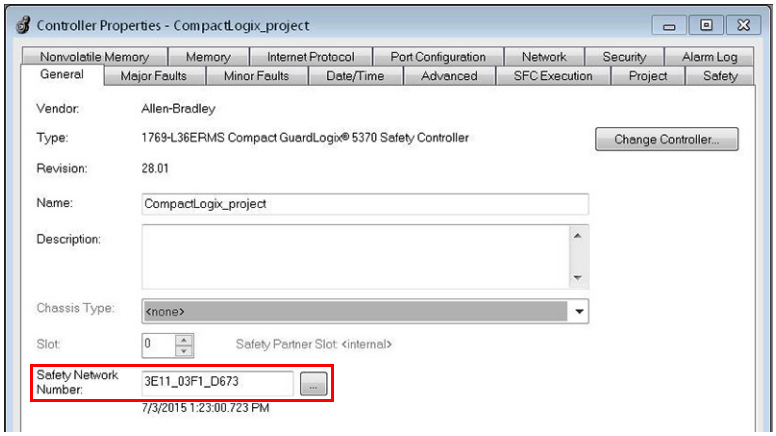


A red bar under the icon distinguishes safety programs and routines from standard project components in the Controller Organizer.

When a new safety project is created, the Logix Designer application also automatically creates a time-based safety network number (SNN).

This SNN defines the EtherNet/IP™ on which the controller resides as a safety subnet. It can be viewed and modified via the General tab on the Controller Properties dialog box.

For most applications, this automatic, time-based SNN is sufficient. However, there are cases when you must enter a specific SNN.



For more information on the safety task, safety programs, and safety routines, see Develop Safety Applications on page 113.

For more information on SNN management, see Communicate Over Networks on page 45.

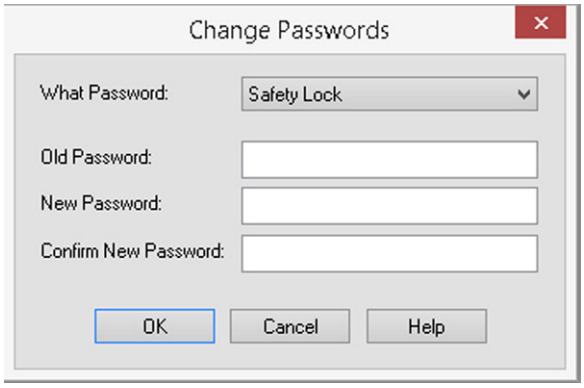
Set Passwords for Safety-lock and -unlock

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

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

Follow these steps to set passwords.

1. 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.

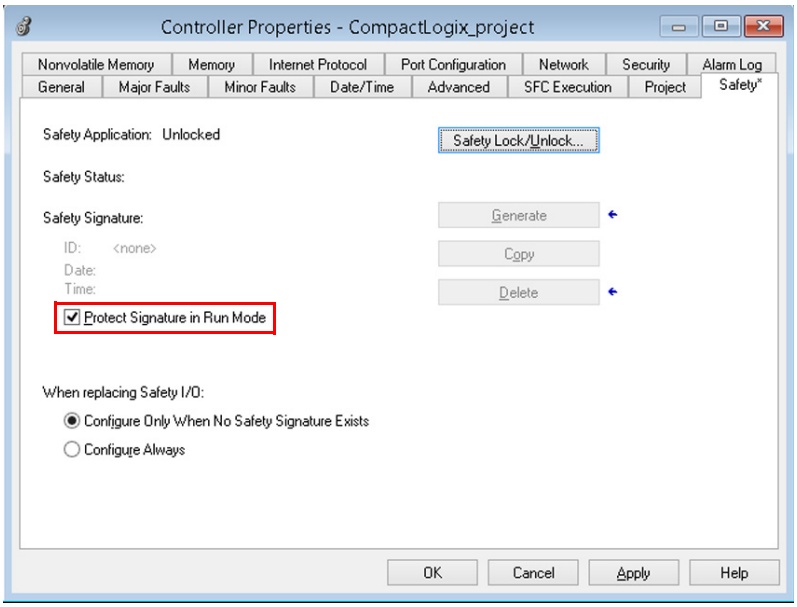
   Passwords can be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols can be used: ‘ ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? /.

Protect the Safety Task Signature in Run Mode

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

Follow these steps to protect the safety task signature.

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



4. Click OK.

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 the Compatible Module option, you can typically replace a device with another device that has the following characteristics: • Same catalog number • Same or higher Major Revision • Minor Revision as follows: – If the Major Revision is the same, the Minor Revision must be the same or higher. – If the Major Revision is higher, the Minor Revision can be any number.
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. Exact Match is required if you are using Firmware Manager.

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

IMPORTANT If electronic keying parameters are changed online, connections to the device and any devices that are connected through the device are interrupted. Connections from other controllers can also be broken.

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

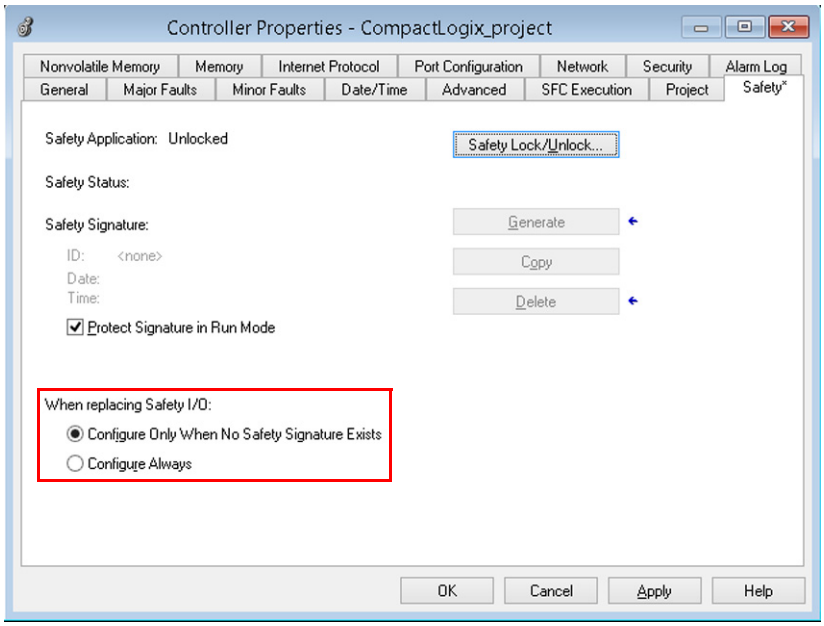
For more detailed information on electronic keying, see Electronic Keying in Logix 5000 Control Systems Application Technique, publication LOGIX-AT001.

I/O Device Replacement Options

The Safety tab of the Controller Properties dialog box lets you define how the controller handles the replacement of an I/O device in the system. This option determines whether the controller sets the safety network number (SNN) of an I/O device that it is connected to and has configuration data for when a safety task signature[1] exists.

Follow these steps to configure how the controller handles the replacement of an I/O device in the system.

1. Open the Controller Properties dialog box.
2. Click the Safety tab.
3. Select the configure option for the controller to use when replacing safety I/O.



4. Click OK.

ATTENTION: Enable the Configure Always feature only if the entire routable CIP Safety™ control system is not being relied on to maintain SIL 3 during the replacement and functional testing of a device.
For more information, see Chapter 4, Communicate Over Networks on page 45.

(1) The safety task signature is a number that is used to uniquely identify each project's logic, data, and configuration, this identification protects the system's safety integrity level (SIL). See Safety Task Signature on page 12 and Generate a Safety Task Signature on page 131 for more information.

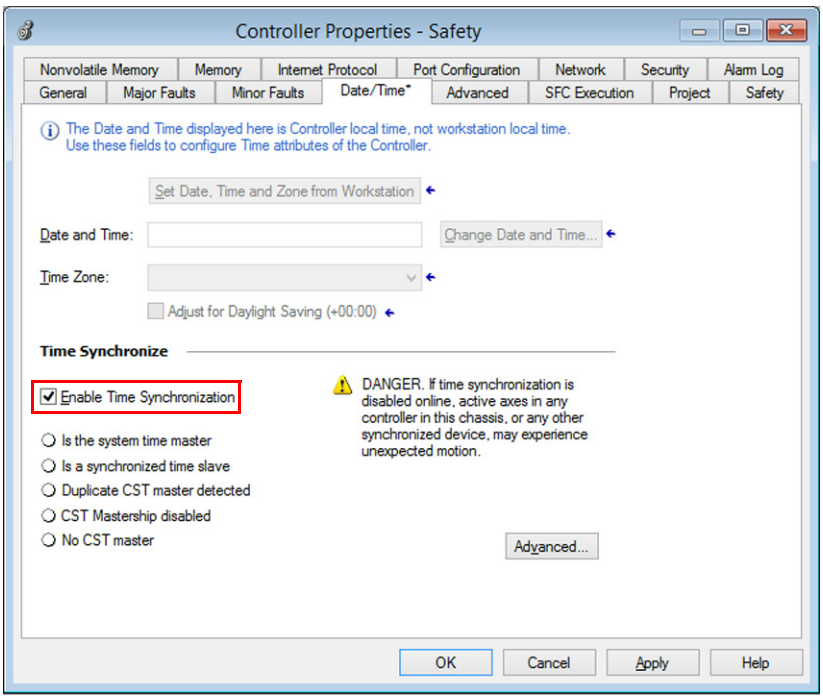
Enable Time Synchronization

In a Compact GuardLogix 5370 controller system, the controller must be designated as the coordinated system time (CST) leader. Time synchronization provides a standard mechanism to synchronize clocks across a network of distributed devices.

IMPORTANT Time synchronization is required for motion applications.

Follow these steps to configure the controller to become the CST leader.

1. Open the Controller Properties dialog box.
2. Click the Date/Time tab.
3. Check Enable Time Synchronization.



4. Click OK.

Configure a Peer Safety Controller

You can add a peer safety controller to the I/O configuration folder of your safety project to allow standard or safety tags to be consumed. To share safety data between peer controllers, you produce and consume controller-scoped safety tags.

For information about how to configure the peer safety controllers, and produced and consumed safety tags, see Produced/Consumed Safety Tags on page 119.

Communicate Over Networks

All Compact GuardLogix® 5370 controllers support these tasks over an EtherNet/IP™ network:

- Control distributed I/O for both safety and standard connections
- Send/receive messages to/from other devices on the same network or another network
- Produce/consume (interlock) data between controllers
- Socket interface

Compact GuardLogix 5370 controllers support these tasks over a DeviceNet™ network:

- Control distributed I/O only for standard connections
- Send messages to devices on the same network; the controller cannot receive messages from other devices on the network.

All Compact GuardLogix 5370 controllers also support temporary connections from your computer via a USB connection.

The Safety Network

The CIP Safety™ protocol is an end-node to end-node safety protocol that allows routing of CIP Safety messages to and from CIP Safety devices through bridges, switches, and routers.

To maintain high integrity when routing through standard bridges, switches, or routers, each end node within a routable CIP Safety Control System must have a unique reference. This unique reference is a combination of a safety network number (SNN) and the node address of the network device.

Manage the Safety Network Number (SNN)

The SNN assigned to safety devices on a network segment must be unique. You must be sure that a unique SNN is assigned to each CIP Safety network that contains safety devices.

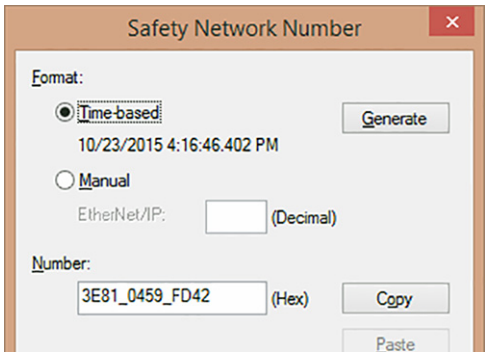
The SNN assigned to safety devices on a network segment must be unique. You must be sure that a unique SNN is assigned to each CIP Safety network that contains safety devices.

Multiple safety network numbers can be assigned to a CIP Safety subnet or a ControlBus™ chassis that contains multiple safety devices.

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

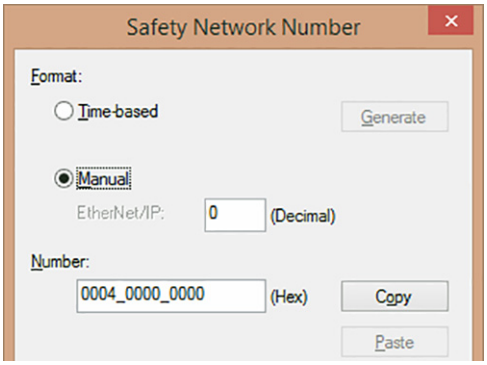
Time-based SNN

If the time-based format is selected, the SNN value that is generated represents the date and time at which the number was generated, according to the computer on which the configuration software is run.



Manual SNN

If the manual format is selected, the SNN represents entered values from 1...9999 decimal.



Assign the Safety Network Number (SNN)

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

Automatic Assignment

When a new controller or module is created, a time-based SNN is automatically assigned via the configuration software. Subsequent new safety-module additions to the same CIP Safety network are assigned the same SNN defined within the lowest address on that CIP Safety network.

Manual Assignment

The manual option is intended for routable CIP Safety systems where the number of network subnets and network interconnections is small, and where the SNN is managed and assigned in a logical way and based on the specific application.

See Change the Safety Network Number (SNN) on page 48.

IMPORTANT	If you assign an SNN manually, make sure that system expansion does not result in duplication of SNN and node address combinations. A warning appears if your project contains duplicate SNN and node address combinations. You can still verify the project, but Rockwell Automation recommends that you resolve the duplicate combinations.

Automatic Versus Manual

In most cases, the automatic assignment of an SNN is sufficient. However, manual manipulation of the SNN is required if the following is true:

- Safety consumed tags are used.
- The project consumes safety input data from a module with configuration that another device owns.
- A safety project is copied to another hardware installation within the same routable CIP Safety system.

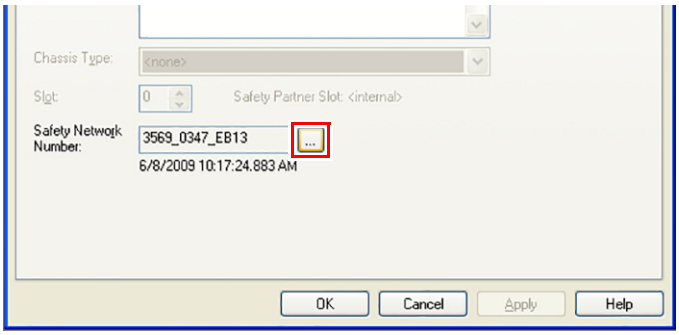
Change the Safety Network Number (SNN)

Before you change the SNN, you must do the following:

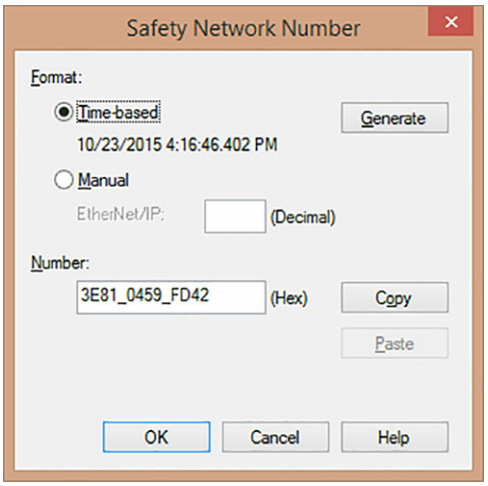
- If the project is safety-locked, then you must unlock it.
  See Safety-lock the Controller on page 129.
- If a safety task signature exists, then you must delete it.
  See Delete the Safety Task Signature on page 132.

Change the SNN of the Controller

1. In the Controller Organizer, right-click the controller and choose Properties.
2. On the General tab of the Controller Properties dialog box, click ... to the right of the safety network number to open the Safety Network Number dialog box.



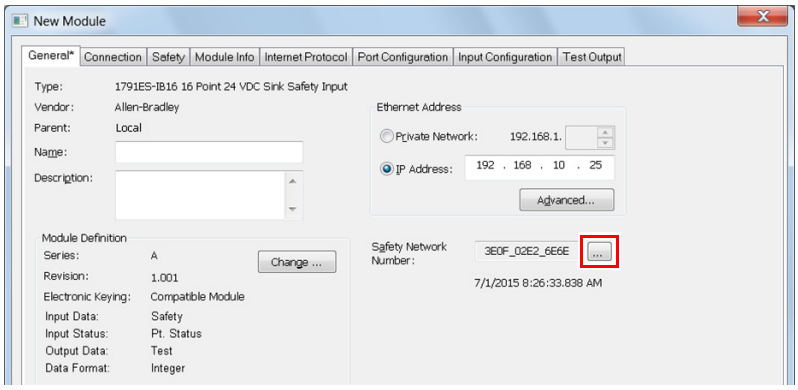
3. Click Time-based and then Generate.



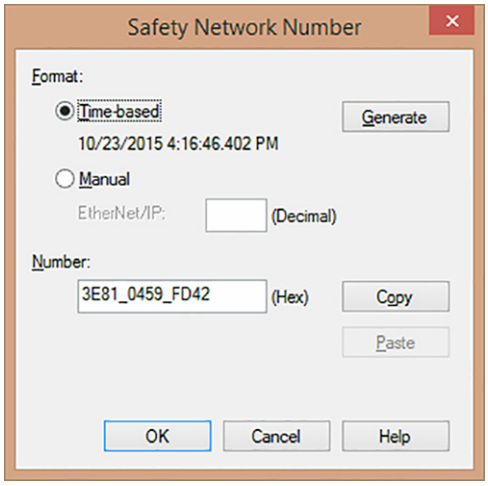
4. Click OK.

Change the SNN of Safety I/O Modules on the CIP Safety Networks

1. In the Controller Organizer, double-click the first safety I/O module underneath the Ethernet network to view the General tab.
2. To open the Safety Network Number dialog box, click ... to the right of the safety network number.



3. To generate a new SNN for that EtherNet/IP network, choose Time-based and click Generate.

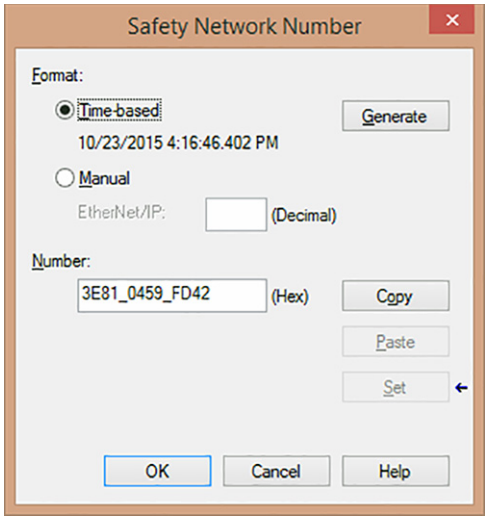


4. Click OK.
5. Click Copy to copy the new SNN to the Windows® Clipboard.
6. Open the General Tab of the Module Properties dialog box of the next safety I/O module under that EtherNet/IP module.
7. To open the Safety Network Number dialog box, click ... to the right of the safety network number.
8. Choose Time-based and click Paste to paste that EtherNet/IP network's SNN into that device.
9. Click OK.
10. Repeat steps 6...9 for the remaining safety I/O modules under that EtherNet/IP communication module.
11. Repeat steps 2...9 for all remaining network communication modules under the I/O Configuration tree.

Copy and Paste an SNN

If you need to copy and paste the SNN from another controller into the module because another controller owns the module's configuration, complete the following steps.

1. In the software configuration tool of the controller that owns the configuration, open the Safety Network Number dialog box for the module.
2. Click Copy.



3. Click the General tab on the Module Properties dialog box of the I/O module in the I/O Configuration tree of the consuming controller project.

   This consuming controller is not the configuration owner.
4. To open the Safety Network Number dialog box, click ... to the right of the safety network number.
5. Click Paste.
6. Click OK.

EtherNet/IP Network Communication

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 Compact GuardLogix 5370 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 56.

Available Software

You use the software that is listed in the following table with a Compact GuardLogix 5370 controller on an EtherNet/IP network.

Software	Required Version	Functions	Required
Studio 5000® environment	28.00.00 or later	• Configure the CompactLogix™ project • Define EtherNet/IP communication • Change IP address for devices on network, including the Compact GuardLogix 5370 controller	Yes
RSLinx® Classic	3.80 or later	• Assign or change IP addresses to devices on an EtherNet/IP network • Configure communication devices • Provide diagnostics • Establish communication between devices	
BOOTP/DHCP utility	Most current version is installed when RSLinx Classic software is installed	Assign IP addresses to devices on an EtherNet/IP network.	No

EtherNet/IP Functionality

The Compact GuardLogix 5370 controllers offer this EtherNet/IP network functionality:

- Dual built-in EtherNet/IP network ports
- Support for the following EtherNet/IP network topologies:
  - Device Level Ring Network Topology
  - Linear Network Topology
  - Star Network Topology
- Support for CIP Safety protocol
- Support for Integrated Motion over an EtherNet/IP network
- Socket interface to communicate with Ethernet devices that do not support the EtherNet/IP application protocol
- Duplicate IP address detection
- Unicast and multicast communication
- Support messaging, produced/consumed tags, HMI, and distributed I/O
- Interface via RJ45, twisted-pair cables
- Support half/full-duplex 10 Mbps or 100 Mbps operation
- Support standard switches
- No network scheduling required
- No routing tables required

Nodes on EtherNet/IP Network

When configuring your Compact GuardLogix 5370 controller system, you must account for the number of Ethernet nodes that you include in the I/O configuration section of your project. Compact GuardLogix 5370 controllers have limits on the number of nodes that they support in the I/O configuration section.

Compact GuardLogix 5370 Controller Ethernet Node Guidelines

Cat. No.	Ethernet Nodes Supported
1769-L30ERMS	16
1769-L33ERMS 1769-L33RMSK 1769-L33ERMOS	32
1769-L36ERMS 1769-L36ERMOS	48
1769-L37ERMS(1) 1769-L37ERMOS(1)	64
1769-L38ERMS(1) 1769-L38ERMOS(1)	80

(1) Available at firmware revision 31.

IMPORTANT To design a control system effectively, Compact GuardLogix 5370 controllers offer the option of using Ethernet node count in accordance with the connection limits on an EtherNet/IP network.

For more information on how to implement an EtherNet/IP network in your Compact GuardLogix 5370 controller system, see these resources:

- EtherNet/IP Capacity Tool Wizard within the Integrated Architecture® Builder tool, https://www.rockwellautomation.com/en-us/support/product/product-selection-configuration/integrated-architecture-builder.html.
  The EtherNet/IP Capacity Tool Wizard helps you in the initial layout of your EtherNet/IP network.
- Ethernet Design Considerations Reference Manual, publication ENET-RM002.

Devices Excluded from the Node Count

When considering the Ethernet node limitation of a Compact GuardLogix 5370 controller, you do not count Ethernet devices that exist on the EtherNet/IP network but are not added to the I/O configuration section of the project.

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

- Computer
- HMIs that are not added to the I/O configuration section, for example, PanelView™ Plus terminals
- MSG instructions
- Devices with which the Compact GuardLogix 5370 controllers use a socket interface to communicate.

  For example, the following devices require communication via a socket interface:

  - Modbus TCP/IP device
  - Barcode scanners

EtherNet/IP Network Topologies

Compact GuardLogix 5370 controllers support these EtherNet/IP network types:

- Device Level Ring (DLR) Network Topology
- Linear Network Topology
- Star Network Topology

Each of these EtherNet/IP network topologies supports applications that use Integrated Motion over an EtherNet/IP network.

Device Level Ring (DLR) 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 is composed of 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.

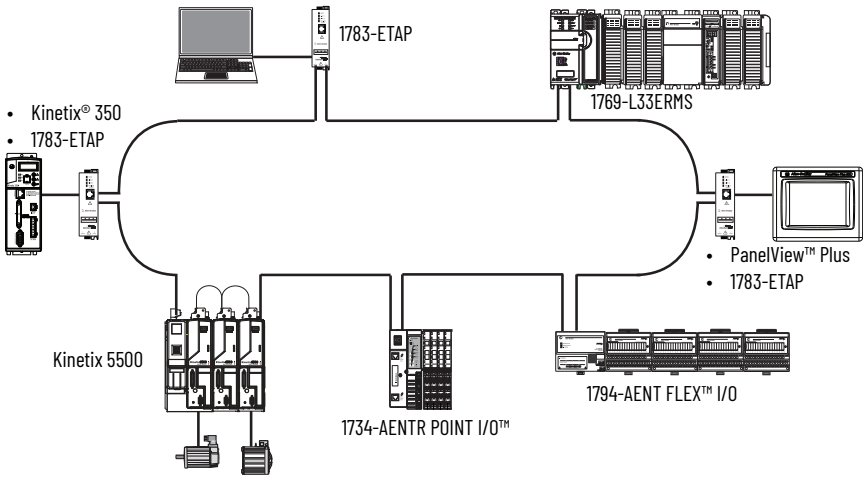
Compact GuardLogix 5370 controllers connect directly to a DLR network topology, that is, without requiring a 1783-ETAP tap to connect to the network. The controllers can function in any of the roles on a DLR network topology, that is, active supervisor node, back-up supervisor node or ring node.

IMPORTANT The topology graphics that are shown in this section are examples of applications that use only DLR network topologies.

We recommend that you exercise caution if you consider designing an application that includes the connection of a DLR topology with a linear or star network topology.

For more information on DLR network topology, see the EtherNet/IP Embedded Switch Technology Application Guide, publication ENET-AP005.

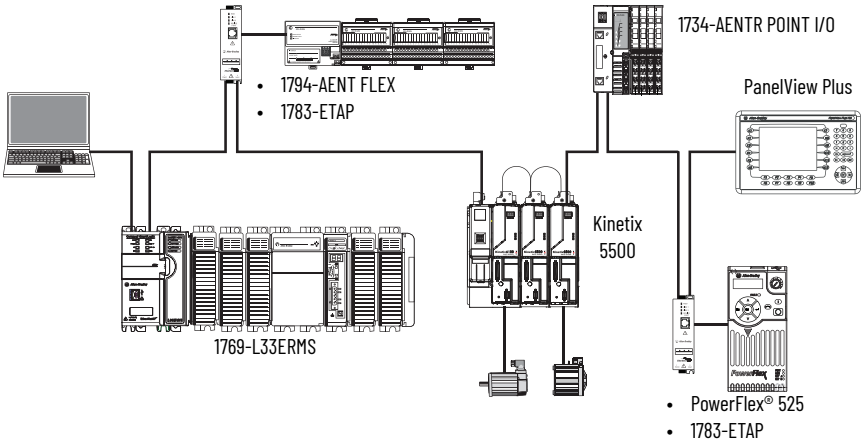
Example 1769-L33ERMS Control System With a DLR Network Topology



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.

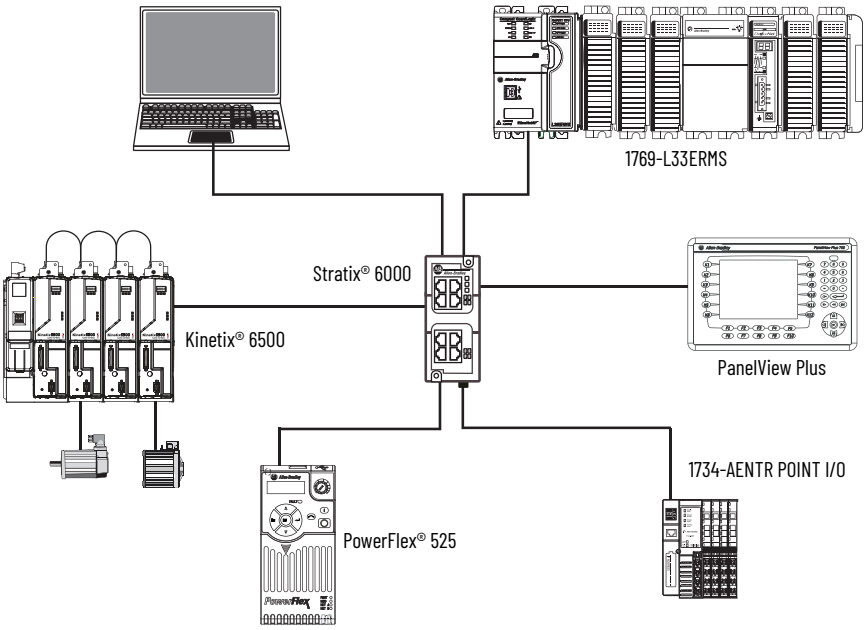
Example 1769-L33ERMS Control System With a Linear Network Topology



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.

Example 1769-L33ERMS Control System With a Star Network Topology



EtherNet/IP Network Connections

Compact GuardLogix 5370 controllers use connections to manage communication on the EtherNet/IP network. A connection is a point-to-point communication mechanism that is used to transfer data between a transmitter and a receiver. Connections can be logical or physical.

You indirectly determine the number of connections the controller uses by configuring the controller to communicate with other devices in the system. Connections are allocations of resources that provide more consistent communication between devices than unconnected messages.

All EtherNet/IP connections are unscheduled. An unscheduled connection is a message transfer between controllers that the requested packet interval (RPI) or the program, such as an MSG instruction, triggers. Unscheduled messaging lets you send and receive data when needed.

Compact GuardLogix 5370 Controller EtherNet/IP Network Port Specifications

Cat. No.	Connections			CIP Unconnected Messages (Backplane + Ethernet)	Packet Rate Capacity (packets/second)(1)		SNMP Support (password required)	Media Support	Produced/Consumed Tags	
	Controller	TCP	CIP		I/O	HMI/MSG			Number of Multicast Tags, Max(2)	Unicast Available
1769-L30ERMS	256	120	256	256	6000 @ 500 bytes/packet	400 messages/ second @ 20% comm. timeslice	Yes	Twisted-pair	• 32 multicast produced tags • 128 unicast produced tags	Yes
1769-L33ERMS										
1769-L33ERMSK										
1769-L33ERMOS										
1769-L36ERMS										
1769-L36ERMOS										
1769-L37ERMS(3)										
1769-L37ERMOS(3)										
1769-L38ERMS(3)										
1769-L38ERMOS(3)										

(1) Total packet rate capacity = I/O Produced Tag, max + HMI/MSG, max Packet rates vary depending on packet size. For more detailed specifications, see the capacity section of the EDS file for the catalog number.
(2) These are the maximum numbers of CIP I/O connections.
(3) Available at firmware revision 31.

Socket Interface

The Compact GuardLogix 5370 controller can use socket interfaces to communicate with Ethernet devices that do not support the EtherNet/IP application protocol.

Examples of devices that do not support the EtherNet/IP application protocol but can be used in a Compact GuardLogix 5370 controller application include the following:

- Modbus TCP/IP device
- Barcode scanners
- RFID readers

The socket interface is implemented via the Socket Object. Compact GuardLogix 5370 controllers communicate with the Socket Object via MSG instructions. All Compact GuardLogix 5370 controllers must use unconnected MSG instructions with socket interfaces.

For more information on socket services, see the following:

- CompactLogix 5370 Controllers User Manual, publication 1769-UM021
- The EtherNet/IP Socket Interface Application Technique, publication ENET-AT002

Quality of Service (QoS) and I/O Module Connections

Compact GuardLogix 5370 controllers support Quality of Service (QoS) technology. QoS lets the controller prioritize EtherNet/IP network traffic. By default, the Compact GuardLogix 5370 controllers are QoS-enabled. QoS can be disabled by configuring a message instruction in the Logix Designer application.

Some EtherNet/IP devices do not support QoS technology unless the device firmware is upgraded to a required minimum firmware revision level. For example, the ControlLogix 1756-ENBT communication module must use firmware revision 4.005 or later to support QoS technology.

To make sure communication between Compact GuardLogix 5370 controllers and I/O modules are maintained, verify that the EtherNet/IP devices use the minimum firmware revision level of the product that is required to support QoS technology.

For more information on the following, see Rockwell Automation Knowledgebase Tech Note 66325:

- Minimum firmware revision levels of EtherNet/IP devices to support QoS technology
- Enable/disable QoS

DeviceNet Network Communication

The Compact GuardLogix 5370 controllers communicate with other devices over the DeviceNet network via a Compact I/O™ 1769-SDN DeviceNet scanner. The DeviceNet network uses the Common Industrial Protocol (CIP) to provide the control, configuration, and data collection capabilities for industrial devices.

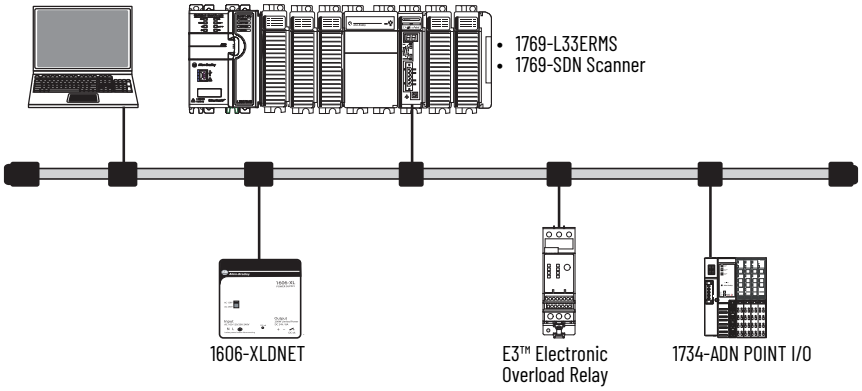
IMPORTANT Compact GuardLogix controllers support standard connections to the DeviceNet network. CIP Safety over DeviceNet networks is not supported.

Available Software

The software applications that are listed in this table are required when using a Compact GuardLogix 5370 controller on a DeviceNet network.

Software	Required Version	Functions
Studio 5000 environment	28.00.00 or later	Configure the CompactLogix project.
RSLinx Classic	3.80 or later	• Configure communication devices • Provide diagnostics • Establish communication between devices
RSNetWorx™ for DeviceNet	25.00.00 or later if used with the Studio 5000 environment versions in this table	• Configure DeviceNet devices • Define the scanlist for the DeviceNet network

Example 1769-L33ERMS Control System With a DeviceNet Network



Compact I/O 1769-SDN DeviceNet Scanner

You can connect a Compact GuardLogix 5370 controller to a DeviceNet network via a Compact I/O 1769-SDN DeviceNet scanner for **standard** communication.

IMPORTANT	CIP Safety is not supported on a DeviceNet network with the 1769-SDN scanner. DeviceNet safety I/O modules cannot be connected to a Compact GuardLogix 5370 controller system via the 1769-SDN scanner.

Considerations

Before installing the scanner, consider the following:

- You can connect the scanner to an adjacent controller, power supply, or I/O module.
- You must account for these two requirements jointly:
  - Power supply distance rating; see page 58
  - Current capacity in Compact GuardLogix controller systems; see page 60
- The scanner, as a leader, can own up to 63 follower I/O nodes.
- Another DeviceNet leader can own a scanner that is simultaneously a leader and also a follower.

Scanner Features

The scanner has the following functionality:

- Supports messaging to devices, not controller to controller
- Supports control-level network to device-level network for programming, configuration, control, or data collection
- Shares a common application layer with EtherNet/IP networks
- Offers diagnostics for improved data collection and fault detection

Power Supply Distance Rating

Compact GuardLogix 5370 controller systems allow you to install 1769-SDN scanners as local expansion modules. The 1769-SDN scanner has a power supply distance rating to consider before you install it.

Power supply distance rating is the number of slots a 1769-SDN scanner can be installed away from the power supply. The 1769-SDN scanner has a power supply distance rating of four. Therefore, your Compact GuardLogix 5370 controller system can include up to three modules between the 1769-SDN scanner and the power supply.

Compact GuardLogix 5370 controller systems do not have embedded I/O modules. You begin counting local expansion slots with the first Compact I/O module installed next to the power supply when determining where to install a 1769-SDN scanner and meet its power supply distance rating.

In Compact GuardLogix 5370 controller systems, you can install 1769-SDN scanners to the left or right side of the power supply. You can also use local and extra banks in Compact GuardLogix 5370 controller systems, with each allowing the inclusion of a 1769-SDN scanner.

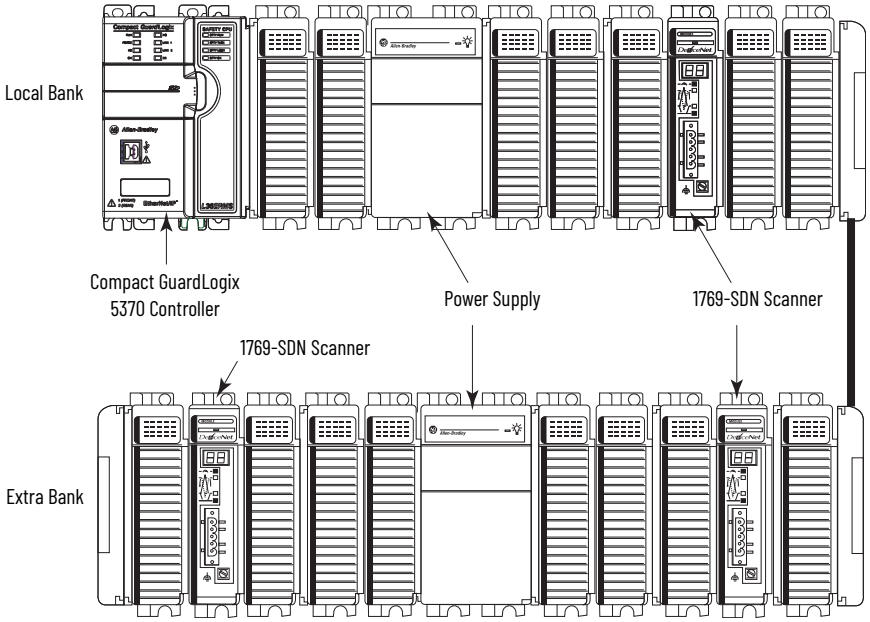
In the local bank, the controller must be the leftmost device in the system and you can only install up to three modules between the controller and the power supply. Therefore, any 1769-SDN scanners that are installed to the left of the power supply in the local bank, are in a module slot that meets the power supply distance rating requirements of the module.

Compact GuardLogix 5370 controller systems also support the use of extra banks for the local expansion modules of the system. Each additional bank requires a 1769 Compact I/O power supply. The bank can be designed with local expansion modules on either side of the power supply.

In this case, you must install the 1769-SDN scanner with no more three Compact I/O modules between the scanner and the power, regardless of whether the modules are installed to the left or right of the power supply.

The following figure shows 1769-SDN scanners that are installed in a 1769-L36ERMS control system that meet the power supply distance rating of the module.

Power Supply Distance Rating Example for a 1769-SDN Scanner



Current Capacity in Compact GuardLogix 5370 Controller Systems

In a local or extra bank, the modules that are installed on either side of the power supply cannot draw more current than the power supply can supply. This requirement partially dictates module placement on the bank.

For example, if a bank uses a 1769-PA2 Compact I/O power supply, each side of the bank has a current capacity of 1 A at 5V DC and 0.4 A at 24V DC. Due to the 1769-SDN scanner's current draw of 440 mA at 5V DC and 0 mA at 24V DC, you can only install up to two scanners on each side of the power supply in the bank in this case.

For more information on 1769 Compact I/O power supply maximum current capacity, and calculations you can use to design the modules that are used in local or extra banks, see Calculate System Power Consumption on page 67.

Add and Configure Standard I/O Modules

Select I/O Modules

Compact GuardLogix® 5370 controller systems offer these standard I/O module options:

- Local Expansion Modules
- Standard Distributed I/O Modules Over an EtherNet/IP Network
- Standard Distributed I/O Modules Over a DeviceNet Network

Local Expansion Modules

Compact GuardLogix 5370 controller systems support the use of standard Compact I/O™ modules as local expansion modules along a CompactBus backplane.

Consider the following when using local expansion modules:

- The controllers support this many local Compact I/O modules across up to three I/O banks, that is, the local bank and two more banks.

Cat. No.	Local Expansion Modules Supported, Max
1769-L30ERMS	8
1769-L33ERMS 1769-L33ERMSK	16
1769-L36ERMS 1769-L37ERMS(1) 1769-L38ERMS(1)	30
1769-L33ERMOS 1769-L36ERMOS 1769-L37ERMOS(1) 1769-LE8ERMOS(1)	—

(1) Available at firmware revision 31.

- When possible, use specialty Compact I/O modules to meet unique application requirements.
- Consider using a 1492 wiring system for each I/O module as an alternative to the terminal block that comes with the module.
- Use 1492 PanelConnect™ modules and cables if you are connecting input modules to sensors.

Install Local Expansion Modules

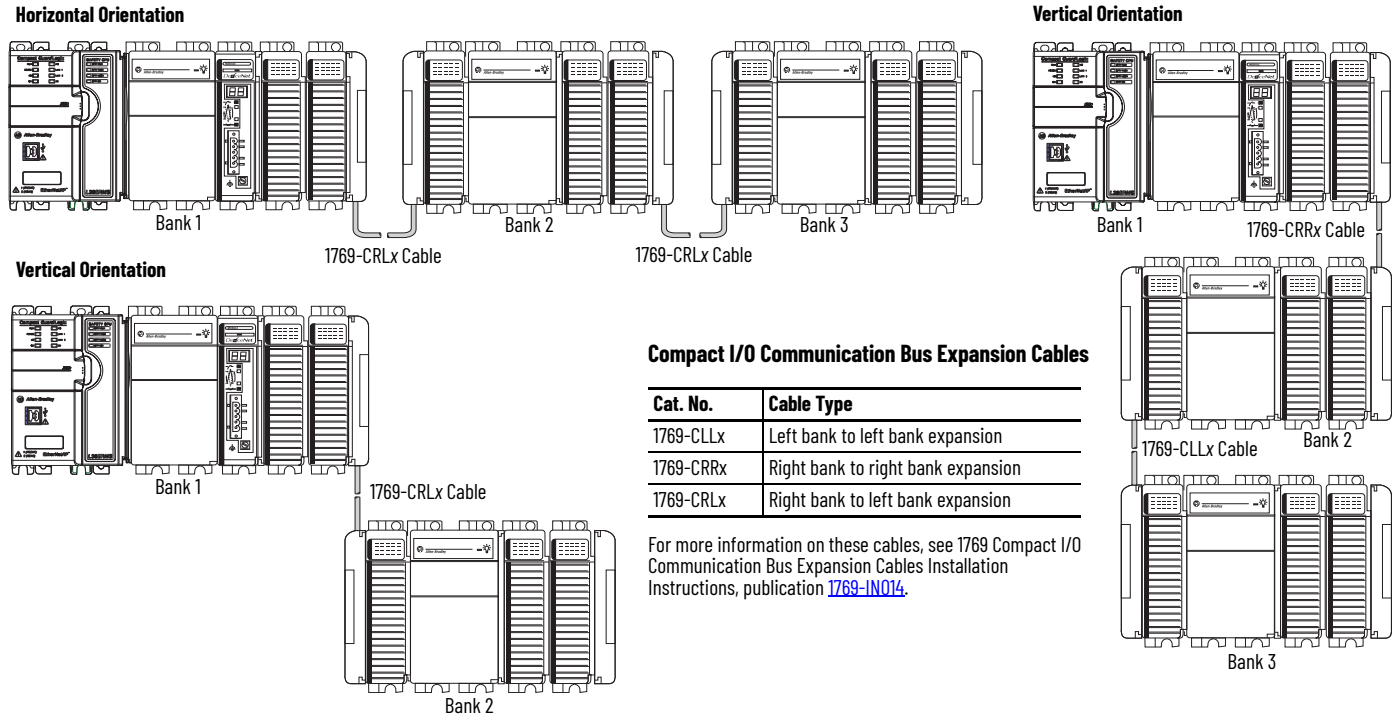
Complete these steps to install local expansion modules in your Compact GuardLogix 5370 controller system.

1. Attach the 1769 Compact communication or I/O modules as described in these publications:
   - Compact I/O Modules Installation Instructions, publication 1769-IN088
   - Compact I/O DeviceNet Scanner Module Installation Instructions, publication 1769-IN060
2. If your system uses only a local bank, complete these steps.
   a. Use the tongue-and-groove slots to attach a 1769-ECR Compact I/O end cap terminator to the last module in the system.
   b. Move the lever of the end cap bus terminator fully to the left until it clicks to lock the end cap bus terminator.

3. If your system uses more banks, follow these steps.
   a. Install a 1769-CR*x* Compact I/O communication bus expansion cable at the right end of the local bank.
   b. Connect the 1769-CR*x* cable to the additional bank as necessary.

      The side that you connect to on the extra bank, determines the expansion cable that is installed at the end of the local bank. The following figure shows examples of how to connect a local bank to extra banks.

Example of Banks and System Configurations



Compact I/O Communication Bus Expansion Cables

Cat. No.	Cable Type
1769-CLLx	Left bank to left bank expansion
1769-CRRx	Right bank to right bank expansion
1769-CRLx	Right bank to left bank expansion

For more information on these cables, see 1769 Compact I/O Communication Bus Expansion Cables Installation Instructions, publication 1769-IN014.

   c. Complete the installation of the remaining banks in your system.

IMPORTANT Make sure that you install an end cap at the end of the last bank in your system.

Wire Local Expansion Modules

Wire each Compact I/O module that is used as a local expansion module according to the technical documentation for that module.

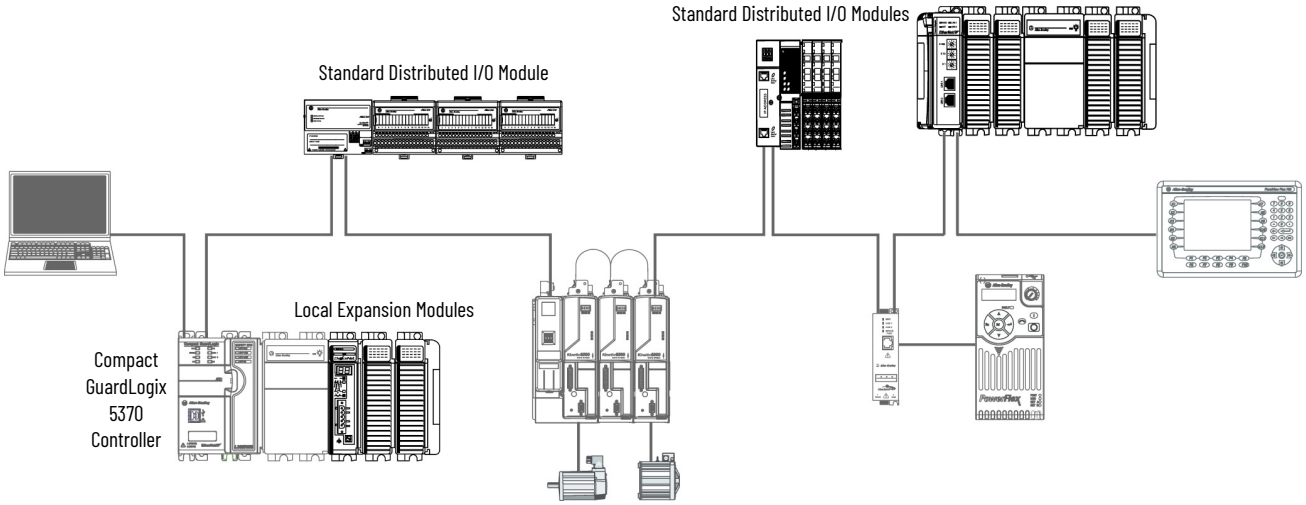
Standard Distributed I/O Modules Over an EtherNet/IP Network

You can include standard distributed I/O modules over an EtherNet/IP™ network in your Compact GuardLogix 5370 controller system. Consider the following when you use distributed I/O modules over an EtherNet/IP network:

- Each remote EtherNet/IP adapter in the system must be counted toward the maximum number of EtherNet/IP nodes for the controller.

  For more information on the maximum number of EtherNet/IP nodes, see Nodes on EtherNet/IP Network on page 52.
- The configurable RPI settings vary depending on which distributed I/O modules are used in the system.

Example 1769-L33ERMS Controller System With Modules Over an EtherNet/IP Network



Standard Distributed I/O Modules Over a DeviceNet Network

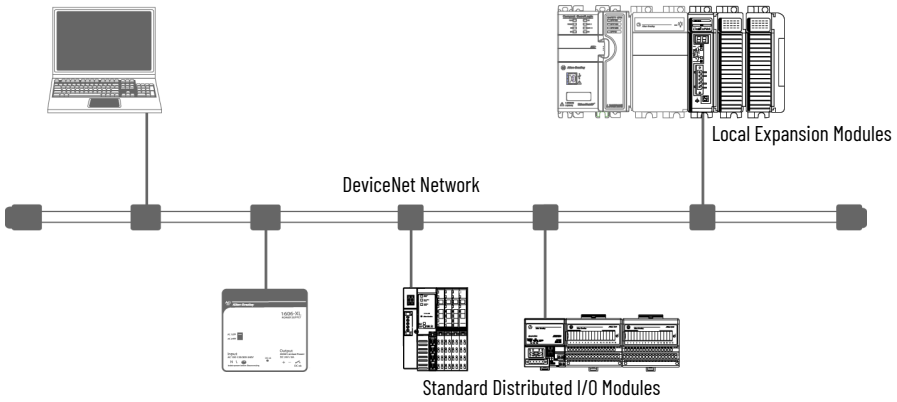
You can include standard distributed I/O modules over a DeviceNet™ network in your Compact GuardLogix 5370 controller system.

IMPORTANT CIP Safety™ is not supported on DeviceNet with the 1769-SDN module. DeviceNet safety I/O modules cannot be connected to a Compact GuardLogix system via the 1769-SDN module.

Consider the following when you use distributed I/O modules over a DeviceNet network:

- For information on how the Compact GuardLogix system communicates via the Compact I/O 1769-SDN DeviceNet scanner, see DeviceNet Network Communication on page 57.
- To add distributed I/O modules to your Compact GuardLogix 5370 controller system, see Configure Standard Distributed I/O Modules on a DeviceNet Network on page 78.

Example 1769-L33ERMS Controller System With Modules Over a DeviceNet Network



Validate Standard I/O Layout

After you have selected your I/O modules, you must validate the system that you want to design. Consider these points when validating I/O layout placement:

- Estimate Requested Packet Interval
- Module Fault Related to RPI Estimates
- Calculate System Power Consumption
- Power Supply Distance Rating
- Physical Placement of I/O Modules

Estimate Requested Packet Interval

The requested packet interval (RPI) defines the frequency at which the controller sends data to and receives data from I/O modules. You set an RPI rate for each I/O module in your system.

The Compact GuardLogix 5370 controllers attempt to scan an I/O module at the configured RPI rate. For individual I/O modules, a Module RPI Overlap minor fault occurs if there is at least one I/O module that cannot be serviced within its RPI time.

The configuration parameters for a system determine the impact on actual RPI rates. These configuration factors can affect the effective scan frequency for any individual module:

- Rates at which RPI rates are set for other Compact I/O modules
- Number of other Compact I/O modules in the system
- Types of other Compact I/O modules in the system
- Application user task priorities

Requested Packet Interval Guidelines

Type of Module	Guidelines[1]
All digital	The following guidelines apply: • 1…2 modules can be scanned in 0.5 ms. • 3…4 modules can be scanned in 1 ms. • 5…30 modules can be scanned in 2 ms.
Mix of digital and analog or all analog	The following guidelines apply: • 1…2 modules can be scanned in 0.5 ms. • 3…4 modules can be scanned in 1 ms. • 5…13 modules can be scanned in 2 ms. • 14…30 modules can be scanned in 3 ms.
Specialty	The following conditions apply: • For every 1769-SDN module in the system, increase the RPI of every other module by 2 ms. • For every 1769-HSC module in the system, increase the RPI of every other module by 1 ms. • For every 1769-ASCII module in the system, increase the RPI of every other module by 1 ms. • For every 1769-SM2 module in the system, increase the RPI of every other module by 2 ms.

(1) The guidelines in this table do not factor in the following items, which affect Compact GuardLogix 5370 controller CPU loading:
- I/O RPI timing does not affect the task priority. Event and periodic tasks have higher priority than I/O and user tasks.
- IOT (Immediate Output Instruction)
- Messaging
- CompactBus browsing, such as DeviceNet network access through 1769-SDN with Compact GuardLogix 5370 Ethernet or USB connection

Module RPI guidelines can require adjustment (increase of 1 ms or more) if the Compact GuardLogix 5370 controller application includes one or more of the items in this table. Monitor controller minor faults to determine if Module RPI overlaps have occurred.

You can set the RPI rates of individual Compact I/O modules higher than the rates listed in the previous table. The RPI shows how quickly modules can be scanned, not how quickly an application can use the data. The RPI is asynchronous to the program scan. Other factors, such as program execution duration, affect
I/O throughput.

Module Fault Related to RPI Estimates

When the guidelines that are described in the previous table are followed, most Compact GuardLogix 5370 controller systems operate as expected. Some systems that follow the guidelines can experience a Module RPI Overlap minor fault as described in the following table.

Module RPI Overlap Fault

Name	Fault Information	Condition In Which Fault Occurs
Module RPI Overlap	(Type 03) I/O fault (Code 94) Module RPI overlap detected Module Slot = *x*, where *x* is the slot number of the I/O module in the I/O configuration section	This fault is logged when the current RPI update of an I/O module overlaps with its previous RPI update. The Minor Faults tab in the Controller Properties dialog box indicates in which module the RPI overlap fault occurs. If multiple I/O modules experience the fault, the application indicates that the fault occurred on the first such I/O module. Typically, it is an I/O module with a large I/O array size. Example modules that use large I/O array sizes include the 1769-SDN and 1769-HSC modules. In these cases, we recommend that you adjust the RPI of the module to remove the fault. Once the fault is cleared from the first I/O module, the application indicates the next module that experiences the fault. This pattern continues until the fault is cleared from all affected I/O modules. To avoid this fault, set the RPI rate of the I/O modules to higher numerical values. We recommend you use an RPI value that is not a common multiple of other module RPI values, such as 2.5 ms, 5.5 ms, or 7 ms. • We recommend that you do not run Compact GuardLogix 5370 controller systems with Module RPI Overlap faults. • A system that experiences many Module RPI Overlap faults cannot operate optimally because I/O data is not sampled at the expected rate that the RPI settings determine. • When the project is downloaded or the RPI value of an I/O module is adjusted, it is expected to have a minor fault. Faults under these conditions are transitionary. Clear the fault and wait for the fault to reappear before adjusting the RPI value or the task priorities.

Calculate System Power Consumption

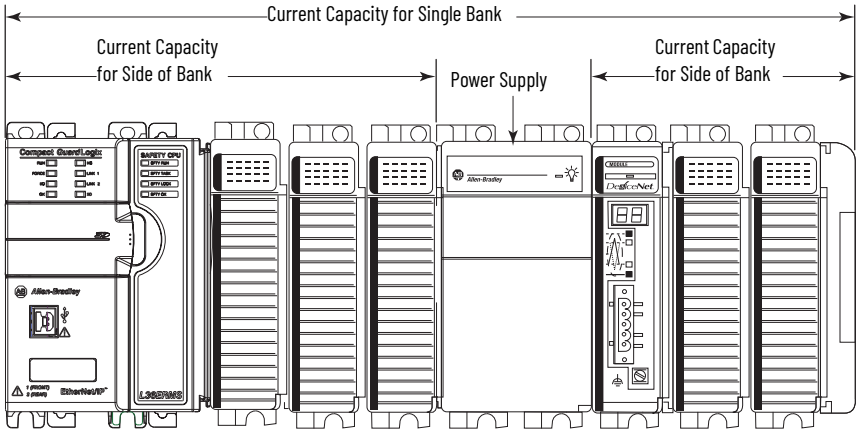
The 1769 Compact I/O power supplies provide power to Compact GuardLogix local and more banks. The provided power is measured in current capacity.

Consider these points when you design your Compact GuardLogix 5370 controller system banks:

- 1769 Compact I/O power supplies have two maximum current capacity requirements that affect how you design and configure one bank.

  The following are the maximum current capacity requirements:

  - Maximum current capacity for one bank
  - Maximum current capacity for each side of the power supply



- The maximum current capacity requirements vary by the power supply that is used in the bank.

Power Supply Cat. No.	Current Capacity, Max for Single Bank	Current Capacity, Max for Each Side of the Bank[1]
1769-PA2	2 A at 5V DC and 0.8 A at 24V DC	1 A at 5V DC and 0.4 A at 24V DC
1769-PB2		
1769-PA4	4 A at 5V DC and 2 A at 24V DC	2 A at 5V DC and 1 A at 24V DC
1769-PB4		

(1) Specification for banks with devices on left and right sides of the power supply.

Calculate Power Consumption in Single Bank

IMPORTANT A single bank requires the Compact GuardLogix 5370 controllers to reside in the leftmost slot. At a minimum, you must calculate the power consumption of the controller on the left side of the power supply.

If more modules are installed on the left side of the power supply, you must also calculate the power consumption for those modules.

If more modules are installed to the right of the power supply, you must calculate the power consumption for that side separately.

Use this table to calculate power consumption in one bank.

Module Power Consumption Calculation for a Local Bank

Side of Power Supply	Device Cat. No.	Number of Modules[1]	Module Current Requirements		Calculated Current = (Number of Modules) x (Module Current Requirements)	
			at 5V DC (in mA)	at 24V DC (in mA)	at 5V DC (in mA)	at 24V DC (in mA)
Left - Required	1769-L30ERMS 1769-L33ERMS 1769-L33ERMSK 1769-L36ERMS 1769-L37ERMS 1769-L38ERMS	1	500	225	500	225
Left - Optional	I/O Module-specific	Up to 3	Module-specific	Module-specific		
	Total Current Required[2]:					
Right	I/O Module-specific **IMPORTANT**: Insert a separate row in this calculation for each I/O module.	Up to 8	Module-specific	Module-specific		
	Total Current Required[2]:					
Total Current Required for Single Bank if Modules Are Installed on Both Sides of the Power Supply[3]:						

(1) In the local bank, you can only install up to three modules to the left of the power supply because the Compact GuardLogix 5370 controllers have a power supply distance rating of four and must be within four slots of the Compact I/O power supply. You can install up to eight modules on the right side of the power supply in the local bank, and both sides of the power supply in more banks, if power supply distance ratings for the modules validate the system design.
(2) This number must not exceed the power supply current capacity for this side of the bank.
(3) This number must not exceed the power supply current capacity for the bank.

Calculate Power Consumption in an Additional Bank

IMPORTANT In additional banks, you can install I/O modules to the left side, right side, or both sides of the power supply.
The system design determines how to use the following table.

Use this table to calculate power consumption in an additional bank.

Module Power Consumption Calculation for an Additional Bank

Side of Power Supply	Device Cat. No.	Number of Modules(1)	Module Current Requirements		Calculated Current = (Number of Modules) x (Module Current Requirements)	
			at 5V DC (in mA)	at 24V DC (in mA)	at 5V DC (in mA)	at 24V DC (in mA)
Left - Optional in an extra bank	I/O Modules **IMPORTANT**: Insert a separate row in this calculation for each I/O module.	Up to 8	Module-specific	Module-specific		
	Total Current Required(2):					
Right - Optional in one bank	I/O Modules **IMPORTANT**: Insert a separate row for each I/O module.	Up to 8	Module-specific	Module-specific		
	Total Current Required(2):					
Total Current Required for Bank if Modules Are Installed on Both Sides of the Power Supply(3):						

(1) You can install up to eight modules in additional banks if the power supply distance ratings for the modules validate the system design.
(2) This number must not exceed the power supply current capacity for this side of the bank.
(3) This number must not exceed the power supply current capacity for the bank.

Physical Placement of I/O Modules

Depending on the controller catalog number, Compact GuardLogix 5370 controllers support 8...30 I/O modules. For more information on catalog numbers, see Local Expansion Modules on page 62.

Consider these factors when determining the physical placement of I/O modules:

- You can install I/O modules in local and extra banks.
- You can install I/O modules to the left and right of the power supply.
- When a system requires multiple banks, you can install the additional banks horizontally or vertically, as shown in the Example of Banks and System Configurations on page 63.
- Each I/O module also has a power supply distance rating and maximum current draw. Considered jointly, distance ratings and current draw determine where I/O modules can be placed in a bank and what configuration of modules can be installed in the bank.

  For more information on power supply distance ratings, see Power Supply Distance Rating on page 71. For more information on system power consumption, see Calculate System Power Consumption on page 67.

Local Bank

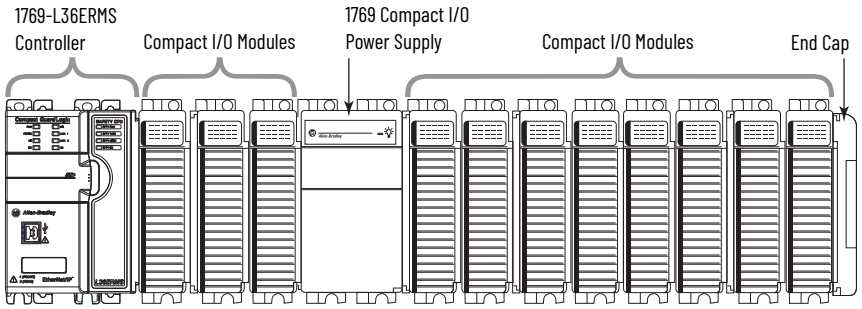
To validate the local bank design, confirm that the design meets these requirements:

- The controller is the leftmost device in the local bank.
- No more than three modules are installed between the controller and the left side of the power supply.
- No more than eight modules are installed to the right of the power supply.
- The power consumption of the modules on each side of the power supply does not exceed the capacity of the power supply for that side.
- The total power consumption by all modules in the bank does not exceed the capacity of the power supply for the entire bank.
- Modules are installed such that all power supply distance rating and system power consumption requirements are met.

  For example, the 1769-SDN scanner has a power supply distance rating of four. If the design includes the installation of a 1769-SDN scanner with greater than three modules between it and the power supply, the design is invalid.

IMPORTANT If you install a module that violates its power supply distance rating specification, the system can appear to operate normally for a time, but could experience operational issues over time, such as I/O faults.

Example of a Local Bank



Additional Banks

If your application calls for twelve or more I/O modules, at minimum, you must install the modules in extra banks. The conditions of each application determine the number of extra banks.

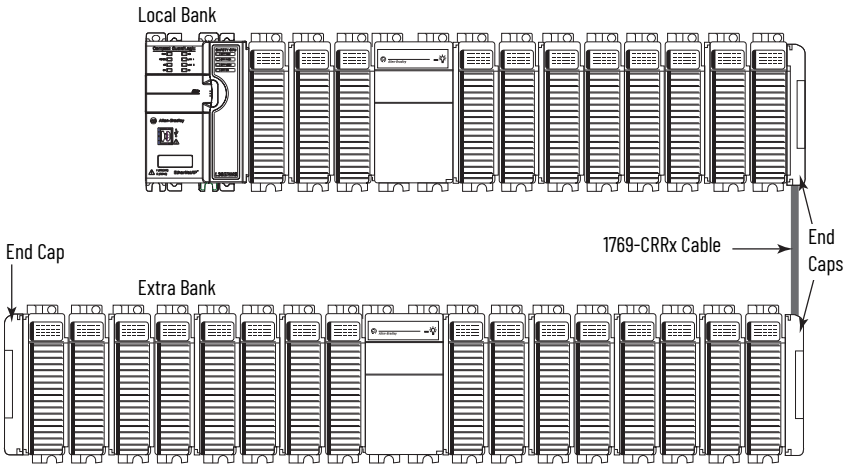
Once the local bank design is validated, you must validate the design for any additional banks. To validate extra bank designs, confirm that the design meets these requirements:

- Compact I/O communication bus expansion cables are used properly.

  Compact I/O expansion cables have the same dimensions as the end caps regardless of whether they are installed at the right or left side of the communication bus

- No more than eight modules are installed on either side of the power supply.
- The power consumption of the modules on each side of the power supply does not exceed the capacity of the power supply for that side.

- Modules are installed such that all power supply distance rating requirements are met.
- End caps are installed properly, as shown in the following graphic.



Power Supply Distance Rating

Compact GuardLogix 5370 controller systems do not have embedded I/O modules. You begin counting local expansion slots with the first Compact I/O module installed next to the power supply when determining where to install a Compact I/O module and meet its power supply distance rating.

In Compact GuardLogix 5370 controller systems, you can install Compact I/O modules to the left or right side of the power supply. You can also use local and extra banks in Compact GuardLogix 5370 controller systems, with each allowing the inclusion of Compact I/O modules.

Local Bank

In the local bank, the controller must be the leftmost device in the system and you can only install up to three modules between the controller and the power supply. Therefore, any Compact I/O modules that are installed to the left of the power supply in the local bank must be in a module slot that meets the module's power supply distance rating requirements.

Additional Banks

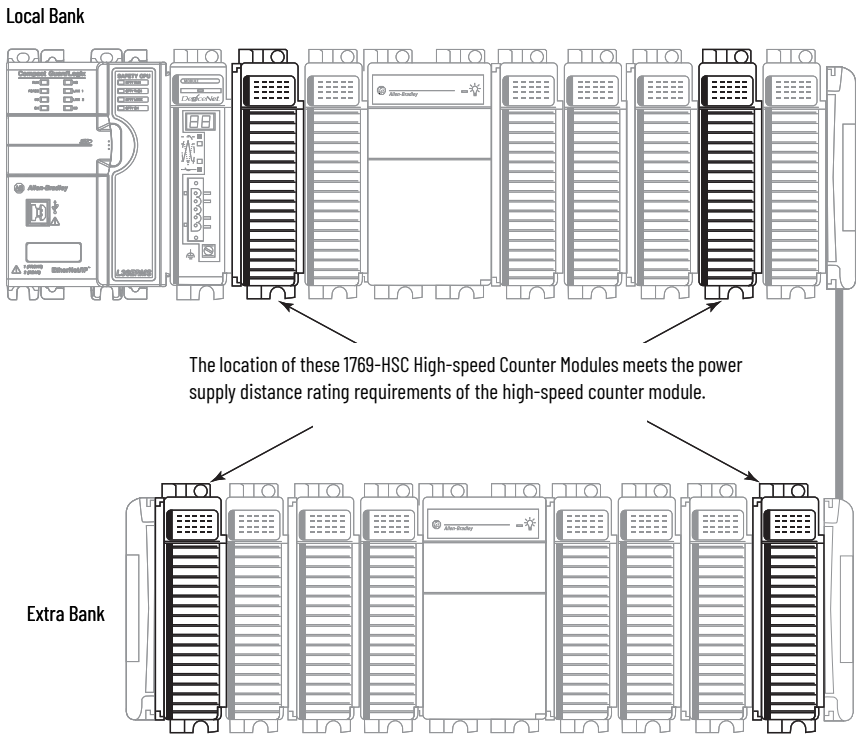
Compact GuardLogix 5370 controller systems also support the use of extra banks for the local expansion modules of the system. Every additional bank requires a 1769 Compact I/O power supply. The bank can be designed with local expansion modules on either side of the power supply.

Most Compact I/O modules have power supply distance rating values that allow you to install them in any slot on either side of the power supply in extra banks. Some Compact I/O modules have power supply distance ratings that affect where you can install them in the Compact GuardLogix 5370 controller system.

For example, the 1769-HSC Compact high-speed counter modules each have a power supply distance rating of four. These modules can be installed in local expansion module slots one through three.

In this case, you must install no more than three Compact I/O modules between the high-speed counter modules and the power supply, regardless of whether the modules are installed to the left or right of the power supply.

Example of High-speed Counter Modules Installed in a 1769-L36ERMS Control System

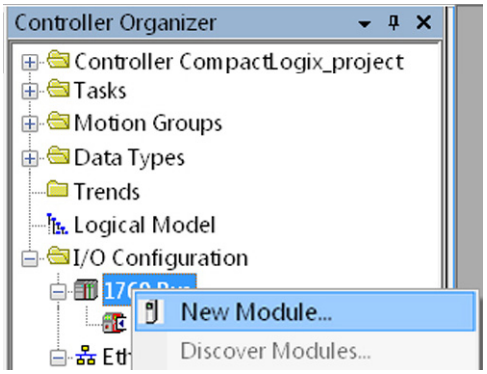


For more information about the power supply distance ratings for Compact I/O modules, see CompactLogix Selection Guide, publication 1769-SG001.

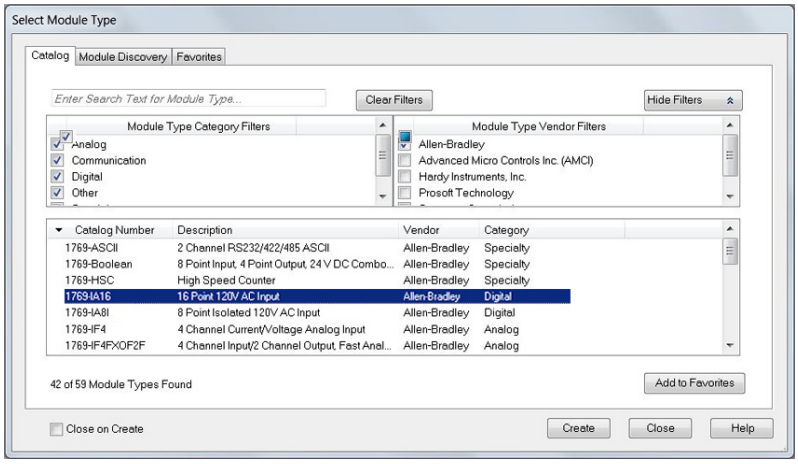
Configure Standard I/O

Complete these steps to add a Compact I/O module to your Compact GuardLogix 5370 controller system and configure it.

1. In the Controller Organizer, select and right-click the 1769 Bus under I/O Configuration, and choose New Module.

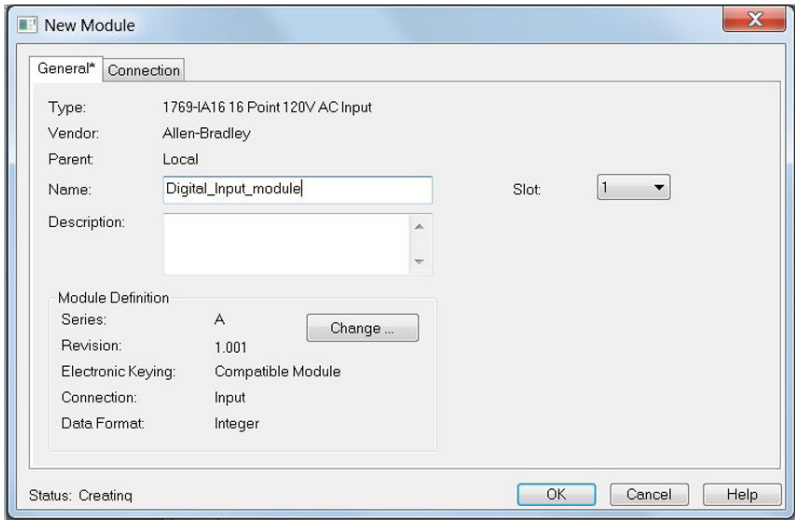


2. Select the desired I/O module and click Create.



The New Module dialog box appears.

3. Configure the new I/O module as necessary and click OK.



Common Configuration Parameters

While the configuration options vary from module to module, there are some common options you typically configure when using Compact I/O modules in a Compact GuardLogix 5370 controller system, as described in the following table.

Common Configuration Parameters

Configuration Option	Description
Requested packet interval (RPI)	The RPI specifies the interval at which data is transmitted or received over a connection. For 1769 Compact Local I/O modules, data is transmitted to the controller at the RPI. When scanned on the local bus or over an EtherNet/IP network, input modules are scanned at the RPI specified in the module configuration. Typically, you configure an RPI in milliseconds (ms). For I/O modules, the range is 0.5...750 ms. When scanned over a DeviceNet network, distributed input modules are scanned at the rate that the DeviceNet adapter that connects the input modules to the network supports. For example, the scan rate for distributed 1734 POINT I/O™ over DeviceNet can only occur as quickly as the 1734-ADN DeviceNet adapter can transmit the data.
Module definition	Set of configuration parameters that affect data transmission between the controller and the I/O module. The parameters include the following: • Series - Hardware series of the module. • Revision - Major and minor firmware revision levels that are used on the module. • Electronic Keying - See LOGIX-AT001 for Electronic Keying information. • Connection - Type of connection between the controller writing the configuration and the I/O module, such as Output. • Data format - Type of data that is transferred between the controller and I/O module and what tags are generated when the configuration is complete.
Module Fault on Controller If Connection Fails While in Run Mode	This option determines how the controller is affected if the connection to an I/O module fails in Run mode. You can configure the project so that a connection failure causes a major fault on the controller or not. The default setting is for the option to be enabled, that is, if the connection to an I/O module fails in Run mode, a major fault occurs on the controller.

I/O Connections

A Logix 5000 system uses connections to transmit I/O data, as described in the following table.

I/O Module Connections

Connection	Description
Direct	A direct connection is a real-time, data-transfer link between the controller and an I/O module. The controller maintains and monitors the connection. Any break in the connection, such as a module fault, causes the controller to set fault status bits in the data area that is associated with the module. Typically, analog I/O modules, diagnostic I/O modules, and specialty modules require direct connections.
Rack-optimized	For digital I/O modules, you can select rack-optimized communication. This option is used with distributed I/O modules and the Rack Optimization connection selection is made when configuring the remote adapter. For example, if you want to use a rack-optimized connection with digital I/O modules in a remote 1734 POINT I/O system, you configure the 1734-AENT(R) module to use a connection type of Rack Optimization. A rack-optimized connection consolidates connection usage between the controller and the digital I/O modules in a remote chassis or on one DIN rail. Rather than having individual, direct connections for each I/O module, there is one connection for the entire rack (or DIN rail).

Configure Standard Distributed I/O Modules on an EtherNet/IP Network

Your Compact GuardLogix 5370 controller system can use distributed I/O modules on an EtherNet/IP network.

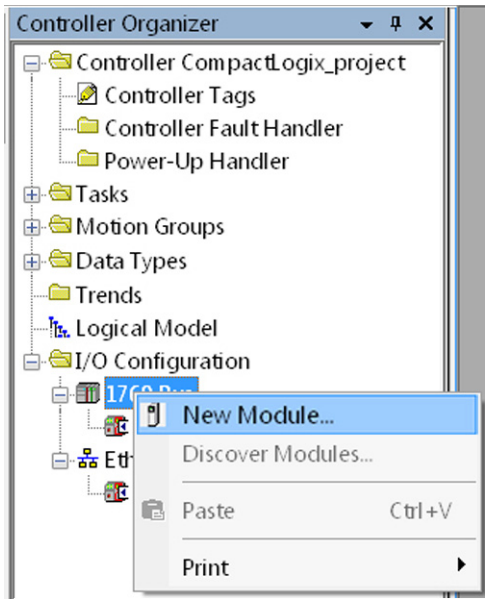
IMPORTANT When you add distributed I/O modules, remember to count the remote Ethernet adapter to remain within the maximum number of EtherNet/IP network nodes limitation for your controller.

The remote I/O modules that are connected to the controller via the Ethernet adapter are not counted toward the maximum Ethernet node limit for the controller.

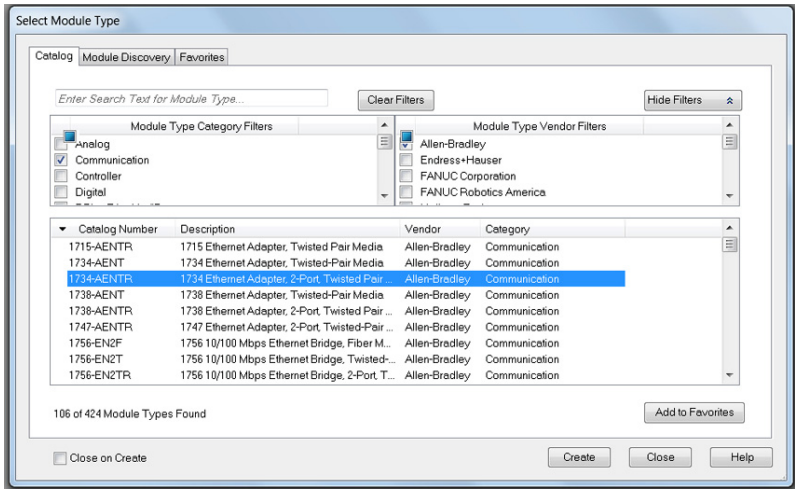
For more information on node limitations, see Nodes on EtherNet/IP Network on page 52.

Complete these steps to configure distributed I/O modules on an EtherNet/IP network.

1. In the Controller Organizer, select and right-click the 1769 Bus under I/O Configuration, and choose New Module.

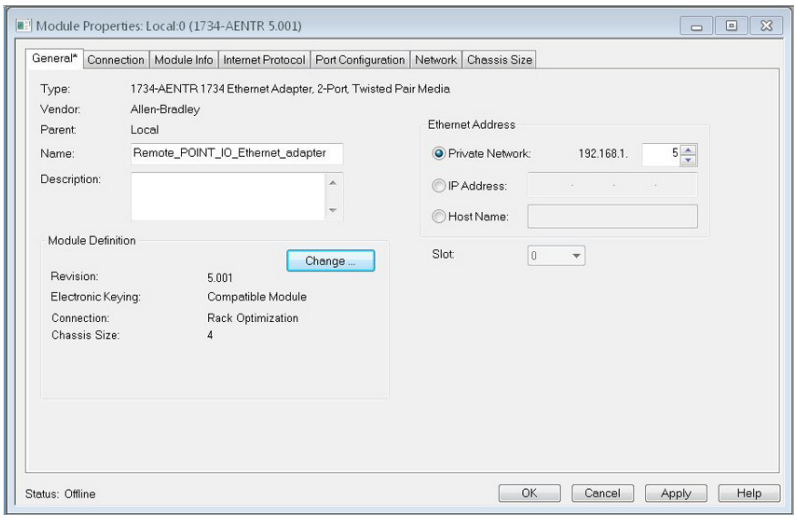


2. Select the desired Ethernet adapter and click Create.

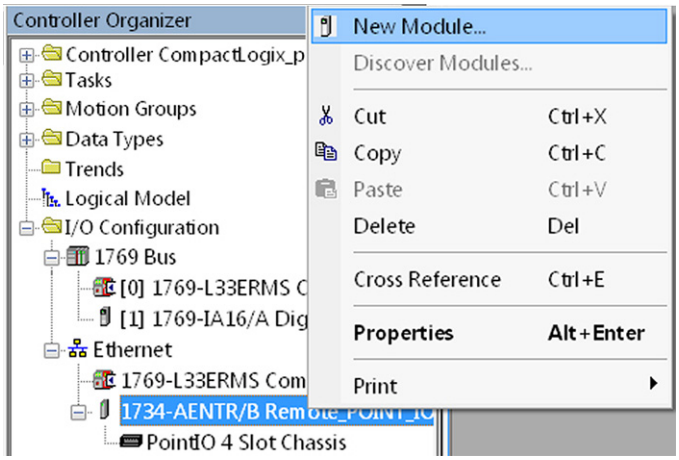


The New Module dialog box appears.

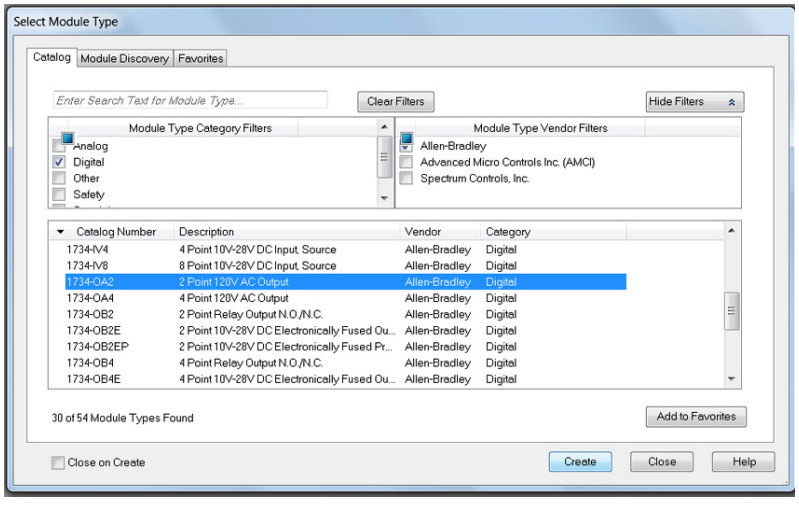
3. Configure the new Ethernet adapter as necessary and click OK.



4. In the Controller Organizer, select and right-click the new adapter, and choose New Module.

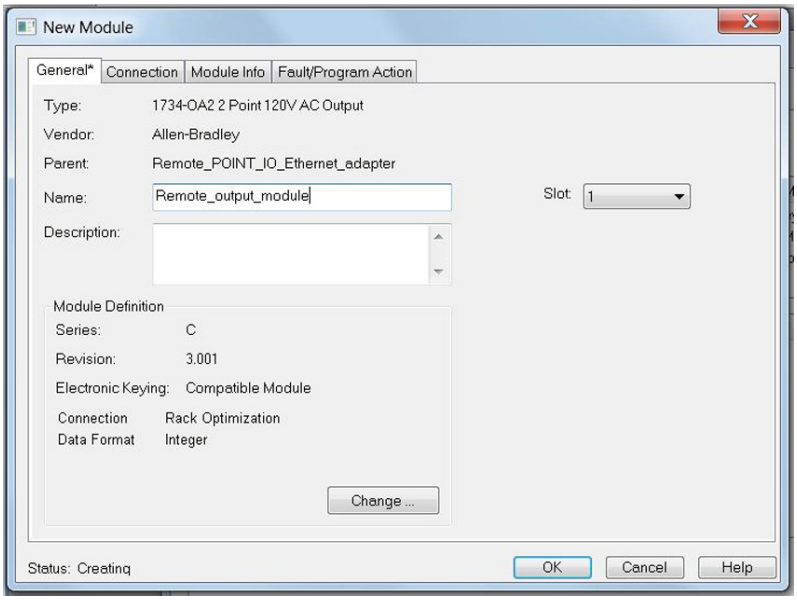


5. Select the desired I/O module and click Create.



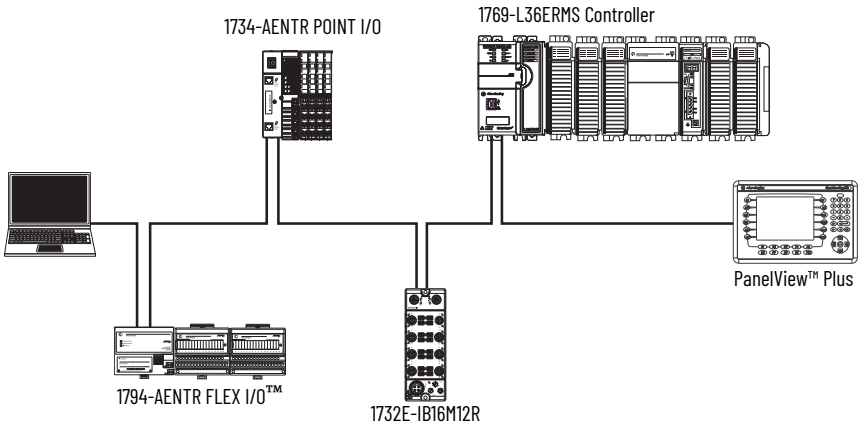
The New Module dialog box appears.

6. Configure the new I/O module as necessary and click OK.



7. To add additional distributed I/O modules, repeat steps 4...6.

Example 1769-L36ERMS Control System with Distributed I/O Modules on an EtherNet/IP Network

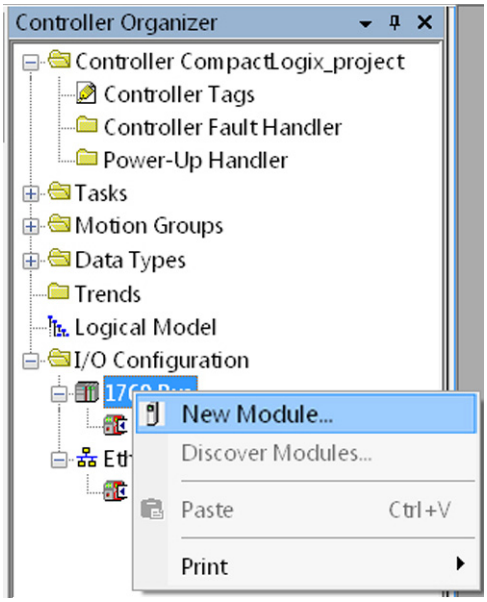


Configure Standard Distributed I/O Modules on a DeviceNet Network

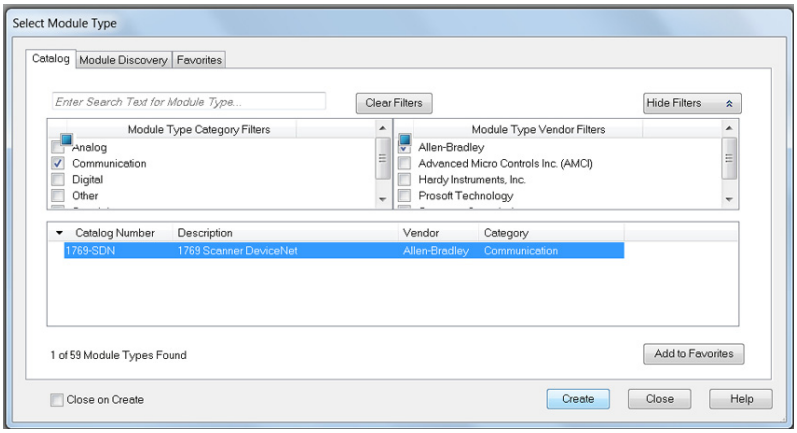
Your Compact GuardLogix 5370 controller system can use standard distributed I/O modules on a DeviceNet network.

To configure standard distributed I/O modules on a DeviceNet network, complete these steps.

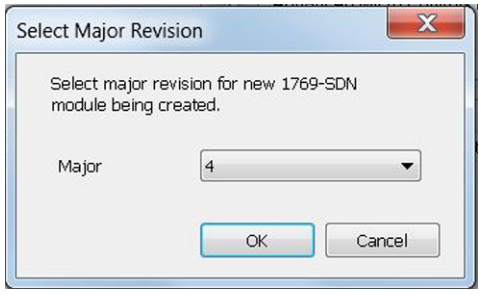
1. If you have not done so, install a 1769-SDN Compact I/O DeviceNet scanner into the local bank of your Compact GuardLogix 5370 controller system.
2. In the Controller Organizer, select and right-click the 1769 Bus under I/O Configuration, and choose New Module.



3. Select the 1769-SDN scanner and click Create.

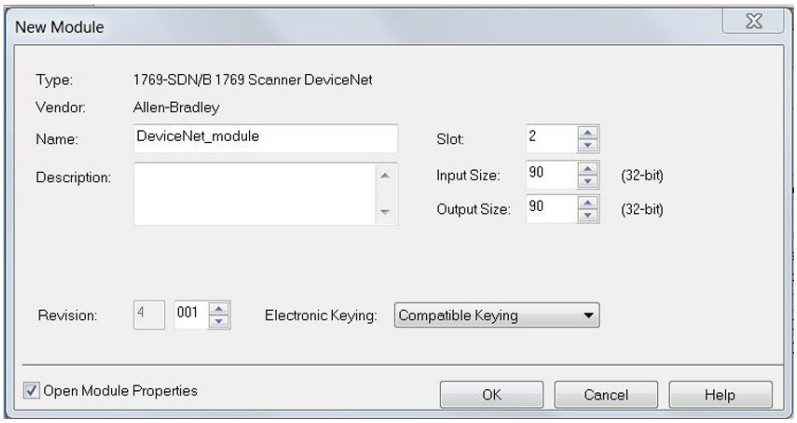


4. Choose a Major Revision and click OK.



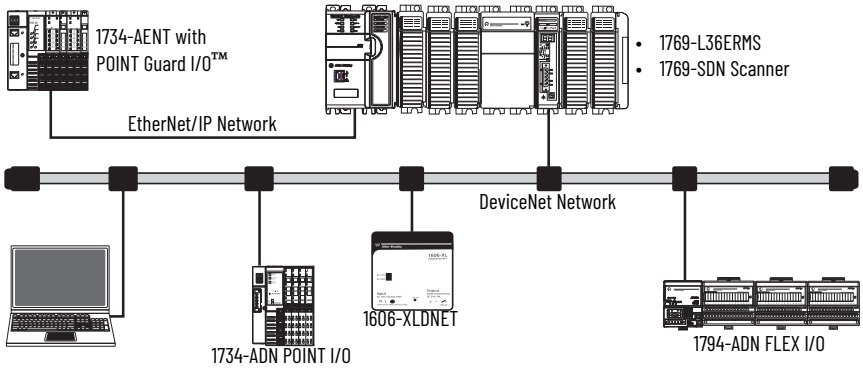
The New Module dialog box appears.

5. Configure the new 1769-SDN scanner as necessary and click OK.



6. Use RSNetWorx for DeviceNet software to define the scan list in the 1769-SDN scanner to communicate data between the devices and the controller through the scanner.

Example 1769-L36ERMS Control System with Distributed I/O Modules on an DeviceNet Network

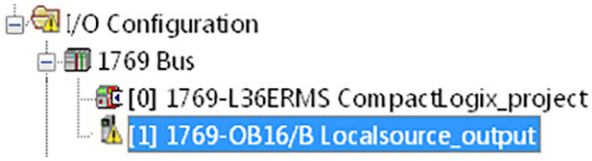


Monitor Standard I/O Modules

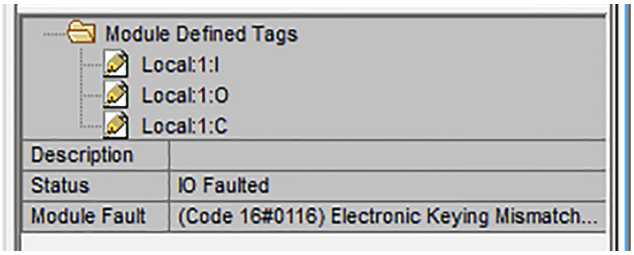
With Compact GuardLogix 5370 controllers, you can monitor I/O modules in the following ways:

- QuickView® Pane below the Controller Organizer
- Connection tab in the Module Properties dialog box
- Programming logic to monitor fault data so you can act

When a fault occurs on an I/O module, a yellow triangle on the module in the Controller Organizer alerts you to the fault.

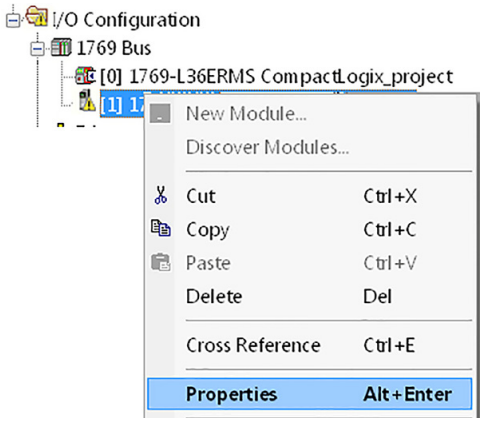


The following graphic shows the Quick View Pane, which indicates the fault type.



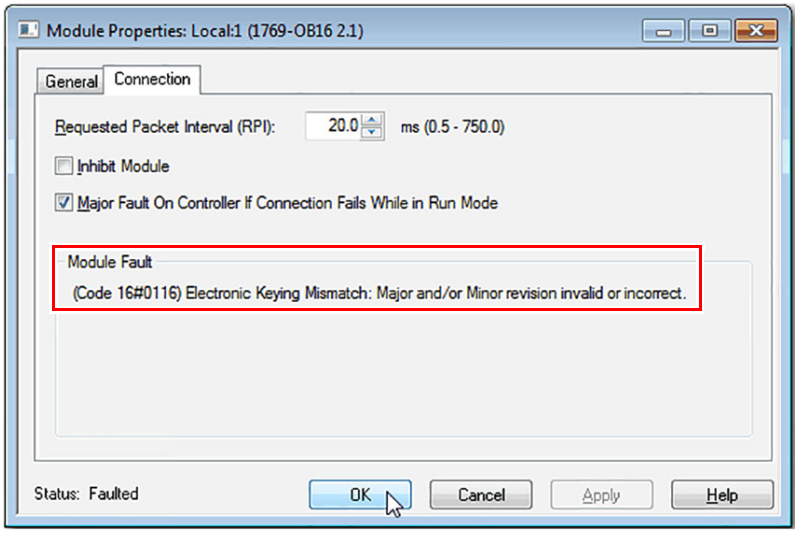
To view the fault description on the Connection tab in the Module Properties dialog box, complete these steps.

1. In the Controller Organizer, select and right-click the faulted I/O module under I/O Configuration, and choose Properties.



2. On the Module Properties dialog box, click the Connection tab.

   In the Module Fault section, use the fault description to diagnose and remedy the issue.



End Cap Detection and Module Faults

End cap detection is performed through the last module on a 1769 Bus. If that module experiences a fault such that it cannot communicate on the 1769 Bus, the following events occur:

- End cap detection fails
- Controller faults

Notes:

Add, Configure, Monitor, and Replace CIP Safety I/O Devices

Add and Configure Safety I/O Devices

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

- IP address for EtherNet/IP™ networks; see page 87
- Safety network number (SNN); see page 87
- Reaction time limit; see page 87
- Configuration signature; see page 91
- Safety input, output, and test parameters, refer to the module's user documentation and the Logix Designer application's online help.

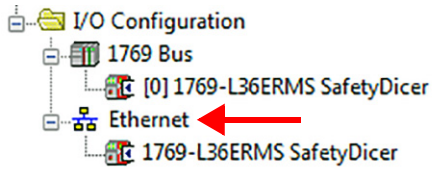
You can configure safety I/O devices via the Compact GuardLogix® controller by using the Logix Designer application.

Safety I/O devices support standard and safety data. Device configuration defines what data is available.

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

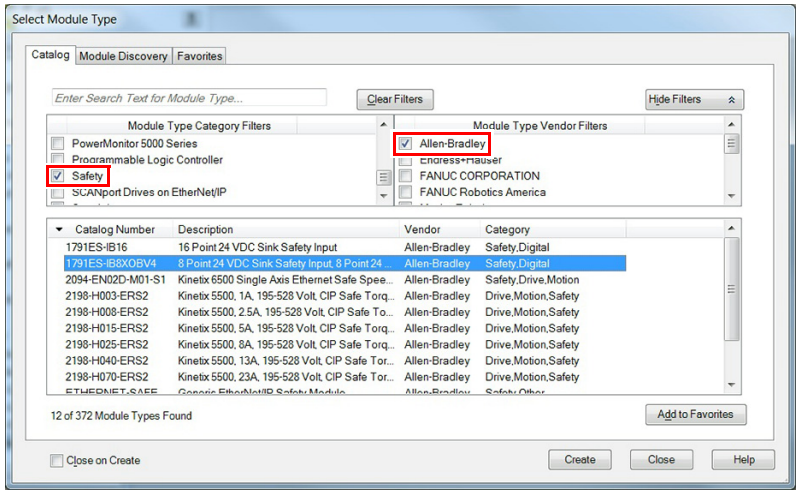
You cannot add or delete a safety I/O device while online.

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

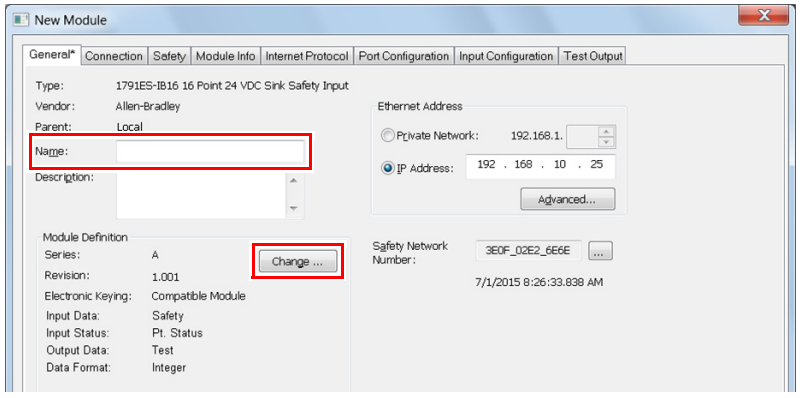


2. From the Catalog tab, select the safety I/O device.

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



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

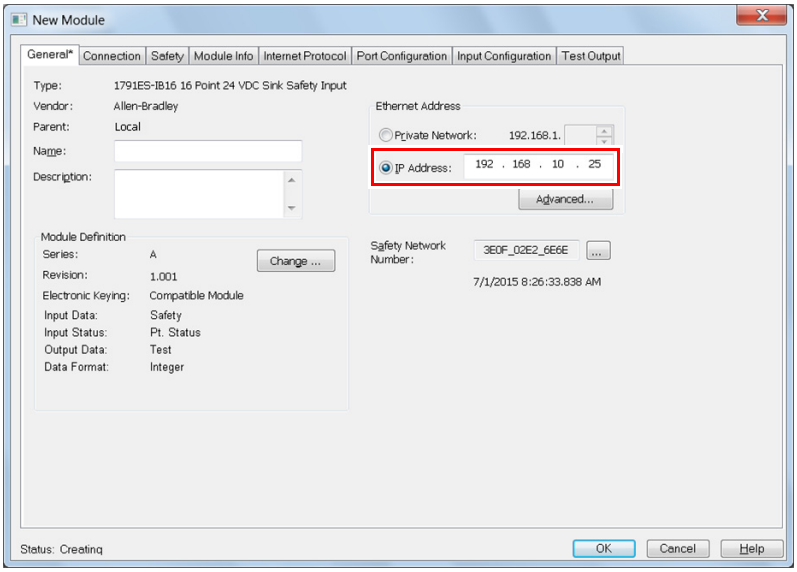


5. To modify the Module Definition settings, click Change (if necessary).

Set the IP Address

To set the IP address, you can adjust the rotary switches on the device; use DHCP software (available from Rockwell Automation); use the Logix Designer application (as shown in this step); or retrieve the default address from nonvolatile memory.

1. Enter the IP address for EtherNet/IP networks.



2. Click OK.

Set the IP Address by Using Network Address Translation (NAT)

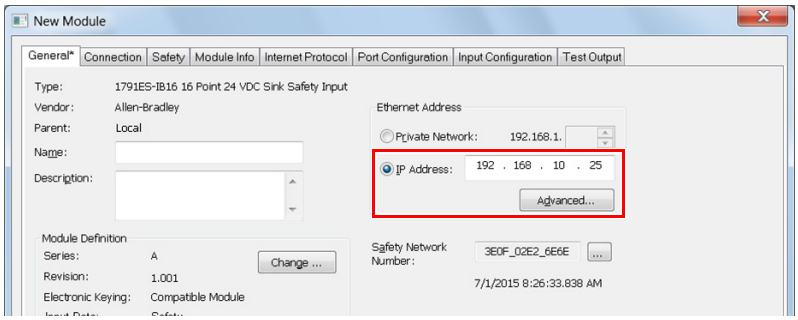
NAT translates one IP address to another IP address via a NAT-configured router or switch. The router or switch translates the source and destination addresses within data packets as traffic passes between subnets.

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

If you are using NAT, follow these steps to set the IP address.

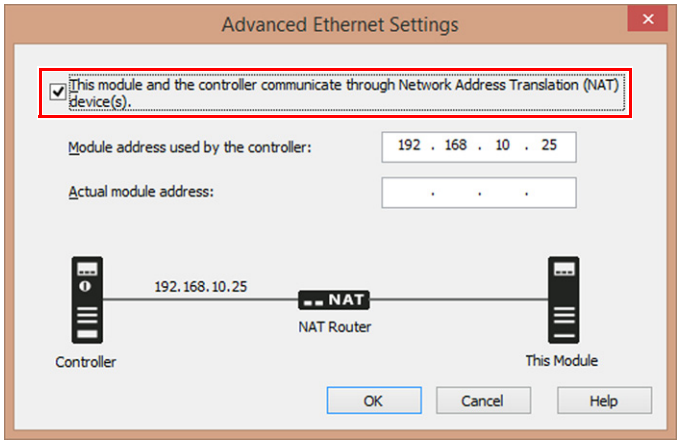
1. In the IP Address field, type the IP address for the controller.

   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. To indicate that this module and the controller communicate through NAT devices, select the checkbox.



4. Type the Actual module address.

If you configured the IP address with 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's Internet Protocol tab.

5. Click OK.

The controller uses the translated address but CIP Safety™ protocol requires the actual address of the device.

Unicast Connections on EtherNet/IP Networks

Unicast connections are point-to-point connections between a source and a destination node. You do not have to enter a minimum or maximum RPI range or default value for this type of connection.

To configure unicast connections, choose the Connection tab and check Use Unicast Connection over EtherNet/IP.

Set the Safety Network Number (SNN)

The assignment of a time-based SNN is automatic when adding new safety I/O devices. Subsequent safety device additions to the same network are assigned the same SNN defined within the lowest address on that CIP safety network.

For most applications, the automatic, time-based SNN is sufficient. However, there are cases when the manipulation of an SNN is required.

See The Safety Network on page 46.

Set the Connection Reaction Time Limit

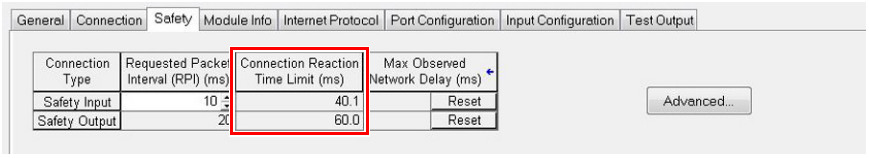
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data that is used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. The following equations are used to determine the Connection Reaction Time Limit:

Input Connection Reaction Time Limit =
Input RPI x [Timeout Multiplier + Network Delay Multiplier]

Output Connection Reaction Time Limit =
Safety Task Period x [Timeout Multiplier + Network Delay Multiplier - 1]

The Connection Reaction Time Limit is shown on the Safety tab of the Module Properties dialog box.

Connection Reaction Time Limit



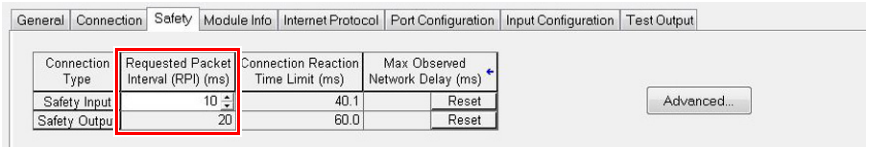
Specify the Requested Packet Interval (RPI)

The RPI specifies the period that data updates over a connection. For example, an input module produces data at the RPI that you assign.

For safety input connections, you can set the RPI on the Safety tab of the Module Properties dialog box. The RPI is entered in 1 ms increments, with a range of 1...100 ms. The default is 10 ms.

The Connection Reaction Time Limit is adjusted immediately when the RPI is changed via the Logix Designer application.

Requested Packet Interval



For safety output connections, the RPI is fixed at the safety task period. If the corresponding Connection Time Reaction Limit is not satisfactory, you can adjust the safety task period via the Safety Task Properties dialog box.

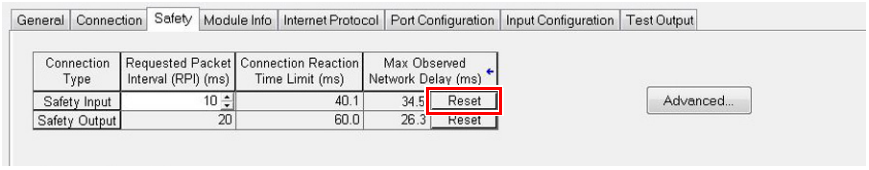
See Safety Task Period Specification on page 114 for more information on the safety task period.

For typical applications, the default RPI is usually sufficient. For more complex requirements, use the Advanced button to modify the Connection Reaction Time Limit parameters, as described on page 89.

View the Maximum Observed Network Delay

When the Compact Guardlogix controller receives a safety packet, the software records the maximum observed network delay. For safety inputs, the Maximum Observed Network Delay displays the round-trip delay from the input module to the controller and the acknowledge back to the input module. For safety outputs, it displays the round-trip delay from the controller to the output module and the acknowledge back to the controller. The Maximum Observed Network Delay is shown on the Safety tab of the Module Properties dialog box. When online, click Reset to reset the Maximum Observed Network Delay.

Reset the Maximum Observed Network Delay

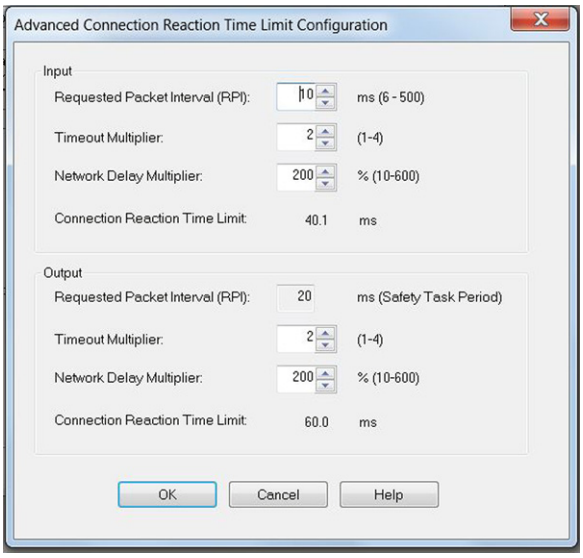


IMPORTANT The actual Maximum Network Delay time from the producer to the consumer is less than the value displayed in the Maximum Network Delay field on the Safety tab. In general, the actual maximum message delay is approximately one-half the Maximum Network Delay value that is displayed.

Set the Advanced Connection Reaction Time Limit Parameters

Configure connection parameters like the timeout multiplier and network delay multiplier on the Advanced Connection Reaction Time Limit dialog box.

Advanced Configuration



- **Timeout Multiplier** - Determines the number of RPIs to wait for a packet before declaring a connection timeout. This translates into the number of messages that can be lost before a connection error is declared.

  For example, a timeout multiplier of 1 indicates that messages must be received during each RPI interval. A Timeout Multiplier of 2 indicates that 1 message can be lost as long as at least 1 message is received in 2 times the RPI (2 x RPI).

- **Network Delay Multiplier** - Defines the message transport time that the CIP Safety protocol enforces. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and the acknowledge back to the producer. You can use the Network Delay Multiplier to reduce or increase the Connection Reaction Time Limit in cases where the enforced message transport time is significantly less or more than the RPI. For example, it can be helpful to adjust the Network Delay Multiplier when the RPI of an output connection is the same as a lengthy safety task period.

  For cases where the input RPI or output RPI are relatively slow or fast as compared to the enforced message delay time, the Network Delay Multiplier can be approximated by using one of the two methods.

Method 1: Use the ratio between the input RPI and the safety task period. Use this method only when all the following conditions apply:

- If the path or delay is approximately equal to the output path or delay.
- The input RPI has been configured so that the actual input message transport time is less than the input RPI.
- The safety task period is slow relative to the Input RPI.

  Under these conditions, the Output Network Delay Multiplier can be approximated as follows:

  Input Network Delay Multiplier x [Input RPI ¸ Safety Task Period]

EXAMPLE Calculate the Approximate Output Network Delay Multiplier

If:

Input RPI = 10 ms
Input Network Delay Multiplier = 200%
Safety Task Period = 20 ms

Then, the Output Network Delay Multiplier equals:

200% x [10 ÷ 20] = 100%

Method 2: Use the Maximum Observed Network Delay. If the system is run for an extended time through its worst-case loading conditions, the Network Delay Multiplier can be set from the Maximum Observed Network Delay. This method can be used on an input or output connection. After the system has been run for an extended time through its worst-case loading conditions, record the Maximum Observed Network Delay.

The following equation approximates the Network Delay Multiplier:

[Maximum Observed Network Delay + Margin_Factor] ¸ RPI

EXAMPLE Calculate the Network Delay Multiplier from Maximum Observed Network Delay

If:

RPI = 50 ms
Maximum Observed Network Delay = 20 ms
Margin_Factor = 10

Then, the Network Delay Multiplier equals:

[20 + 10] ÷ 50 = 60%

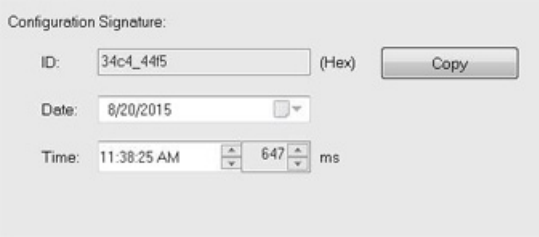
Configuration Signature

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 a module's configuration.

Configuration via the Logix Designer Application

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

View and Copy the Configuration Signature



Different Configuration Owner (listen-only connection)

When another controller owns the I/O device configuration, you must copy the module configuration signature from the controller's project and paste it into the Safety tab of the Module Properties dialog box.

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

Reset Safety I/O Device 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. Communication error is displayed if the device read fails.

When online, click Reset Ownership to reset the device to its out-of-box configuration.

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

Address Safety I/O Data

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

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

- To monitor safety tag data, see Develop Safety Applications on page 113.
- For information on how to address standard I/O devices, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

Safety I/O Modules Address Format

A Safety I/O module address follows this format:

Modulename:Type.Member

Safety I/O Module Address Format Explanation

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 Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Output-only module	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	Combination I/O	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Kinetix 5500, Kinetix 5700, and PowerFlex 527 Drive Address Format

A Kinetix® 5500, Kinetix 5700, and PowerFlex® 527 drive address follows this format:

Drivename:Type.Member

Drive Safety I/O Drive Address Format Explanation

Where	Is	
Drivename	The name of the Kinetix or PowerFlex drive	
Type	Type of data	Input: SI Output: SO
Member	Specific data from the I/O device	
	Input-only module	Drivename:SI.ConnectionStatus Drivename:SI.RunMode Drivename:SI.ConnectionFaulted Drivename:SI.Status Drivename:SI.TorqueDisabled Drivename:SI.SafetyFault Drivename:SI.ResetRequired
	Output-only module	Drivename:SO.Command Drivename:SO.SafeTorqueOff Drivename:SO.Reset

Monitor Safety I/O Device Status

You can monitor safety I/O device status via explicit messaging or via the status indicators on the I/O devices.

These publications provide information on I/O module troubleshooting:

- Guard I/O™ EtherNet/IP Modules User Manual, publication 1791ES-UM001
- POINT Guard I/O™ Safety Modules Installation and User Manual, publication 1734-UM013
- Kinetix 5500 Servo Drives User Manual, publication 2198-UM001
- Kinetix 5700 Servo Drives User Manual, publication 2198-UM002
- PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002

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

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

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

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

1. In the Controller Organizer, right-click the device and choose Properties.
2. Click the Connection tab.
3. Check Inhibit Connection.
4. Click Apply and then OK.

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

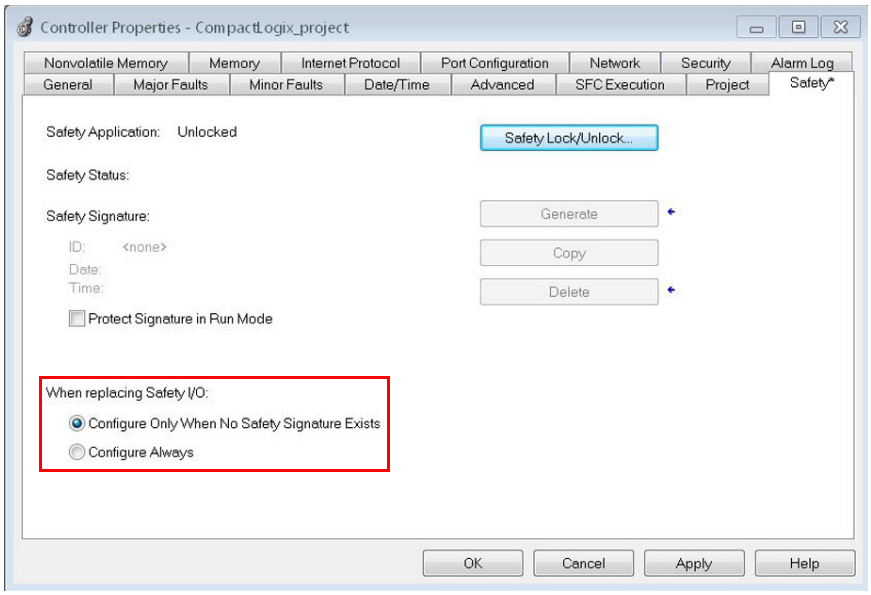
1. In the Controller Organizer, right-click the device and choose Properties.
2. Click the Safety tab.
3. Click Reset Ownership.

Replace a Safety I/O Device

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

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

Safety I/O Device Replacement



- If you are relying on a portion of the CIP Safety system to maintain SIL 3 behavior during device replacement and functional testing, the Configure Always feature cannot be used. Go to Configure Only When No Safety Signature Exists Replacement on page 95.
- If the entire routable CIP Safety control system is not being relied on to maintain SIL 3/PLe during the replacement and functional testing of a device, the Configure Always feature can be used. Go to Configure Always Replacement on page 100.

Configure Only When No Safety Signature Exists Replacement

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

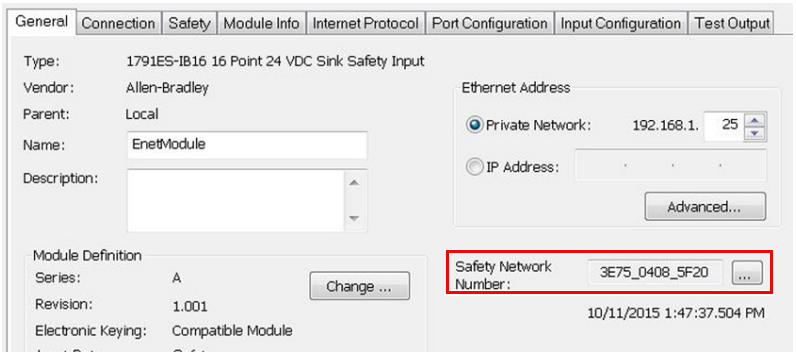
If the project is configured as 'Configure Only When No Safety Signature Exists', follow the appropriate steps in the following table to replace a safety I/O device based on your scenario. Once you have completed the steps correctly, the DeviceID matches the original, which enables the safety controller to download the proper device configuration and re-establish the safety connection.

Replacing a Module

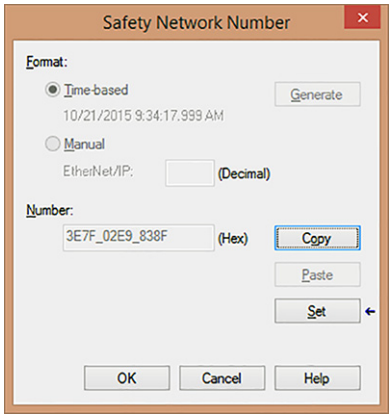
Compact GuardLogix Safety Signature Exists	Replacement Module Condition	Action Required
No	No SNN (Out-of-box)	None. The device is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The device is ready for use.
Yes	No SNN (Out-of-box)	See Scenario 1 - Replacement Device is Out-of-box and Safety Signature Exists on page 96.
Yes	Different SNN from original safety task configuration	See Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists on page 97.
No		See Scenario 3 - Replacement Device SNN is Different from Original and No Safety Signature Exists on page 99.

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

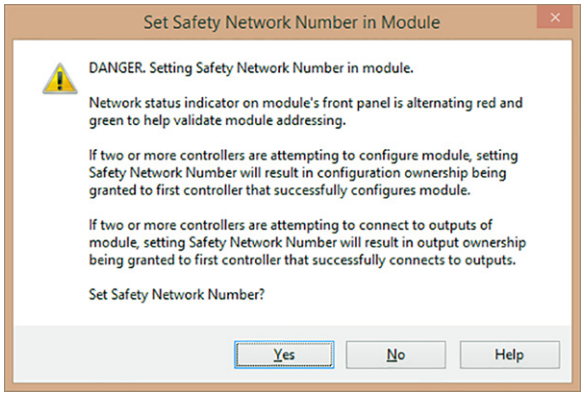
1. Replace the I/O device with the new I/O device.
2. Right-click the replacement safety I/O device and choose Properties.
3. To open the Safety Network Number dialog box, click ... to the right of the safety network number.



4. Click Set.



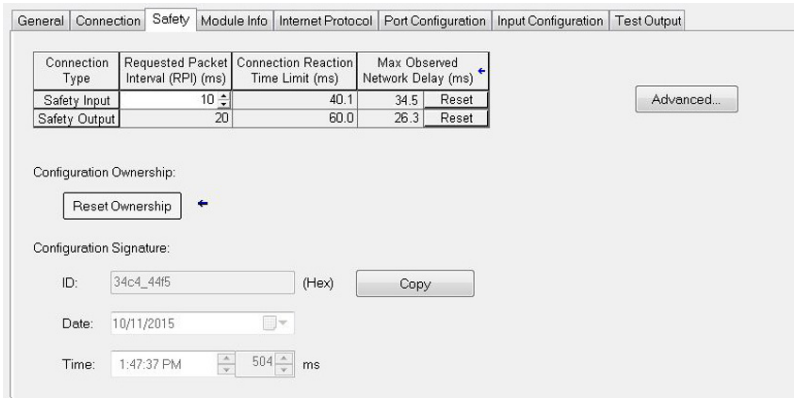
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.



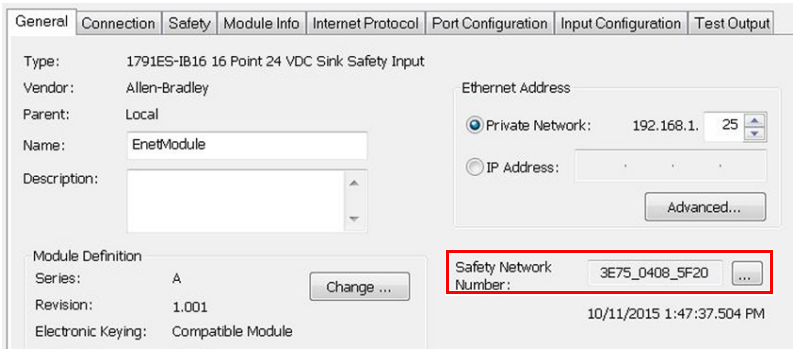
6. Follow your company-determined procedures to test the replaced I/O device and system and to authorize the system for use.

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

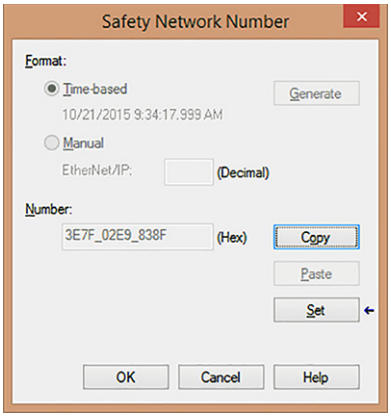
1. Replace the I/O device with the new I/O device.
2. Right-click your safety I/O device and choose Properties.
3. Click the Safety tab.



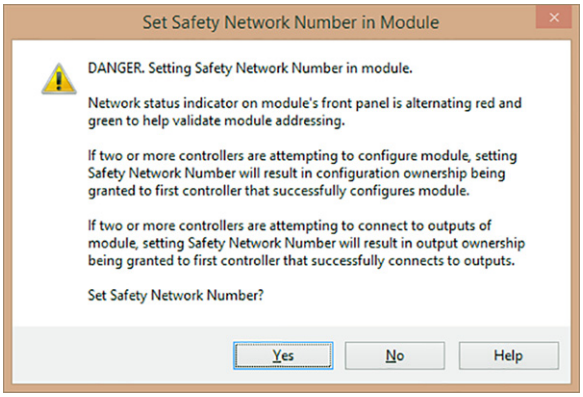
4. Click Reset Ownership.
5. Click OK.
6. Right-click the device and choose Properties.
7. To open the Safety Network Number dialog box, click ... to the right of the safety network number.



8. Click Set.



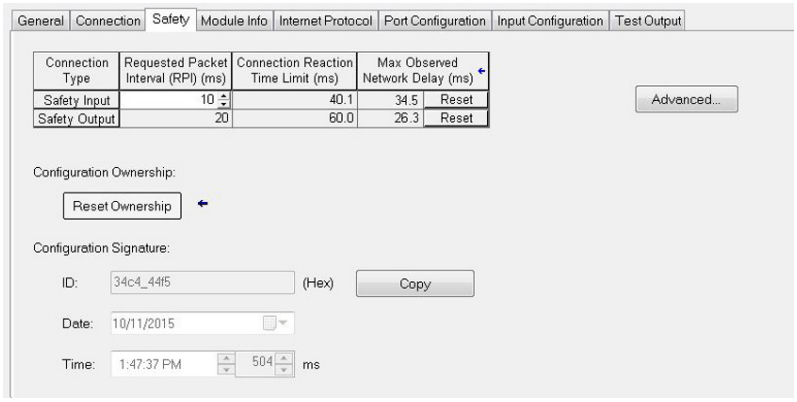
9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.



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

Configure Always Replacement

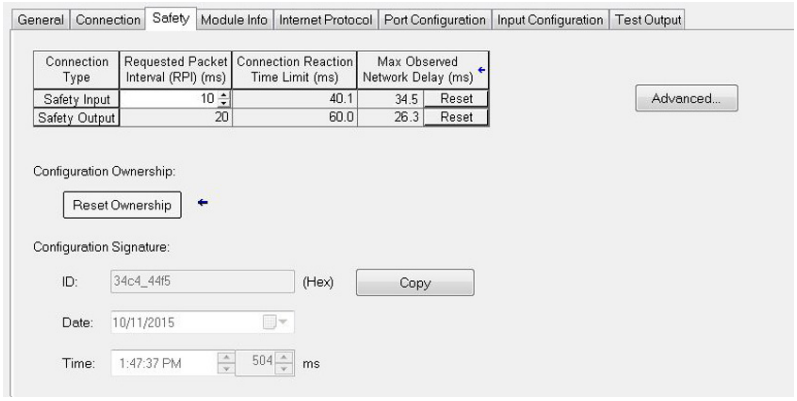
ATTENTION: Enable the 'Configure Always' feature only if the entire CIP Safety Control System is **not** being relied on to maintain SIL 3 behavior during the replacement and functional testing of a device.
Do not place devices that are in the out-of-box condition on a CIP Safety network when the Configure Always feature is enabled, except while following this replacement procedure.

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

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

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

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

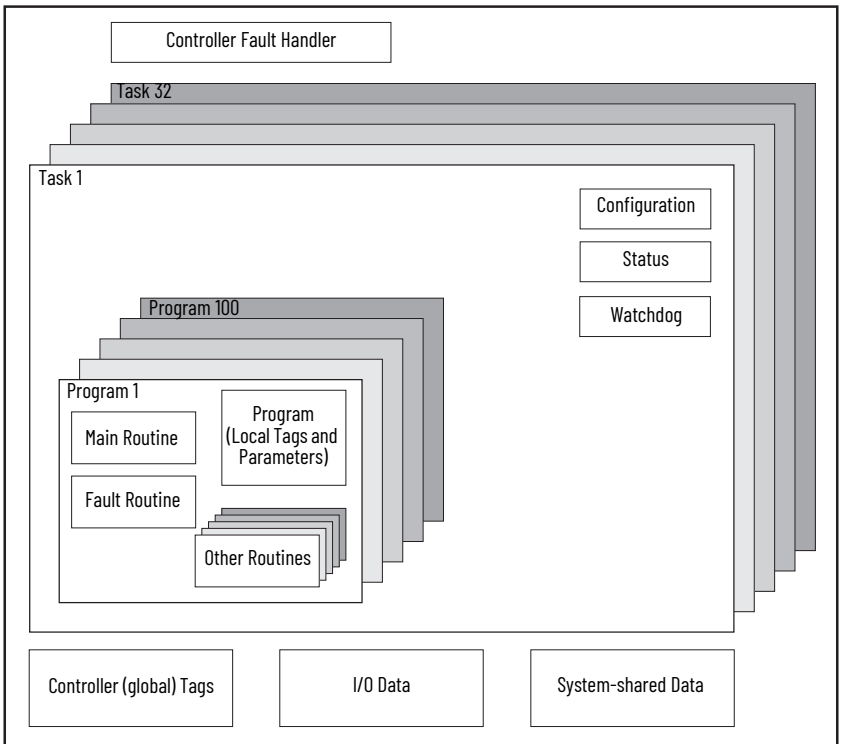


4. Click Reset Ownership.
5. Click OK.
6. Follow your company-determined procedures to test the replaced I/O device and system and to authorize the system for use.

Elements of a Control Application

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

- Tasks
- Programs
- Routines
- Local Tags and Parameters

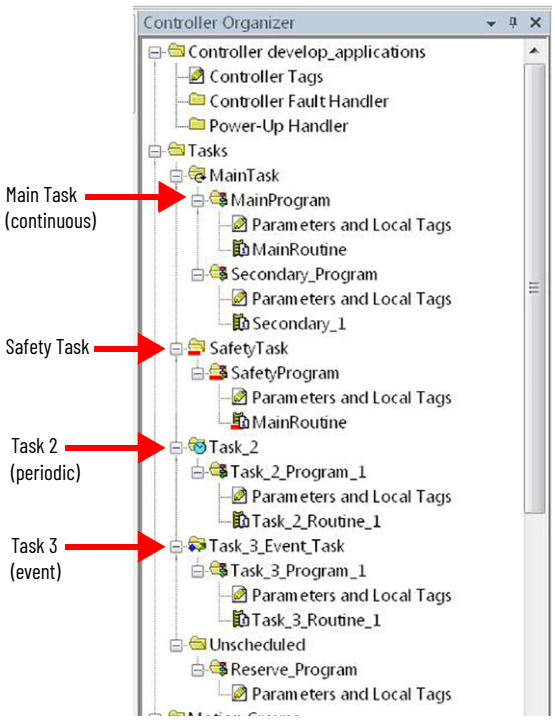


Tasks

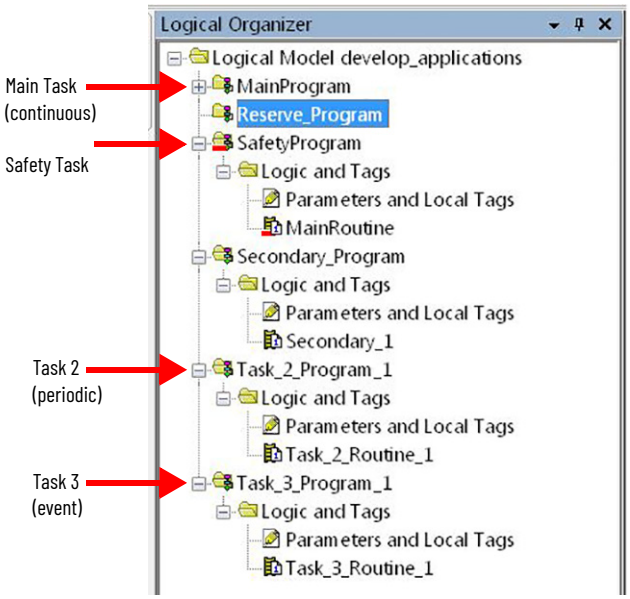
A Logix 5000™ controller lets you use multiple tasks to schedule and prioritize the execution of your programs that are based on criteria. This multitasking allocates the processing time of the controller among the different operations in your application:

- The controller executes only one task at a time.
- One task can interrupt the execution of another task and take control.
- In any given task, multiple programs can be used. However, only one program executes at a time.
- You can display tasks in the Controller or Logical Organizer views, as necessary.

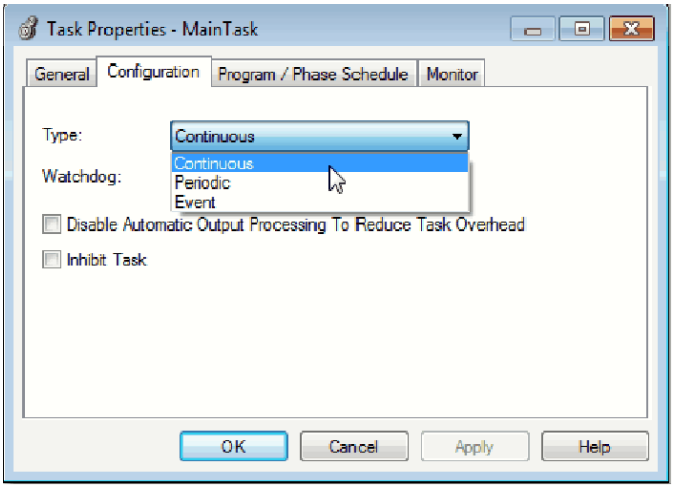
Controller Organizer



Logical Organizer



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



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

Task Types and Execution Frequency

Task Type	Task Execution	Description
Continuous	Always	The continuous task runs in the background. Any CPU time that is not allocated to other operations (such as motion, communication, and other tasks) is used to execute the programs in the continuous task: • The continuous task runs constantly. When the continuous task completes a full scan, it restarts immediately. • A project does not require a continuous task. If used, there can be only one continuous task.
Periodic	• At a set interval, such as every 100 ms • Multiple times in the scan of your other logic	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. • The performance of a periodic task depends on the type of Logix 5000 controller and on the logic in the task. • The periodic task processes I/O data for CompactLogix™, FlexLogix™, DriveLogix™, and SoftLogix™ controllers with the following considerations: – For CompactLogix, FlexLogix, and DriveLogix controllers, operates at priority 6 – For SoftLogix controllers, operates at Windows® priority 16 (Idle) – Higher-priority tasks take precedence over the I/O task and can affect processing – Executes at the fastest RPI that is scheduled for the system – Executes for as long as it takes to scan the configured I/O modules
Event	Immediately when an event occurs	An Event task performs a function only when an event (trigger) occurs. The trigger for the Event task can be the following: • A consumed tag trigger • An EVENT instruction • An axis trigger • A motion event trigger • Module input data state change

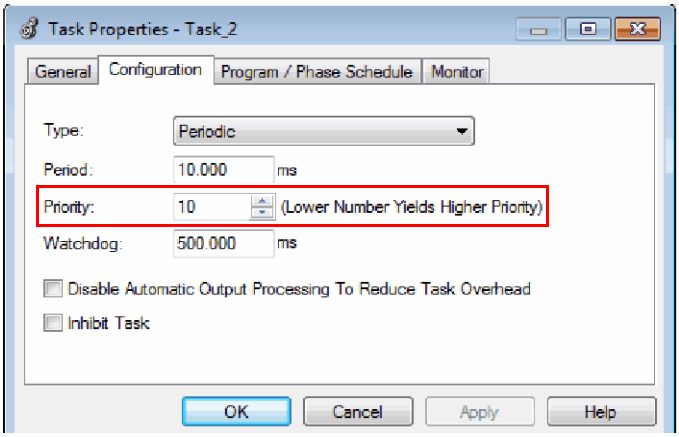
The Compact GuardLogix® 5370 controller supports up to 32 tasks, only one of which can be continuous.

A task can have up to 100 separate Programs per task, each with its own executable routines and program-scoped tags. Once a task is triggered (activated), all programs that are assigned to the task execute in the order in which they are grouped. Multiple tasks cannot share Programs and Programs appear only once in the Controller Organizer.

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. A periodic or event task interrupts the continuous task, which has the lowest priority.

You can configure periodic tasks to execute from the lowest priority of 15 up to the highest priority of 1. To configure the task priority, use the Task Properties dialog box.



Programs

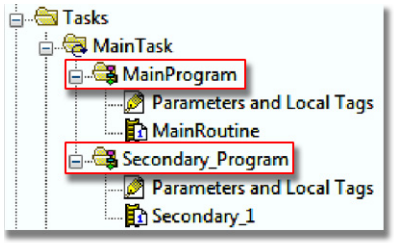
The controller operating system is a preemptive multitasking system that is in compliance with IEC 1131-3. This system provides the following:

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

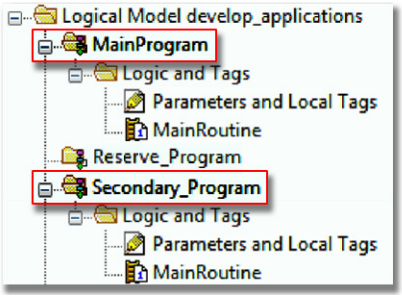
Each program contains the following:

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

Controller Organizer



Logical Organizer

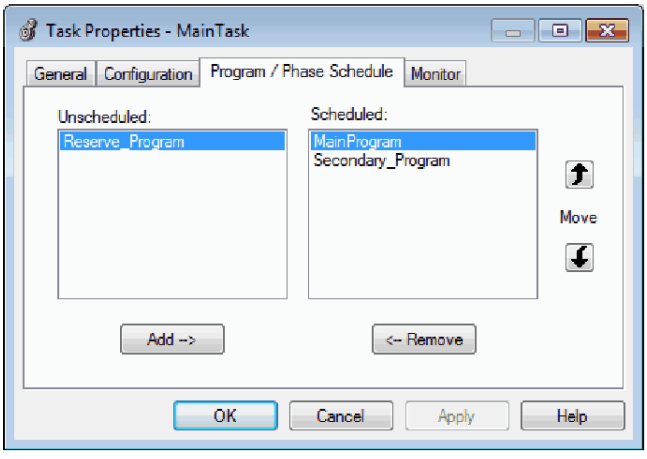


Scheduled and Unscheduled Programs

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

Unscheduled programs in 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 in 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.



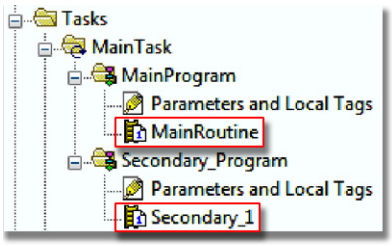
Routines

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

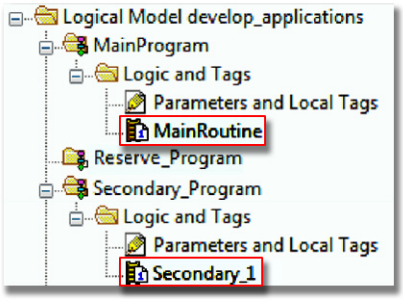
Each program has a main routine. This is the first routine to execute when the controller triggers the associated task and calls the associated program. Use logic, such as the Jump to Subroutine (JSR) instruction, to call other routines.

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

Controller Designer



Logical Designer



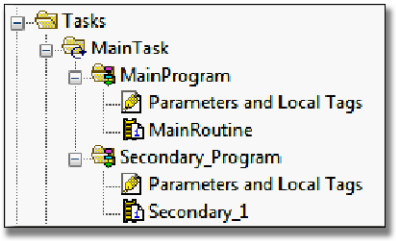
Local Tags and Parameters

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. For example, as shown in the following figure, you can use the tag name **north_tank_mix** instead of a numeric format, such as N7:0.0.

The tag name itself identifies the data. The tag lets you do the following:

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

Controller Organizer - Main Program Parameters and Local Tags



Program Tags Window - Main Program 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 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.

Extended Properties

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

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

Pass-through behavior is the ability to assign extended properties at a higher level of a structure or add-on instruction and have that extended property automatically available for all members. Pass-through behavior is available for descriptions, state identifiers, and engineering units and you can configure it. Configure pass-through behavior on the Project tab of the Controller Properties dialog box. If you choose not to show pass-through properties, only extended properties that have been configured for a given component are displayed.

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

You must know which tags have limits that are associated with them as there is no indication in the tag browser that extended properties are defined for a tag. If, however, 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.

Access Extended Properties in Logic

You can access limits that are defined on tags by using the .@Min and .@Max syntax:

- You cannot write to extended properties values in logic.
- To use extended tag properties in an Add-On Instruction, you must pass them in as input operands to the Add-On Instruction.
- Alias tags that have extended properties cannot access the extended properties in logic.
- Limits can be configured for input and output parameters in Add-On Instructions. However, limits cannot be defined on an InOut parameter of an Add-On Instruction.
- Limits cannot be accessed inside Add-On Instruction logic. Limits are for use only by HMI applications.

If an array tag uses indirect addressing to access limits in logic, the following conditions apply:

- If the array tag has limits that are configured, the extended properties are applied to any array element that does not explicitly have that particular extended property configured. For example, if the array tag MyArray has max configured to 100, any element of the array that does not have Max configured inherits the value of 100 when being used in logic. However, it is not visible that the value inherited from MyArray is configured in the tag properties.
- At least one array element must have a limit that is configured for indirectly referenced array logic to verify. For example, if MyArray[x].@Max is being used in logic, at least one array element of MyArray[] must have Max extended property that is configured if MyArray has not configured Max.
- A data type default value is used under the following circumstances:
  - Array is accessed programmatically with indirect reference.
  - Array tag does not have the extended property configured.
  - A member of an array does not have the extended property configured.

  For example, for an array of SINT type, when max limit is called in logic for a member, use the value of 127.

If an array element is directly accessed, the element has to have the extended property defined. If not, verification fails.

Programming Languages

The Compact GuardLogix 5370 controller supports these programming languages, online and offline.

Language	Is best-used in programs with
Relay ladder	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 can have to interpret to troubleshoot the machine or process
Function block diagram[1]	Continuous process and drive control
	Loop control
	Calculations in circuit flow
Sequential function chart (SFC)[1]	High-level management of multiple operations
	Repetitive sequence of operations
	Batch process
	Motion control that uses structured text
	State machine operations
Structured text[1]	Complex mathematical operations
	Specialized array or table loop processing
	ASCII string handling or protocol processing

(1) Only with standard programs.

For information about programming in these languages, see the Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001.Add-On Instructions

Add-On Instructions

You can design and configure sets of commonly used instructions to increase project consistency. Similar to the built-in instructions 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 animating logic for one instance.
- Help protect intellectual property with Source Protection.
- 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.

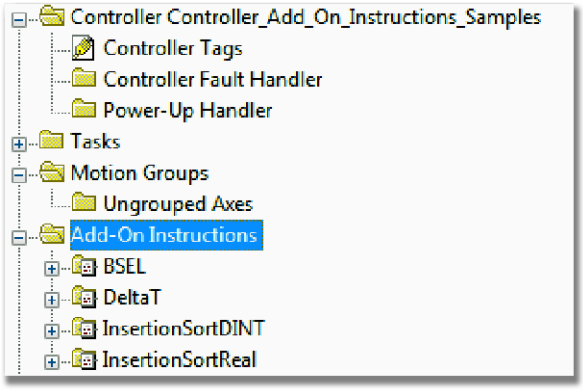
Add-On Instruction Capabilities and Advantages

Capability	Description
Save Time	With Add-On Instructions, you can combine your most commonly used logic into sets of reusable instructions. You save time when you create instructions for your projects and share them with others. Add-On Instructions increase project consistency because commonly used algorithms all work in the same manner, regardless of who implements the project.
Use Standard Editors	You create Add-On Instructions by using one of three editors: • Relay Ladder • Function Block Diagram(1) • Structured Text(1) Once you have created instructions, you can use them in any editor.
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 name so that you don't accidentally overwrite another instruction of the same name.
Use Context Views	Context views let you visualize the logic of an instruction for an instant, which simplifies online troubleshooting of your Add-On Instructions. Each instruction contains a revision, a change history, and an auto-generated help page.
Create Custom Help	When you create an instruction, you enter information for the description fields in dialogs, information that becomes what is known as Custom Help. Custom Help makes it easier for you to get the help you need when implementing the instructions.
Apply Source Protection	As the creator of Add-On Instructions, you can limit users of your instructions to read-only access, or you can bar access to the internal logic or local parameters that are used by the instructions. This source protection lets you stop unwanted changes to your instructions and protects your intellectual property.

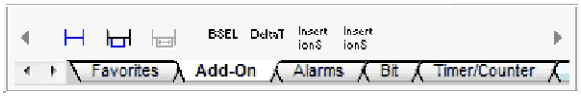
(1) Only with standard programs.

Once defined in a project, Add-On Instructions behave similarly to the built-in instructions in Logix 5000 controllers. They appear on the instruction toolbar for easy access, as do internal instructions.

Controller Organizer



Instruction Toolbar



Access the Module Object

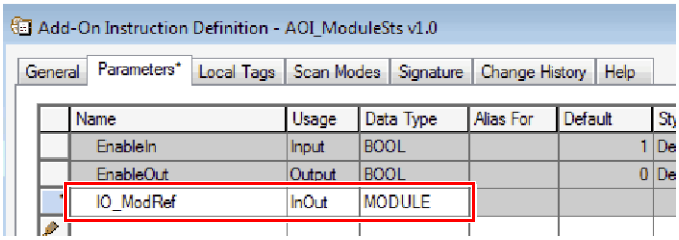
The MODULE object provides status information about a module. To select a particular module object, set the Object Name operand of the GSV/SSV instruction to the module name. The specified module must be present in the I/O Configuration section of the controller organizer and must have a device name.

Create the Add-On Instruction

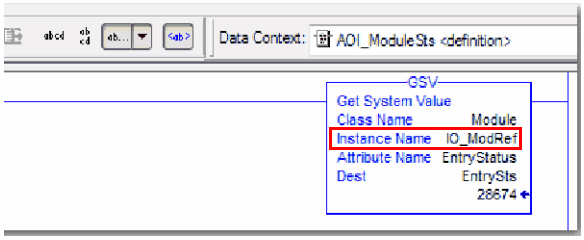
With Logix Designer application, you can access a MODULE object directly from an Add-On Instruction. Previously, you could access the MODULE object data but not from within an Add-On Instruction.

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

Add-On Instruction Logic



Program Logic



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

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

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

The Path attribute is available with Logix Designer application, which provides a communication path to the module.

For more information on the attributes available in the MODULE object, see the Logix Controllers Instructions Reference Manual, publication 1756-RM009.

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

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.

There are several objects and attributes that you can use the GSV and SSV instructions to monitor and set the system. For more information about GSV instructions, SSV instructions, objects, and attributes, see the Logix Controllers Instructions Reference Manual, publication 1756-RM009, and Use GSV/SSV Instructions on page 151.

System Overhead Time Slice

The Compact GuardLogix 5370 controller communicates with other devices at a specified rate (scheduled) or when there is processing time available to service the communication.

The system overhead time slice specifies the percentage of time a controller devotes to service communication. If you have a continuous task, the System Overhead Time Slice that is entered in the Advanced tab of the Controller Properties dialog box specifies continuous task/service communication ratio. However, if there is no continuous task, the overhead time slice has no effect.

Ratio between Continuous Task and Service Communication

At this time slice	The continuous task runs	Service communication occurs for up to
10%	9 ms	1 ms
20%	4 ms	1 ms
25%	3 ms	1 ms
33%	2 ms	1 ms
50%	1 ms	1 ms
66%	1 ms	2 ms
75%	1 ms	3 ms
80%	1 ms	4 ms
90%	1 ms	9 ms

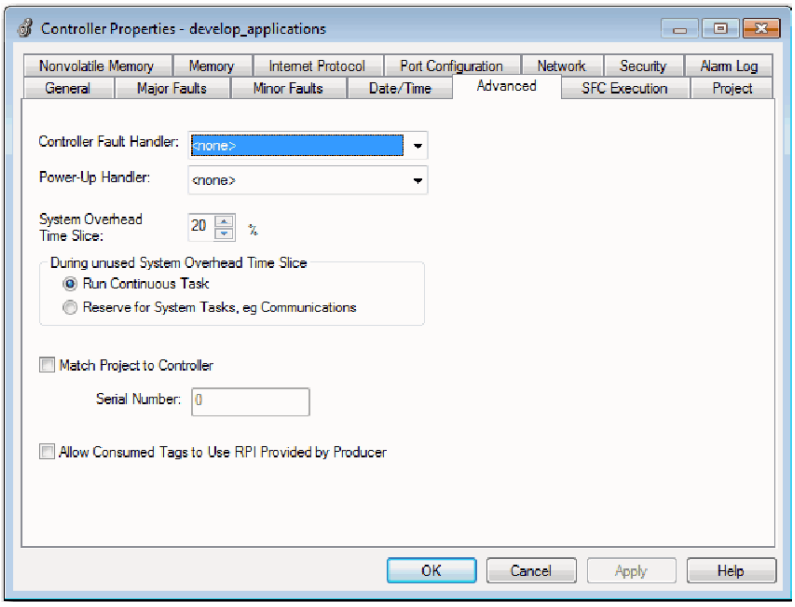
As shown in the previous table, if the system overhead time slice is less than or equal to 50%, the duration stays fixed at 1 ms. The same applies for 66% and higher, except there are multiple 1 ms intervals. For example, at 66% there are two 1 ms intervals of consecutive time and at 90% there are nine 1 ms intervals of consecutive time.

Configure the System Overhead Time Slice

To configure the system overhead time slice, perform this procedure.

1. In the Controller Organizer, right-click the controller and choose Properties.

   The Controller Properties dialog box appears.
2. Click the Advanced tab.
3. Enter a numeric value in the System Overhead Time Slice box.
4. Use Run Continuous Task (default) or Reserve for System Tasks.
   - Click Run Continue Task when there is no communication or background tasks to process; the controller immediately returns to the continuous task.
   - Click Reserve for System Task to allocate the entire 1 ms of the system overhead time slice whether the controller has communication or background tasks to perform before returning back to the continuous task. This lets you simulate a communication load on the controller during design and programming before HMIs, controller to controller messaging, and so forth, are configured.
5. Click OK.



Develop Safety Applications

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

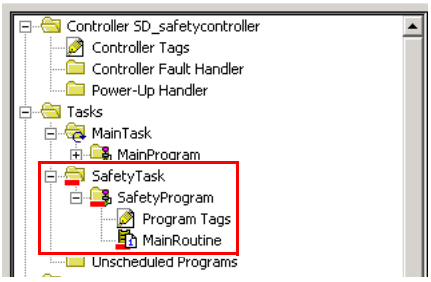
For guidelines and requirements to develop and commission SIL 3 and PLe safety applications, refer to the GuardLogix® 5570 and Compact GuardLogix® 5370 Controller Systems Safety Reference Manual, publication 1756-RM099.

The Safety Reference Manual addresses the following topics:

- Create a detailed project specification
- Write, document, and test the application
- Generate the safety task signature to identify and help protect the project
- Confirm the project by printing or displaying the uploaded project and manually compare the configurations, safety data, and safety program logic
- Verify the project through test cases, simulations, functional verification tests, and an independent safety review, if necessary
- Lock the safety application
- Calculate the system reaction time

The Safety Task

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

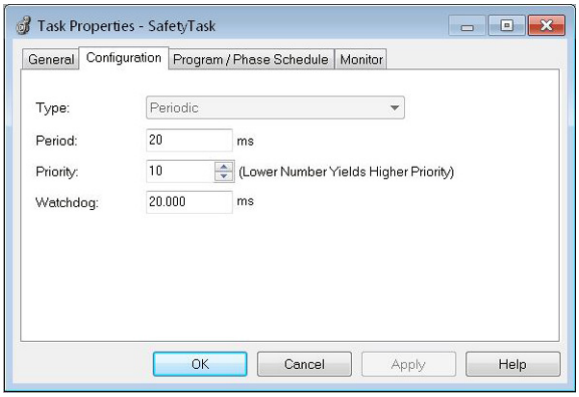


Within the safety task, you can use multiple safety programs, which are composed of multiple safety routines. The Compact GuardLogix controller supports one safety task. The safety task cannot be deleted.

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

Safety Task Period Specification

The safety task is a periodic timed task. To set the task priority and watchdog time, use the Task Properties - Safety Task dialog box. To open the dialog box, right-click the Safety Task and select Properties.



The safety task is a high priority. You specify the safety task period (in ms) and the safety task watchdog (in ms). The safety task period is the period that the safety task executes. The safety task watchdog is the maximum time that is 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 the 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.

The GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099, provides detailed information on system reaction time calculation.

Safety Task Execution

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

- The safety task does not begin executing until the primary controller and safety partner establish their control partnership. (Standard tasks begin executing as soon as the controller transitions to Run mode.)
- All safety input tags (inputs, consumed, and mapped) are updated and frozen at the beginning of safety task execution.

  See page Map Safety Tags on page 127 for more information.
- Safety output tag (output and produced) values are updated at the conclusion of safety task execution.

Safety Programs

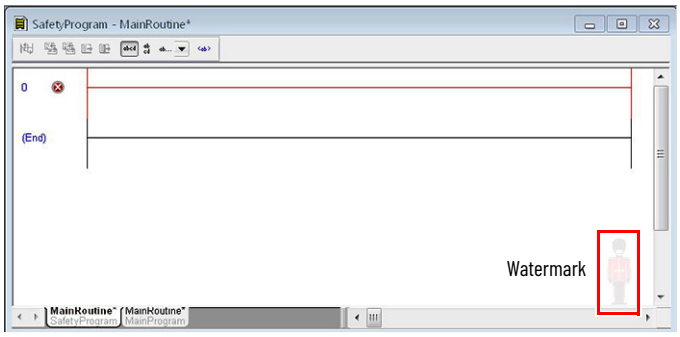
Safety programs have all the attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines. One safety routine must be designated as the main routine, and another safety routine can be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

Safety programs cannot contain standard routines or standard tags.

Safety Routines

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

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



Safety Tags

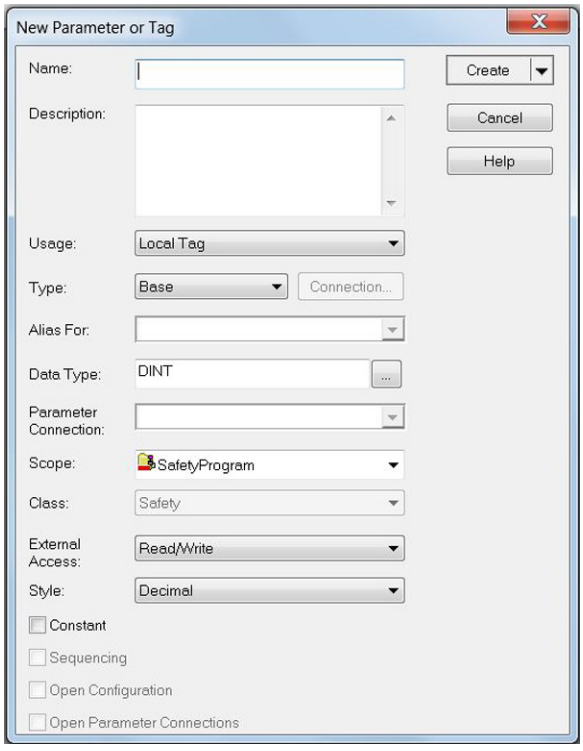
A tag is an area of a controller's memory where data is stored. Tags are the basic mechanism to allocate memory, reference data from logic, and monitor data. Safety tags have all the attributes of standard tags with the addition of mechanisms that are certified to provide SIL 3 data integrity.

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

- Name
- Description (optional)
- Tag type
- Data type
- Scope
- Class
- Style
- External Access

You can also specify if the tag value is a constant.

To create a safety tag, right-click Controller Tags or Program Tags to open the New Tag dialog box and choose New Tag.



Tag Type

This table defines the four types of tags.

Tag Type	Description
Base tag	These tags store values for use by logic within the project.
Alias tag	A tag that references another tag. An alias tag can refer to another alias tag or a base tag. An alias tag can also refer to a component of another tag by referencing a member of a structure, an array element, or a bit within a tag or member. **IMPORTANT:** Do not use alias tags between standard and safety tags in safety applications. Instead, standard tags can be mapped to safety tags. See Map Safety Tags on page 127.
Produced tag	A tag that a controller makes available for use by other controllers. A maximum of 15 controllers can simultaneously consume (receive) the data. A produced tag sends its data to one or more consuming tags without the use of logic. Produced tag data is sent at the RPI of the consuming tag.
Consumed tag	A tag that receives the data of a produced tag. The data type of the consumed tag must match the data type of the produced tag. The requested packet interval (RPI) of the consumed tag determines the period when the data updates.

Data Type

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, as user-defined data types.

Logix controllers contain predefined data types for use with specific instructions.

Valid Data Types for Safety Tags

AUX_VALVE_CONTROL	DCI_STOP_TEST_MUTE	MANUAL_VALVE_CONTROL
BOOL	DINT	MUTING_FOUR_SENSOR_BIDIR
CAM_PROFILE	DIVERSE_INPUT	MUTING_TWO_SENSOR_ASYM
CAMSHAFT_MONITOR	EIGHT_POS_MODE_SELECTOR	MUTING_TWO_SENSOR_SYM
CB_CONTINUOUS_MODE	EMERGENCY_STOP	MOTION_INSTRUCTION
CB_CRANKSHAFT_POS_MONITOR	ENABLE_PENDANT	PHASE
CB_INCH_MODE	EXT_ROUTINE_CONTROL	PHASE_INSTRUCTION
CB_SINGLE_STROKE_MODE	EXT_ROUTINE_PARAMETERS	REDUNDANT_INPUT
CONFIGURABLE_ROUT	FBD_BIT_FIELD_DISTRIBUTE	REDUNDANT_OUTPUT
CONNECTION_STATUS	FBD_CONVERT	SAFETY_MAT
CONTROL	FBD_COUNTER	SERIAL_PORT_CONTROL
COUNTER	FBD_LOGICAL	SFC_ACTION
DCA_INPUT	FBD_MASK_EQUAL	SFC_STEP
DCAF_INPUT	FBD_MASKED_MOVE	SFC_STOP
DCI_MONITOR	FBD_TIMER	SINT
DCI_START	FIVE_POS_MODE_SELECTOR	STRING
DCI_STOP	INT	THRS_ENHANCED
DCI_STOP_TEST	LIGHT_CURTAIN	TIMER
DCI_STOP_TEST_LOCK	MAIN_VALVE_CONTROL	TWO_HAND_RUN_STATION

Scope

A tag's scope 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 Tags

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

- Multiple programs in the project
- To produce or consume data
- To communicate with a PanelView™ terminal
- In safety tag mapping

  See Map Safety Tags on page 127 for more information.

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

IMPORTANT Controller-scoped safety tags are readable by any standard routine. The safety tag's update rate is based on the safety task period.

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.

For information on user-defined data type creation, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

Program-scoped Tags

When tags are program-scoped, the data is isolated from the other programs. Reuse of program-scoped tag names is permitted between programs.

Only a safety routine that is scoped in the same safety program can read or write to Safety-program-scoped safety tags.

Class

Tags can be classified as standard or safety. Tags classified as safety tags must have a data type that is permitted for safety tags.

When you create program-scoped tags, the class is automatically specified, depending upon whether the tag was created in a standard or safety program.

When you create controller-scoped tags, you must manually select the tag class.

Constant Value

Controller logic, or an external application such as an HMI, cannot modify a tag that is designated as a constant value. Constant value tags cannot be forced.

The Logix Designer application can modify constant standard tags, and safety tags provided a safety task signature is not present. Safety tags cannot be modified if a safety task signature is present.

External Access

External Access defines the level of access that is allowed for external devices, such as an HMI, to see or modify tag values. Access via the Logix Designer application is not affected by this setting. The default value is read/write.

External Access Setting	Description
None	Tags are not accessible from outside the controller.
Read Only	Tags can be browsed or read, but not written to from outside the controller.
Read/Write	Standard tags can be browsed, read, and written to from outside the controller.

For alias tags, the External Access type is equal to the type configured for the base target tag.

Produced/Consumed Safety Tags

To transfer safety data between Compact GuardLogix controllers, you use produced and consumed safety tags. Produced and consumed tags require connections. The default connection type for produced and consumed tags is unicast.

Produced and Consumed Connections

Tag	Connection Description
Produced	A Compact GuardLogix or Compact GuardLogix controller can produce (send) safety tags to other Compact GuardLogix or Compact GuardLogix controllers. The producing controller uses one connection for each consumer.
Consumed	Compact GuardLogix or Compact GuardLogix controllers can consume (receive) safety tags from other Compact GuardLogix or Compact GuardLogix controllers. Each consumed tag consumes one connection.

Produced and consumed safety tags are subject to the following restrictions:

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

To configure produced and consumed safety tags to properly 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 the next section.

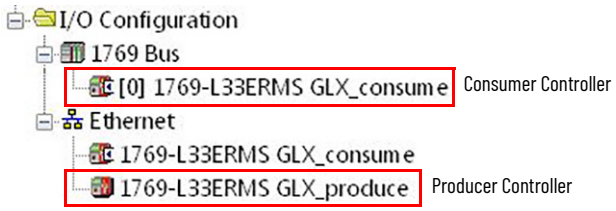
Configure the Peer Safety Controllers' Safety Network Numbers

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).

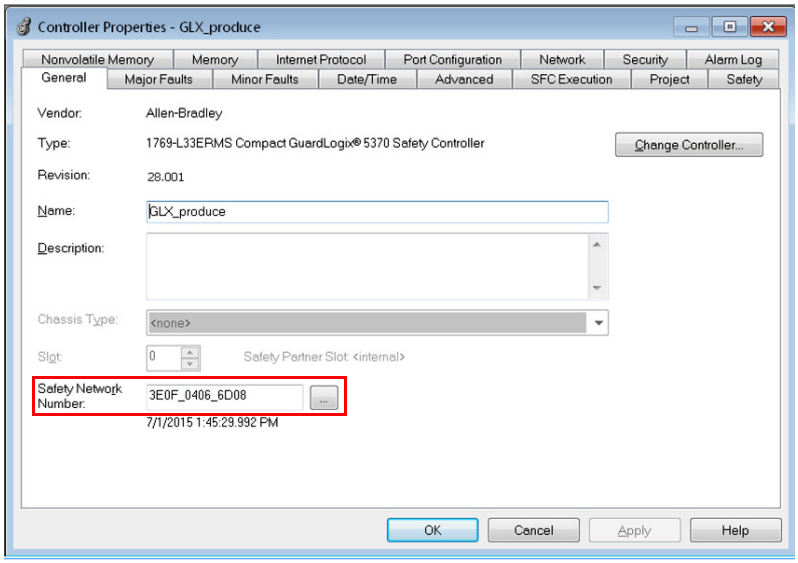
Follow these steps to copy and paste the SNN.

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

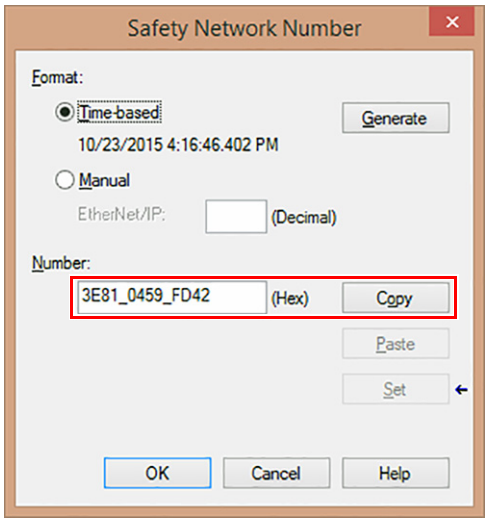
   The same producing controller must not appear more than once in your controller's I/O tree or a verification error occurs.



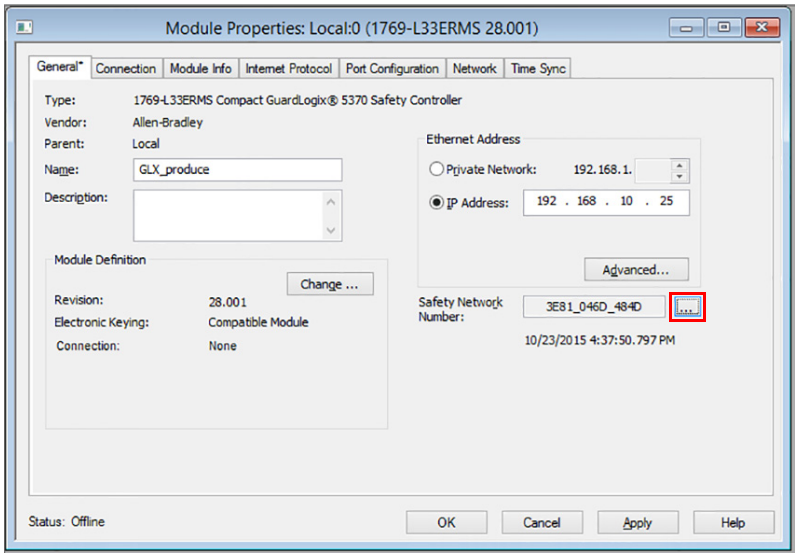
2. In the producer controller's project, right-click the producer controller and choose Controller Properties.
3. Click ... to open the Safety Network Number dialog box.



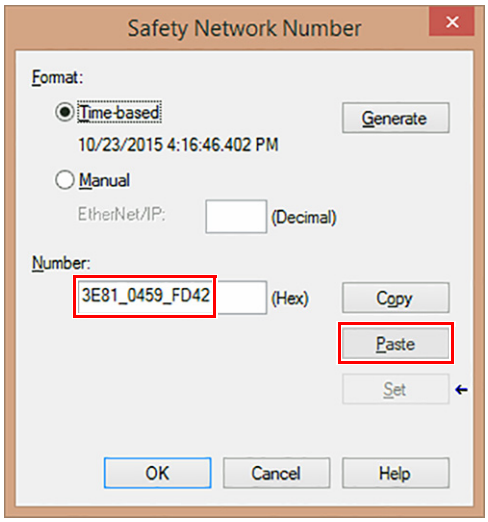
4. Click Copy to copy the producer controller's SNN.



5. In the consumer controller's project, right-click the producer controller and choose Module Properties.
6. Click ... to open the Safety Network Number dialog box.

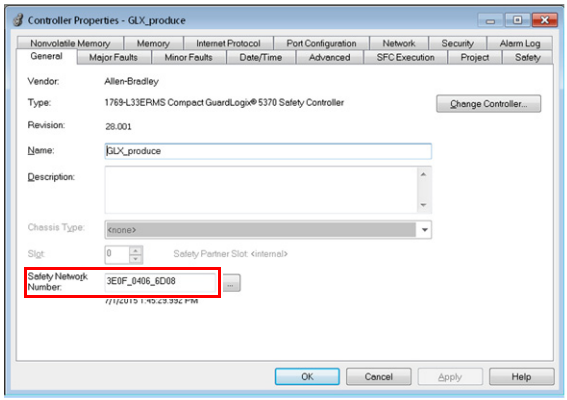


7. Paste the producer controller's SNN into the consumer controller's SNN field and click OK.

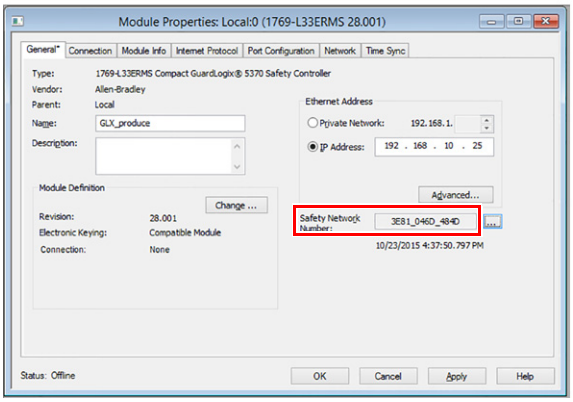


The safety network numbers match.

Producer Controller Properties Dialog Box in Producer Project



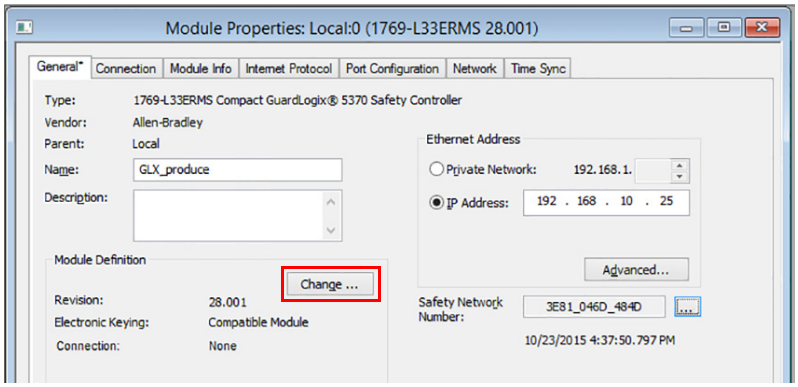
Module Properties Dialog Box in Consumer Project



Change the Electronic Keying

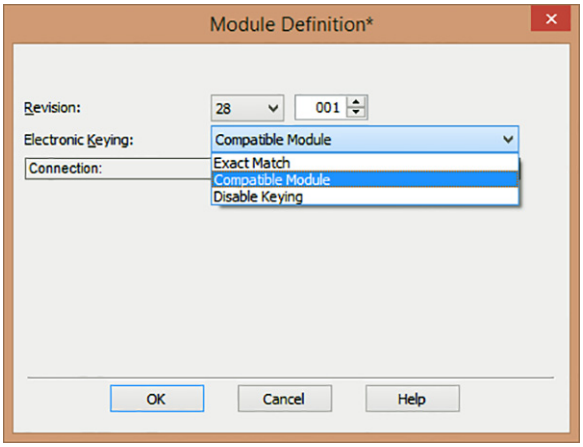
To change the electronic keying, follow these steps.

1. In the consumer controller's project, right-click the producer controller and choose Module Properties.
2. In the Module Definition field, click Change.



The Module Definition dialog box appears.

3. From the Electronic Keying pull-down menu, choose what is appropriate for your application.



IMPORTANT If safety tags are consumed, then you must choose either Exact Match or Compatible Module from the pull-down menu.
Choose Disable Keying only when standard tags are consumed.

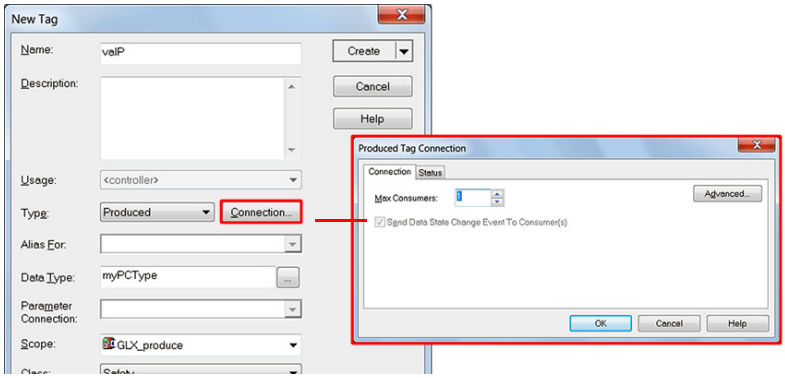
4. To save your changes and close the Module Definition dialog box, click OK.
5. To close the Modules Properties dialog box, click OK.

Produce a Safety Tag

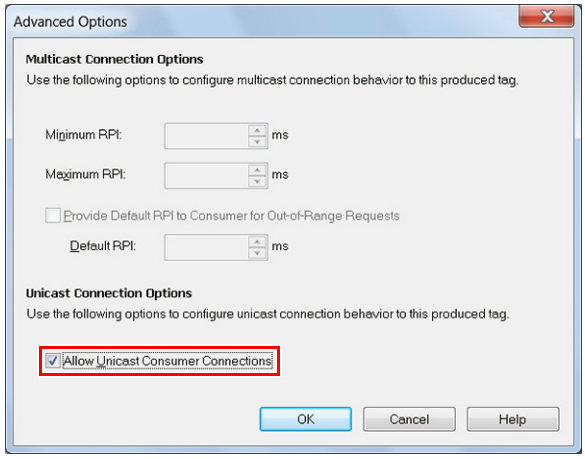
To produce a safety tag, follow this procedure.

1. In the controller project that produces tags, create a user-defined data type that defines the structure of the produced data.

   Make sure that the first data member is of the CONNECTION_STATUS data type.
2. Right-click Controller Tags and choose New Tag.
3. Set the type as Produced, the class as Safety, and the Data Type to the user-defined data type you created in step 1.
4. Click Connection and enter the number of consumers.



5. To change the type of connection, click Advanced and then clear the Allow Unicast Consumer Connections checkbox.



6. Click OK.

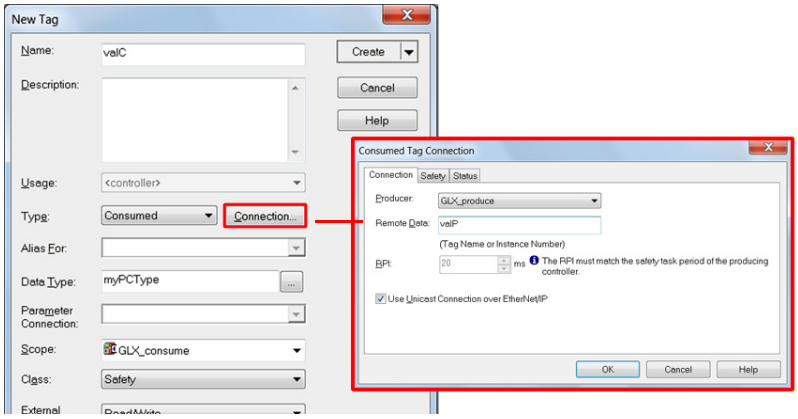
Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

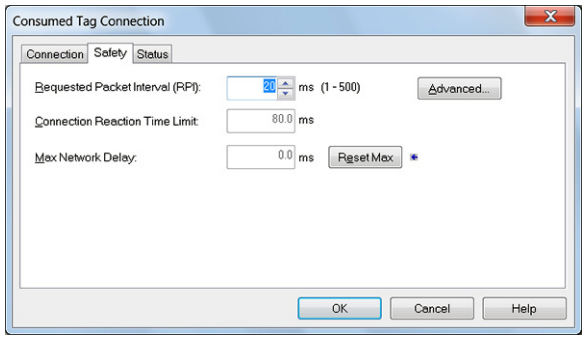
1. In the consumer controller's project, create a user-defined data type identical to the one created in the producer project.

   The 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.



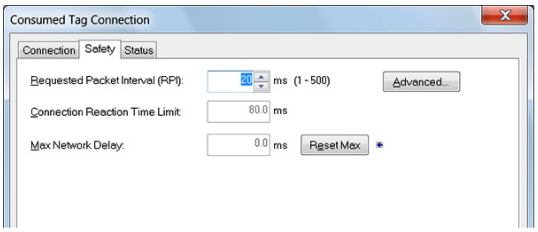
5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.
7. Click the Safety tab.



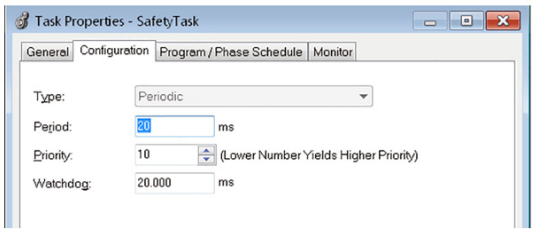
8. In the Requested Packet Interval (RPI) field, enter the RPI for the connection in 1 ms increments. The default is 20 ms.

   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's Project



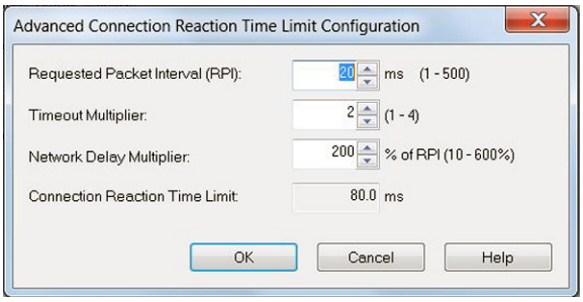
Producer's Project



   The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, you can achieve an acceptable Connection Reaction Time Limit by adjusting the 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. to To reset the Max Network Delay, click Reset Max when the program is online.

9. If the Connection Reaction time limit is acceptable, click OK; or for more complex requirements, click Advanced to set 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 the CIP Safety protocol enforces. 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.

For information on setting the RPI and to understand how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time see Estimate Requested Packet Interval on page 66 and Module Fault Related to RPI Estimates on page 67.

For detailed information on how to use produced and consumed tags, see the Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011.

Map Safety Tags

Controller-scoped standard tags cannot be accessed directly through a safety routine. To allow standard tag data to be used within safety task routines, the Compact GuardLogix controllers provide a feature that maps safety tags, which allows you to copy standard tag values into safety task memory.

Restrictions

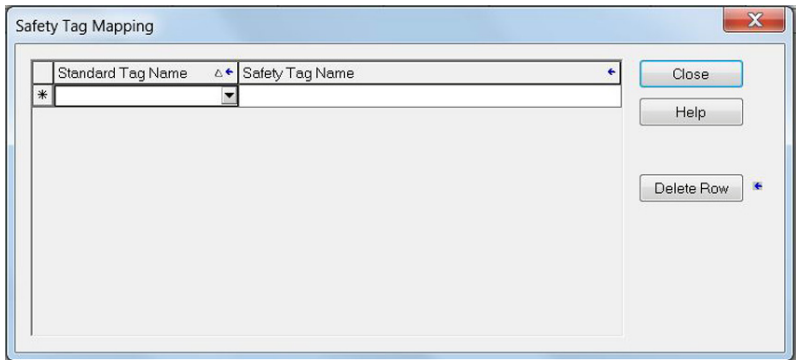
These restrictions apply when you map Safety tags:

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

ATTENTION: When you use standard data in a safety routine, you must verify that the data is used in an appropriate manner. The use of standard data in a safety tag does not make it safety data. You must not directly control a SIL 3/PLe safety output with standard tag data. See the GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099, for more information.

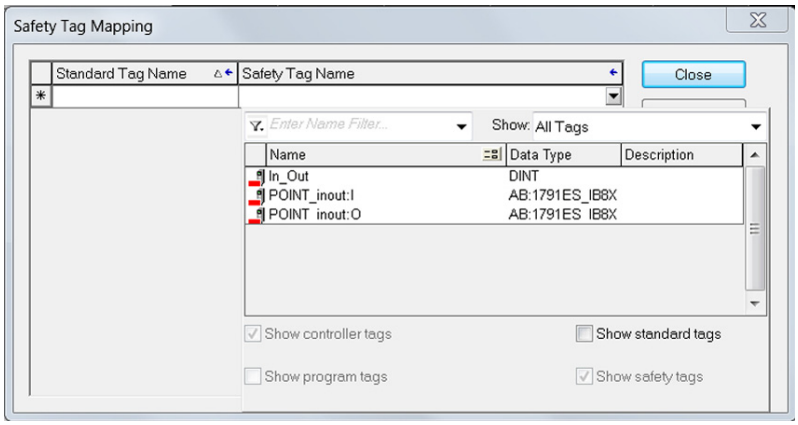
Create Tag Mapping Pairs

1. Choose Map Safety Tags from the Logic menu to open the Safety Tag Mapping dialog box.



2. Type the tag name into the cell or choose a tag from the pull-down menu to add an existing tag to the Standard Tag Name or Safety Tag Name column.

   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, right-click in the empty cell, select New Tag and 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.

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 that explains 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 127.

Safety Application Protection

To help protect your application program from unauthorized changes, you can safety-lock the controller, and generate and record the safety task signature.

Safety-lock the Controller

The Compact Compact GuardLogix controller can be safety-locked to help protect safety-related control components from modification. 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 task signature.

The following actions are not permitted in the safety portion of the application when the controller is safety-locked:

- Program or edit online/offline (including safety Add-On Instructions)
- Force safety I/O
- Change the inhibit state of safety I/O or produced connections
- Safety data manipulation (except by safety routine logic)
- Generate or delete the safety task signature

The text of the online bar's safety status button indicates the safety-lock status.

Safety Status Button

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

- = controller safety-locked
- = controller safety-unlocked

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

Safety-locked or -unlocked status cannot be changed when the keyswitch is in the RUN position.

Safety-lock or -unlock actions are logged in the controller log.
For more information on how to access the controller log, refer to Logix 5000 Controllers Information and Status Programming Manual, publication 1756-PM015.

To safety-lock and -unlock the controller, use the Safety tab of the Controller Properties dialog box, or 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.

You can also set or change the password from the Safety Lock dialog box. See Set Passwords for Safety-lock and -unlock on page 40.

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.

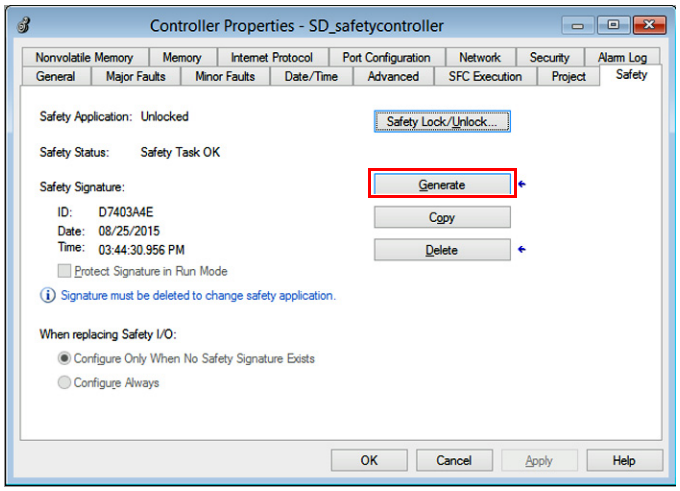
Generate a Safety Task Signature

Before you test for verification, you must generate the safety task signature. You can generate the safety task signature only when online with the safety-unlocked Compact GuardLogix controller in Program mode, and with no safety forces, pending online safety edits, or safety faults. The safety status must be Safety Task OK.

In addition, you cannot generate a safety task signature if the controller is in Run mode with run mode protection enabled.

You can view the safety status via the safety status button on the online bar (see page 129) or on the Safety tab of the Controller Properties dialog box, as shown in the following figure.

To generate the safety task signature, click Generate on the Safety tab of the Controller Properties dialog box. You can also select Tools>Safety>Generate Signature.



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

Safety task signature creation and deletion are logged in the controller log. For more information on how to access the controller log, refer to Logix 5000 Controllers Information and Status Programming Manual, publication 1756-PM015.

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

- Program or edit online/offline (including safety Add-On Instructions)
- Force safety I/O
- Change the inhibit state of safety I/O or producer controllers
- Safety data manipulation (except by safety routine logic)

Copy the Safety Task Signature

You can use the Copy button to create a record of the safety task 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 Task Signature

Click Delete to delete the safety task signature. The safety task signature cannot be deleted when the following is true:

- The controller is safety-locked.
- The controller is in Run mode with the keyswitch in RUN.
- The controller is in Run or Remote Run mode with run mode protection enabled.

ATTENTION: If you delete the safety task signature, you must retest and revalidate your system to meet SIL 3/PLe.
See the GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099, for more information on SIL 3/PLe requirements.

Programming Restrictions

The Logix Designer application imposes restrictions that limit the availability of some menu items and features (that is, cut, paste, delete, search, and replace) to help the modification of protect safety components whenever the following is true:

- The controller is safety-locked.
- A safety task signature exists.
- Safety faults are present.
- Safety status is as follows:
  - Partner missing
  - Partner unavailable
  - Hardware incompatible
  - Firmware incompatible

If even one of the previous 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.

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

- 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.
- Modify or delete the safety task signature, when safety-locked.

Develop Integrated Motion over an EtherNet/IP Network Application

Compact GuardLogix® 5370 controllers support Integrated Motion over an EtherNet/IP network.

Integrated Motion on EtherNet/IP™ applications uses the following:

- Standard EtherNet/IP network
- High-performance drives, which include the following:
  - Kinetix® 350 drives
  - Kinetix 5500 and Kinetix 5700 drives
  - Kinetix 6500 drives
  - PowerFlex® 527 drives
  - PowerFlex 755 drives
- Standard infrastructure components
- Programming software

In addition, Kinetix 5500(1), Kinetix 5700, and PowerFlex 527 drives support integrated Safe Torque Off (STO) via a single safety and motion connection to a Compact GuardLogix 5370 safety controller. The Compact GuardLogix controller issues the STO command over the EtherNet/IP network via CIP Safety™ and the safety drive executes the command.

To configure drives that use Integrated Motion over an EtherNet/IP network, see the drive user manuals that are listed in the Additional Resources on page 10 and the Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003.

(1) Applies only to Kinetix 5500 drives with -ERS2 catalog numbers.

Motion Axes Support

The 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS, 1769-L37ERMS, 1769-L38ERMOS, and 1769-L38ERMS controllers support these axes:

- AXIS_VIRTUAL
- AXIS_CIP_DRIVE

AXIS_VIRTUAL Axis

The AXIS_VIRTUAL axis is an internal axis representation that is not associated with any physical drives. That is, you can configure the axis but it does not cause any physical motion in your system.

AXIS_CIP_DRIVE Axis

The AXIS_CIP_DRIVE axis is a motion axis that is used with physical drives to cause physical motion in your system as determined by your application.

Configuration Types

When adding an axis to your project, you must associate the axis to a drive. Among other configuration parameters, you must select a configuration type. The axis configuration type is also considered the drive configuration type.

For example, an AXIS_CIP_DRIVE axis can use a Position Loop configuration and be associated with a Kinetix 350 drive. The axis is considered a Position Loop-configured axis and the associated drive is considered a Position Loop-configured drive.

The following drives support these configuration types:

- Kinetix 350, Kinetix 5500, Kinetix 5700, and Kinetix 6500 drives
  - Position loop
  - Velocity loop
  - Torque loop
- PowerFlex 527 and PowerFlex 755 drives
  - Position loop
  - Velocity loop
  - Torque loop
  - Frequency control

Maximum Number of Position Loop-configured Drives

Any device added to the local Ethernet node in the I/O configuration is counted toward the node limitation of the controller. For more information, see Nodes on EtherNet/IP Network on page 52.

Drives are counted among the number of nodes in the I/O Configuration section of the Logix Designer application. If you use the maximum number of drives that a Compact GuardLogix 5370 controller supports in one system, you cannot add other EtherNet/IP devices to that project.

Position Loop-configured Drive Limits

Among the maximum number drives supported by the controllers, there is a maximum number of Position Loop-configured drives that are supported in the project for the controller.

For example, the 1769-L30ERMS controller supports a maximum of four Position Loop-configured drives.

Compact GuardLogix 5370 Controllers Supporting Integrated Motion on the EtherNet/IP Network

Controller Type	Number of Drives Supported, Max	Number of Position Loop-configured Drives Supported, Max
1769-L30ERMS	16	4
1769-L33ERMS 1769-L33ERMOS	32	8
1769-L36ERMS 1769-L36ERMOS 1769-L37ERMS 1769-L37ERMOS(1) 1769-L38ERMS 1769-L38ERMOS(1)	48	16

(1) Available at firmware revision 31.

If your solution requires more than 16 Position Loop-configured drives, consider using the ControlLogix® platform. The ControlLogix platform enables up to 100 Position Loop-configured drives.

Time Synchronization

Integrated motion over an EtherNet/IP network requires time synchronization, also known as CIP Sync™. CIP Sync provides accurate real-time (real-world time) or Coordinated Universal Time (UTC) synchronization of Compact GuardLogix 5370 controllers and devices that are connected over an EtherNet/IP network.

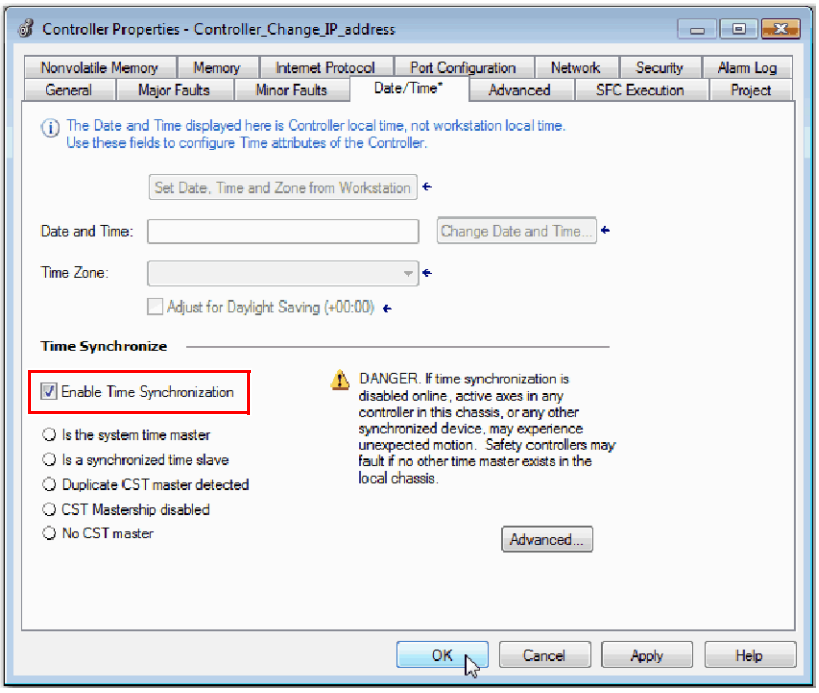
CIP Sync is a time synchronization protocol that can be applied to various applications. This chapter focuses on the use of this protocol in applications with Integrated Motion over an EtherNet/IP network.

All controllers and communication modules must have time synchronization enabled to participate in CIP Sync.

CIP Sync requires that devices in the system function in the following roles:

- Coordinated system time (CST) leader - Sets time for the entire system and passes the time to a leader
- Leader - Sets time for its backplane
- Follower - Uses time set by Leader

You can enable time synchronization on the Date/Time tab of the Controller Properties dialog box.



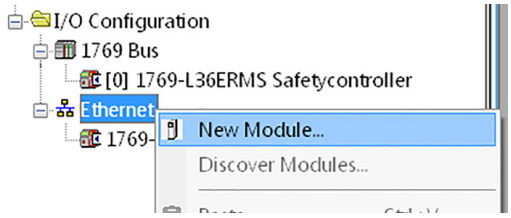
Configure Integrated Motion on the EtherNet/IP Network

To add a drive to your project for integrated motion on the EtherNet/IP network, complete these steps.

IMPORTANT These steps show a 1769-L36ERMS controller and a Kinetix 350 drive. The same steps apply to other Compact GuardLogix 5370 controllers and other drives that support integrated motion on an EtherNet/IP network.

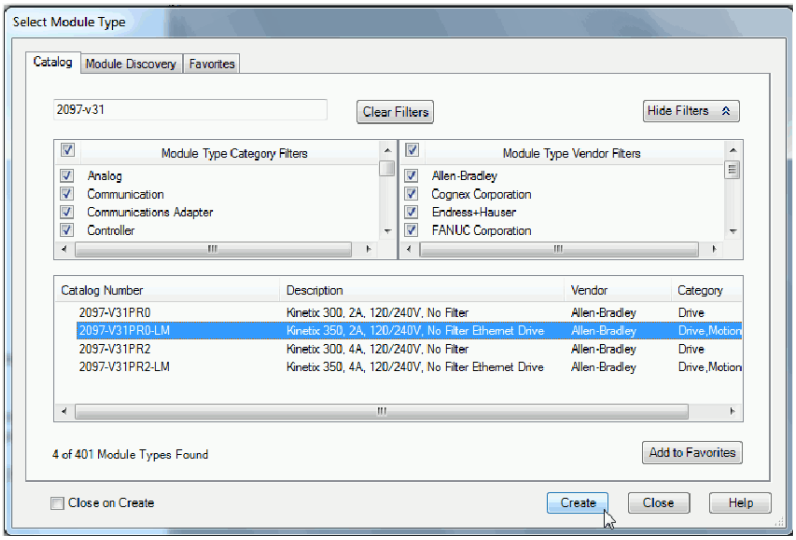
IMPORTANT This section assumes that you have previously created a project for your 1769-L36ERMS controller and enabled time synchronization on the controller. If you have not, do so before continuing.

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



   The Select Module Type dialog box appears.

2. Select the desired drive and click Create.

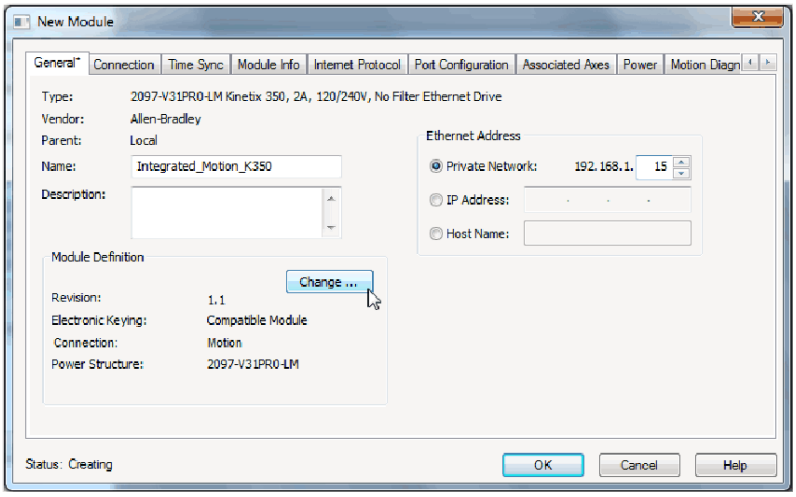


   The New Module dialog box appears.

3. Type a name for the module.
4. Type a description, if desired.
5. Assign an EtherNet/IP address.

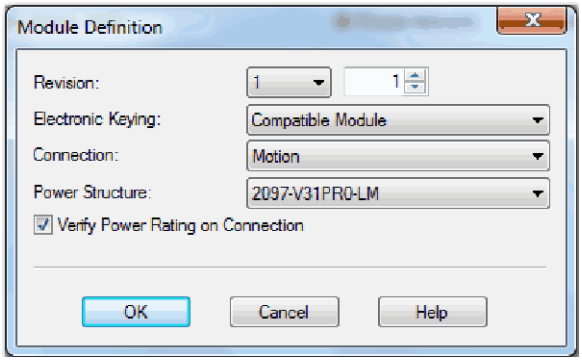
   For information on setting the IP addresses, see the publications for each drive type that is listed in Additional Resources on page 10.

6. To change the configuration for any of the following parameters, click Change.
   - Revision
   - Electronic Keying
   - Connection - For drives that support safety and motion on a single connection, you can choose Motion Only, Motion and Safety, or Safety Only.
   - Power Structure
   - Verify Power Rating on Connection



The Module dialog box appears.

7. Make the desired changes and click OK.



8. To create the drive in your project, click OK.
9. Add other components that your project requires.

Go Online with the Controller

Considerations

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

A number of factors affect these processes, including the Project to Controller Match feature, the safety status and faults, the existence of a safety task signature, and the safety-lock/-unlock status of the project and the controller.

Project to Controller Match

The Project to Controller Match feature affects the download, upload, and go online processes of standard and safety projects.

If the Project to Controller Match feature is enabled in the offline project, the programming software 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, which updates the serial number in the project to match the target controller.

Firmware Revision Match

Firmware revision match 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 if the controller is safety-unlocked.

IMPORTANT To update the firmware of the controller, first install a firmware update kit. An upgrade kit ships on a supplemental CD along with the Logix Designer application.

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

Safety Status/Faults

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

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

Safety Task Signature and Safety-locked and -unlocked Status

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

On Upload

If the controller has a safety task signature, the safety task signature and the safety task 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 task signature in the offline project matches the controller's safety task signature.

On Download

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

Effect of Safety-lock and Safety Task Signature on Download Operation

Safety-lock Status	Safety Task Signature Status	Download Functionality
Controller safety-unlocked	Safety task signature in the offline project matches the safety task signature in the controller.	All standard project components are downloaded. Safety tags are reinitialized to the values that they had when the safety task signature was created. The safety task is not downloaded. Safety-lock status matches the status in the offline project.
	Safety task signatures do not match.	If the controller had a safety task 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 task signatures match.	If the offline project and the controller are safety-locked, all standard project components are downloaded and the safety task is re initialized to the values they had when the safety task 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 task signatures do not match.	You must first safety-unlock the controller to allow the download to proceed. If the controller had a safety task signature, it is automatically deleted, and the entire project is downloaded. Safety-lock status matches the status in the offline project.

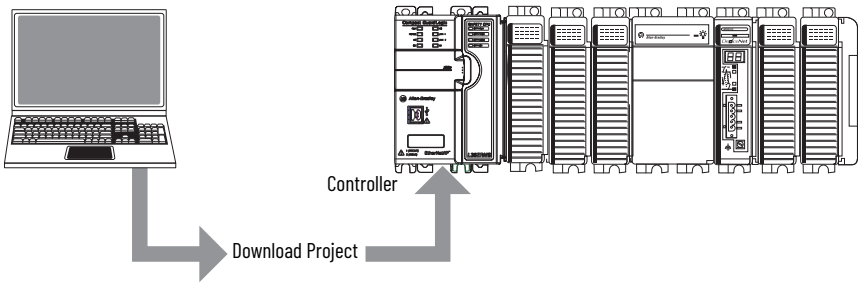
IMPORTANT During a download to a controller that is safety-unlocked, if the firmware in the controller is different than in the offline project, do one of the following:

- Update the controller so that it matches the offline project. Once the update is completed, the entire project is downloaded.
- Update the project to the controller version.

If you update the project, the safety task signature is deleted, and the system requires revalidation.

Download

Follow these steps to transfer your project from your computer to your controller.



1. Turn the keyswitch of the controller to REM.
2. Open the controller project that you want to download.
3. Define the path to the controller.
   a. Click Who Active .
   b. Select the controller.
      To open a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
4. Click Download.
   The software 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 task signature (if one exists)
   - Safety-lock status

5. To complete the download based on the software's response, follow the directions in this table.

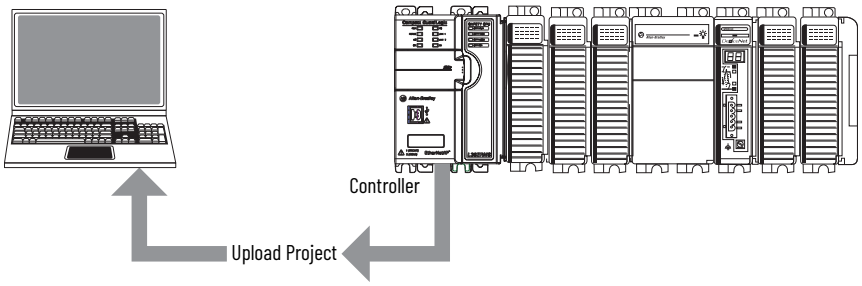
If the software indicates	Then
Download to the controller.	Choose Download. The project downloads to the controller and the Logix Designer application goes online.
Unable to download to the controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller or verify that this is the correct controller. If it is the correct controller, 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.
Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible.	Choose Update Firmware(1). Choose the required revision and click Update. Confirm your selection by clicking Yes.
Unable to download to controller. The internal safety partner hardware has failed.	Replace the controller.
Unable to download to the controller. The firmware update of the controller is incomplete.	Choose Update Firmware(1). Choose the required revision and click Update. Confirm your selection by clicking Yes.
Unable to download to controller. Safety partnership has not been established.	Cancel this download process and attempt a new download.
Unable to download to controller. Incompatible safety task 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 task signature, and download the project. **IMPORTANT:** The safety system requires revalidation.
Cannot download in a manner that preserves the safety task signature. Controller's firmware minor revision is not compatible with safety task signature in offline project.	• If the firmware minor revision is incompatible, to preserve the safety task signature, update the firmware revision in the controller to match the offline project exactly. Then download the offline project. • To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to download to controller. Controller is locked. Controller and offline project safety task 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, you must confirm the deletion by selecting Yes.
A nonrecoverable safety fault will occur in the safety controller. No designated coordinated system time (CST) leader exists.	Check Enable Time Synchronization and click Download to proceed.

(1) The controller must be safety-unlocked.

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

Upload

Follow these steps to transfer a project from the controller to your computer.



1. Define the path to the controller.
   a. Click Who Active .
   b. Select the controller.
   To expand a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
2. Click Upload.
3. If the project file does not exist, select File>Select>Yes.
4. If the project file exists, select it.

   If the project to controller match is enabled, the programming software checks whether the serial number of the open project and the serial number of the controller match.

   If the controller serial numbers do not match, you can do one of the following:

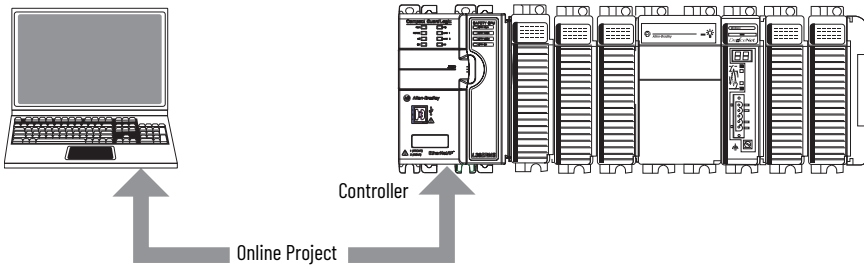
   - Cancel the upload and connect to a matching controller. Then, start the upload procedure again.
   - Select a new project to upload into or select another project by choosing Select File.
   - To update the project serial number so it matches the controller, select the Update Project Serial Number checkbox and choose Upload.
5. The software checks whether the open project matches the controller project.
   a. If the projects do not match, you must select a matching file or cancel the upload process.
   b. If the projects match, the software checks for changes in the offline (open) project.
6. The software checks for changes in the offline project.
   a. If there are no changes in the offline project, you can go online without uploading. Click Go Online.
   b. 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.

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

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

Go Online

Follow these steps to go online to monitor a project that the controller is executing.



1. Define the path to the controller.
   a. Click Who Active  .
   b. Select the controller.
   To expand a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
2. Click Go Online.
   The software 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 task signatures?
3. To connect to the controller, use the directions in the following table.

If the software indicates	Then
Unable to connect to controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller, select another project file, or choose the Update project serial number checkbox and choose Go Online... to connect to the controller and update the offline project serial number to match the controller.
Unable to connect to controller. The revision of the offline project and the controller's firmware are not compatible.	Choose one of the following options: • Choose Update Firmware. Choose the required revision and click Update. Confirm your selection by clicking Yes. **IMPORTANT:** The online project is deleted. • To preserve the online project, cancel the online process and install a version of the Logix Designer application that is compatible with the firmware revision of your controller.
You need to upload or download to go online by using the open project.	Choose one of the following options: • Upload to update the offline project. • Download to update the controller project. • Choose File to select another offline project.
Unable to connect in a manner that preserves safety task signature. Controller's firmware minor revision is not compatible with safety task signature in offline project.	• To preserve the safety task signature when the firmware minor revision is incompatible, update the firmware revision in the controller to match the offline project exactly. Then go online to the controller. • To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to connect to controller. Incompatible safety task 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 programming software are online, the safety-locked status and safety task signature of the controller match the controller's project. The controller overrides the safety-lock status and safety task signature of the offline project. 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.

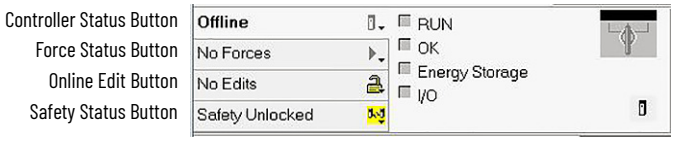
Monitor Status and Handle Faults

See Status Indicators on page 163 for information on the controller's status indicators.

View Status via the Online Bar

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

Status Buttons



When the Controller Status button is selected as shown in the previous graphic, the online bar shows the controller's mode (RUN) and status (OK). The I/O indicator combines the status of standard and safety I/O and behaves just like the status indicator on the controller. The I/O with the most significant error status is displayed next to the status indicator.

When the Safety Status button is selected, as shown in the following graphic, the online bar displays the safety task signature.

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.

If the safety status is	This icon is displayed
Safety Task OK	
Safety Task Inoperable	
Safety Unavailable	
Offline	

Icons are green when the controller is safety-locked, yellow when the controller is safety-unlocked, and red when the controller has a safety fault. When a safety task signature exists, the icon includes a small check mark.

Monitor Connections

You can monitor the status of standard and safety connections.

All Connections

If communication with a device in the I/O configuration of the controller does not occur for 100 ms, communication times out and the controller produces the following warnings:

- An I/O fault status code is indicated on the status display of the Compact GuardLogix® 5370 controller.
- The I/O indicator on the front of the controller flashes green.
- An alert symbol ⚠ shows over the I/O configuration folder and over the device that has timed out.
- A module fault is produced, which you can access through the Connections tab of the Module Properties dialog box for the module or via the GSV instruction.

ATTENTION: Safety I/O and produce/consume connections cannot be configured to automatically fault the controller when a connection is lost. Therefore, you must monitor for connection faults to be sure that the safety system maintains SIL 3/PLe integrity.
See Safety Connections on page 147.

Safety Connections

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

The RunMode value indicates if a device that is in the Run Mode (1) or Idle State (0) actively updates the consumed data. 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.

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) as a result of a loss of the physical connection, the safety data is reset to zero.

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

Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	The producing device controls the data actively. The producing device is in Run mode.
0 = Idle	0 = Valid	The connection is active and the producing device is in the Idle state. The safety data is reset to zero.
0 = Idle	1 = Faulted	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero.
1 = Run	1 = Faulted	Invalid state.

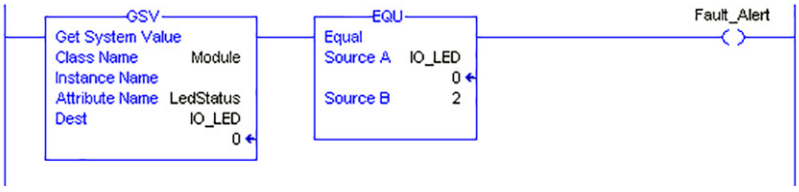
If a module is inhibited, the ConnectionFaulted bit is set to Faulted (1) and the RunMode bit is set to Idle (0) for each connection associated with the module. As a result, safety consumed data is reset to zero.

Determine if I/O Communication has Timed Out

This example can be used with the Compact GuardLogix 5370 controllers:

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

GSV Used to Identify I/O Timeout



For more information about attributes available with the Module object, see the Logix Controllers Instructions Reference Manual, publication 1756-RM009.

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. Use the GSV instructions to get fault code and information via the FaultCode and FaultInfo attributes of the Module object.

For more information about attributes available with the Module object, see the Logix Controllers Instructions Reference Manual, publication 1756-RM009.

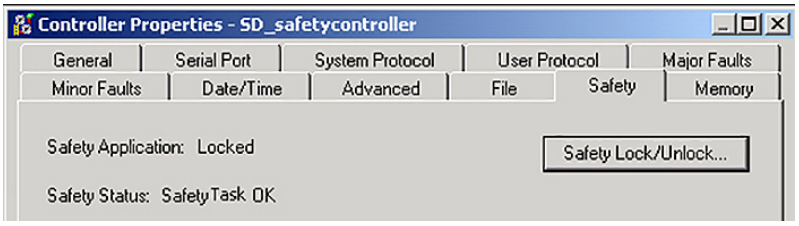
Monitor Status Flags

Logix controllers, including Compact GuardLogix controllers, support status keywords that you can use in your logic to monitor certain events.

For more information on how to use these keywords, refer to the Logix 5000™ Controllers Information and Status Programming Manual, publication 1756-PM015.

Monitor Safety Status

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.



The following are the possible values for safety status:

- Safety partner is unavailable
- Safety firmware is incompatible
- 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 150 for fault codes and corrective actions.

Controller Faults

Faults in the Compact GuardLogix system can be nonrecoverable controller faults, nonrecoverable safety faults in the safety application, or recoverable safety faults in the safety application.

Nonrecoverable Controller Faults

These faults occur when the controller's internal diagnostics fail. If a nonrecoverable controller fault occurs, safety task execution stops and CIP Safety™ I/O modules are placed in the safe state. Recovery requires that you download the application program again.

Nonrecoverable Safety Faults in the Safety Application

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

When the safety task encounters a nonrecoverable safety fault that is cleared programmatically in the Controller Fault Handler, the standard application continues to execute.

ATTENTION: If you override the safety fault, the fault IS NOT cleared and it is your responsibility to prove that safe operation is maintained.
You must provide proof to your certifying agency that allowing a portion of the system to continue to operate maintains safe operation.

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

Recoverable Faults in the Safety Application

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

When a recoverable fault is cleared programmatically, the safety task is allowed to continue 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 also commands the consumers to place them in a safe state.

Recoverable faults let you edit the standard and safety application as required to correct the cause of the fault. However, if a safety task signature exists or the controller is safety-locked, you must first unlock the controller and delete the safety task signature before you can edit the safety application.

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.

Fault Codes

The following table shows the fault codes specific to Compact GuardLogix 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.

Major Safety Faults (Type 14)

Code	Cause	Status	Corrective Action
01	Task watchdog expired. User task has not completed in a specified period of time. A program error caused an infinite loop, the program is too complex to execute as quickly as specified, a higher priority task is keeping this task from finishing.	Nonrecoverable	Clear the fault. If a safety task signature exists, safety memory is reinitialized and the safety task begins executing. If a safety task signature does not exist, you must redownload the program to allow the safety task to 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, for example, a watchdog timeout occurred or memory is corrupt.	Nonrecoverable	Clear the fault. If a safety task signature exists, safety memory is reinitialized via the safety task signature and the safety task begins executing. If a safety task signature does not exist, you must download the program again to allow the safety task to run.
08	Coordinated system time (CST) not found.	Nonrecoverable	Clear the fault. Configure a device to be the CST leader.

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

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.

Depending on your application, you may not want all safety faults to shut down your entire system. In those situations, you can 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 allowing a portion of the system to continue to operate maintains safe operation.

The controller supports two levels for handling major faults:

- Program Fault Routine
- Controller Fault Handler

Both routines can use the GSV and SSV instructions as described on page 151.

Program Fault Routine

Each program can have its own fault routine. The controller executes the program's fault routine when an instruction fault occurs. If the program's fault routine does not clear the fault, or if a program fault routine does not exist, the controller proceeds to execute the controller fault handler, if one exists.

Controller Fault Handler

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

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

For details on how to create and test a fault routine, see the Logix 5000 Controllers Major and Minor Faults Programming Manual, publication 1756-PM014.

Use GSV/SSV Instructions

Logix controllers store system data in objects rather than in status files. You can use the Get System Value (GSV) and Set System Value (SSV) instructions to retrieve and set controller data.

The GSV instruction retrieves the specified information and places it in the specified destination. The SSV instruction changes the specified attribute with data from the source of the instruction. When you enter a GSV or SSV instruction, the programming software displays the object classes, object names, and attribute names for each instruction.

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 those attributes you are allowed to 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 module.

For safety objects, the following table shows attributes for which you can get values by using the GSV instruction, and which attributes you are allowed to set by using the SSV instruction, in the safety and standard tasks.

ATTENTION: Use the GSV/SSV instructions carefully. Changes made to objects can cause unexpected controller operation or injury to personnel.

GSV/SSV Accessibility

Safety Object	Attribute Name	Data Type	Attribute Description	Accessible from the Safety Task		Accessible from Standard Tasks	
				GSV	SSV	GSV(4)	SSV
Safety Task	Instance	DINT	Provides the instance number of this task object. Valid values are 0...31.	X		X	
	MaximumInterval	DINT[2]	The max time interval between successive executions of this task.			X	X
	MaximumScanTime	DINT	Max recorded execution time (ms) for this task.			X	X
	MinimumInterval	DINT[2]	The min time interval between successive executions of this task.			X	X
	Priority	INT	Relative priority of this task as compared to other tasks. Valid values are 0...15.	X		X	
	Rate	DINT	Period for the task (in ms), or timeout value for the task (in ms).	X		X	
	Watchdog	DINT	Time limit (in ms) for execution of all programs associated with this task.	X		X	
Safety Program	Instance	DINT	Provides the instance number of the program object.	X		X	
	MajorFaultRecord(1)	DINT[11]	Records major faults for this program.	X	X	X	
	MaximumScanTime	DINT	Max recorded execution time (ms) for this program.			X	X
Safety Routine	Instance	DINT	Provides the instance number for this routine object. Valid values are 0...65,535.	X			
Safety Controller	SafetyLocked	SINT	Indicates whether the controller is safety-locked or -unlocked.	X		X	
	SafetyStatus(2)	INT	Specifies the safety status as the following: • Safety task OK. (1000000000000000) • Safety task inoperable. (1000000000000001) • Firmware incompatible. (0000000000000011)			X	
	SafetySignatureExists	SINT	Indicates whether the safety task signature is present.	X		X	
	SafetySignatureID	DINT	32-bit identification number.			X	
	SafetySignature	String(3)	32-bit identification number.			X	
	SafetyTaskFaultRecord(1)(2)	DINT[11]	Records safety task faults.			X	
AOI (Safety)	LastEditDate	LINT	Date and time stamp of the last edit to an Add-On Instruction definition.			X	
	SignatureID	DINT	ID number.			X	
	SafetySignatureID	DINT	32-bit identification number.			X	

(1) See Access FaultRecord Attributes on page 153 for information on how to access this attribute.
(2) See Capture Fault Information on page 153 for information on how to access this attribute.
(3) Length = 37.
(4) From the standard task, GSV accessibility of safety object attributes is the same as for standard object attributes.

Access FaultRecord Attributes

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

Parameters for Accessing FaultRecord Attributes

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

For more information on how to use the GSV and SSV instructions, refer to the I/O Instructions chapter of the Logix Controllers Instructions Reference Manual, publication 1756-RM009.

Capture Fault Information

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

Notes:

Store and Load Programs with a Secure Digital Card

IMPORTANT The life expectancy of nonvolatile media is dependent on the number of write cycles that are performed. Nonvolatile media use a technique that levels wear, or technology for prolonging the service life, but avoid frequent writes.

Avoid frequent writes when logging data. We recommend that you log data to a buffer in the memory of your controller and limit the number of times data is written to removable media.

Use SD Cards for Nonvolatile Memory

Compact GuardLogix® 5370 controllers support a Secure Digital (SD) card for nonvolatile memory:

- 1784-SD1 card - Ships with Compact GuardLogix 5370 controller and offers 1 GB of memory. You can order more 1784-SD1 cards if desired.
- 1784-SD2 card - Available for separate purchase and offers 2 GB of memory.

Nonvolatile memory lets you keep a copy of your project on the controller. The controller does not need power or a battery to keep this copy.

You can load the stored project from nonvolatile memory to the user memory of the controller:

- On every power-up
- Whenever there is no project in the controller and it powers up
- Anytime through the programming software

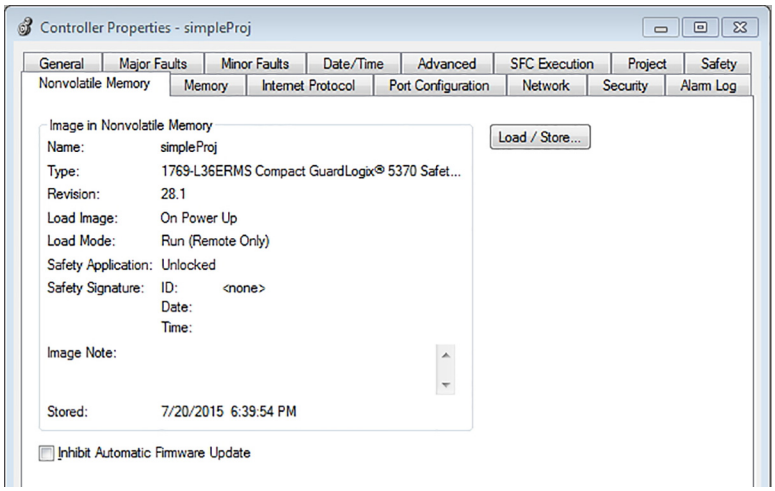
IMPORTANT Nonvolatile memory stores the contents of the user memory at the time that you store the project:

- Changes that you make after you store the project are not reflected in nonvolatile memory.
- If change the project but do not store those changes, you overwrite them when you load the project from nonvolatile memory. If this occurs, you have to upload or download the project to go online.
- If you want to store changes, such as online edits or tag values, store the project again after you make the changes.

ATTENTION: Do not remove the SD card while the controller is reading from or writing to the card, as indicated by a flashing green SD status indicator. This action could corrupt the data on the card or in the controller, and corrupt the latest firmware in the controller. Leave the card in the controller until the SD status indicator turns steady green.

WARNING: When you insert or remove the SD card while power is on, an electric arc can occur. This arc could cause an explosion in hazardous location installations.
Be sure that power is removed or the area is nonhazardous before proceeding.

If an SD card is installed, you can view 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 task signature are shown.



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

Store a Safety Project

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

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

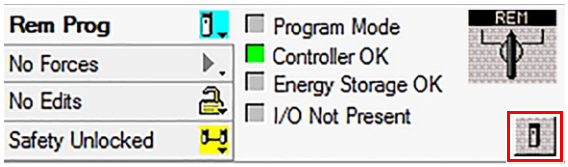
If a safety task signature exists when you store a project, the following occurs:

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

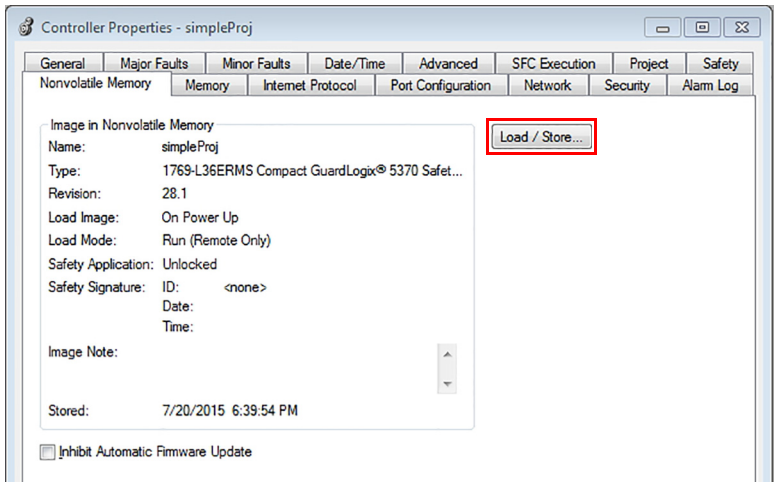
When you store a safety application project on an SD card, we recommend that you select Program (Remote Only) as the Load mode, that is, the mode that the controller usually enters after a load. For more information, see Load a Safety Project on page 159.

Follow these steps to store a project.

1. Go online with the controller.
2. Put the controller in Program mode, that is, Remote Program or Program.
3. On the Online toolbar, click the controller properties icon.

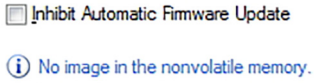


4. Click the Nonvolatile Memory tab.
5. Click Load/Store.

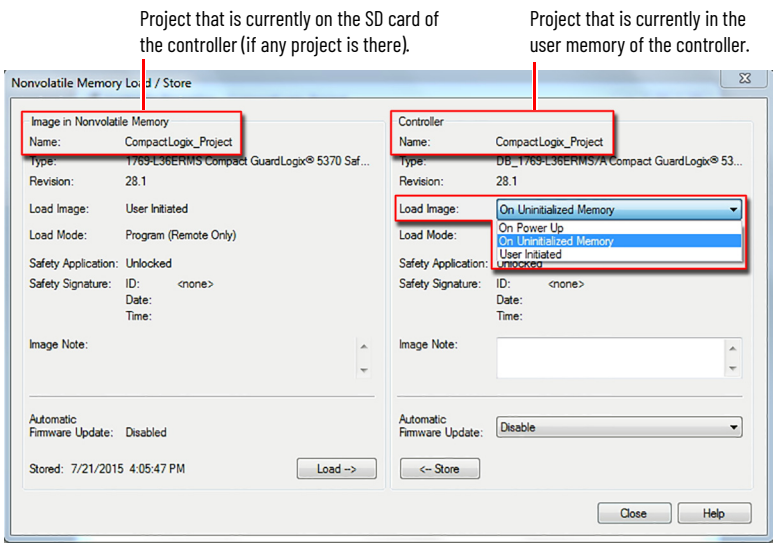


If Load/Store is dimmed (unavailable), verify the following:

- You have specified the correct communication path and are online with the controller.
- The SD card is installed.
  If the SD card is not installed, a message in the lower-left corner of the Nonvolatile Memory tab indicates that the card is missing.

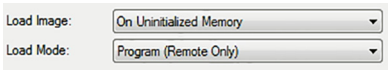


6. Choose when (under what conditions) to load the project into the user memory of the controller.



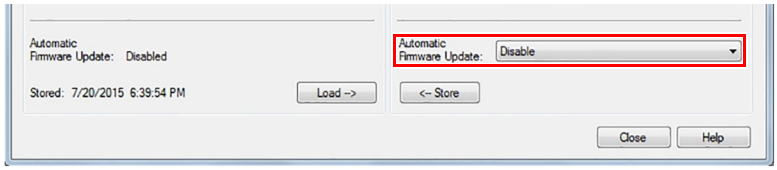
If you choose On Power Up or On Uninitialized Memory, you must also choose the mode that you want the controller to go to after the load:

- Program (Remote Only)
- Run (Remote Only)



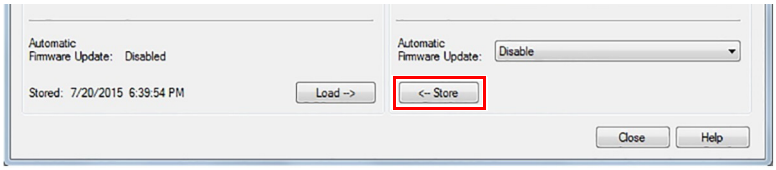
When you store a safety application project on an SD card, we recommend that you select Program (Remote Only) as the Load mode, that is, the mode that the controller usually enters after a load.

7. In the Automatic Firmware Update box, use the default (disable) or choose the Firmware Supervisor option.



IMPORTANT The Firmware Supervisor option is not used to upgrade the controller firmware.

8. Click <--Store.



IMPORTANT Store is not active if an SD card is locked.

A confirmation dialog box appears.

9. To store the project, click Yes.

After you click Store, the project is saved to the SD card as indicated by the controller status indicators. These conditions can exist:

- While the store is in progress, the following occurs:
  - The OK indicator is flashing green.
  - The SD indicator is flashing green.
  - A dialog box indicates that the store is in progress.
- When the store is complete, the following occurs:
  - The controller resets itself.

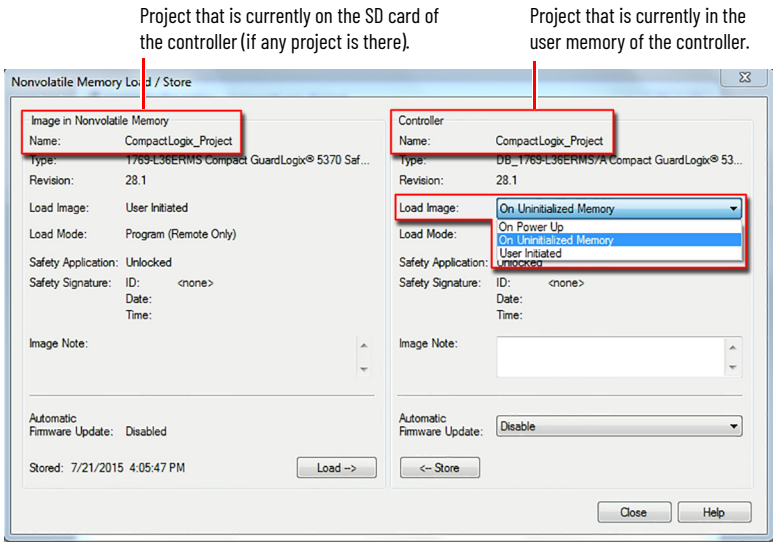
    When the controller is resetting itself, the status indicators execute a sequence of state changes, for example, a brief time with the OK status indicator in the steady red state. Wait for the controller to complete the sequence.
  - After the controller fully resets itself, the OK indicator is steady green.
  - The SD indicator is off.

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

Load a Safety Project

You can only initiate a load from nonvolatile memory if the following is true:

- The controller type that is specified by the project that is stored in nonvolatile memory matches the controller type.
- The major and minor revisions of the project in nonvolatile memory match the major and minor revisions of the controller.
- Your controller is not in Run mode.



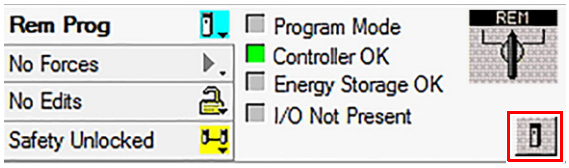
You have several options for when (under what conditions) to load a project into the user memory of the controller.

Project Load Options

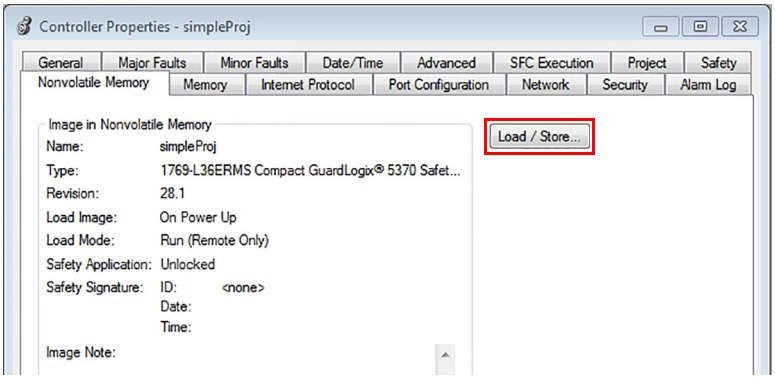
If you want to load the project	Then select this Load Image option	Notes
Whenever you turn on or cycle power	On Power Up	• During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory. • The controller loads the stored project and firmware at every power-up regardless of the firmware or application on the controller. The load occurs whether the controller is safety-locked or has a safety task signature. • You can always use the programming software to load the project.
Whenever there is no project in the controller and you turn on or cycle power	On Uninitialized Memory	• The controller updates the firmware on the controller, if necessary. The application 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 programming software to load the project.
Only through RSLogix 5000® software	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, regardless of the Safety Task status. • You are only allowed to load a project to a safety-locked controller when the safety task 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 task 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 task signature are set to the values contained in nonvolatile memory once the load is complete. • If the firmware on the controller matches the revision in nonvolatile memory, the internal safety partner firmware is updated, if necessary, the application that is stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the selected mode, either Program or Run.

Follow these steps to use the application to load the project from an SD card.

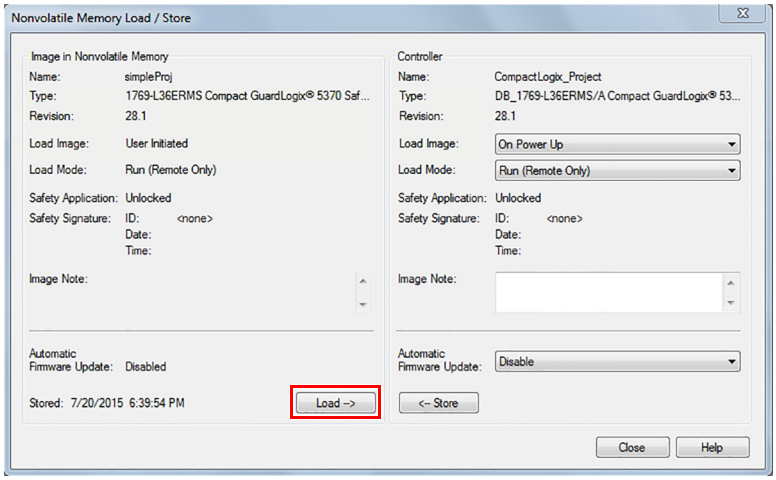
1. Go online with the controller.
2. Put the controller in Program mode, that is, Remote Program or Program.
3. On the Online toolbar, click the controller properties icon.



4. Click the Nonvolatile Memory tab.
5. Click Load/Store.



6. On the nonvolatile memory load/store dialog box, click Load.



A confirmation dialog box appears.

7. To load the project, click Yes.

After you click Load, the project is loaded into the controller as indicated by the controller status indicators. While the load is in progress, the following occurs:

- The controller resets itself.

  During the controller reset, the status indicators execute a sequence of state changes, for example, a brief time with the OK status indicator in the steady red state. Wait for the controller to complete the sequence.
- After the controller fully resets itself, the OK indicator is steady green.
- The SD indicator is off.

Manage Firmware with Firmware Supervisor

You can use the Firmware Supervisor feature in the Logix Designer application to manage firmware on Compact GuardLogix 5370 controllers. Firmware Supervisor lets controllers automatically update devices:

- Local and remote modules can be updated while in Program or Run modes.
- Electronic keying must be configured for Exact Match.
- The firmware kit for the target device must reside on the controller's SD card.
- The device must support firmware updates via the ControlFLASH™ software.

Firmware Supervisor supports non-modular distributed I/O products that sit directly on the network without an adapter, including CIP Safety™ I/O modules on EtherNet/IP™ networks.

Follow these steps to enable Firmware Supervisor.

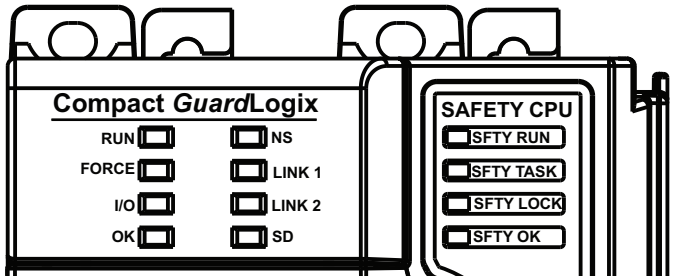
1. On the Controller Properties dialog box, click the Nonvolatile Memory tab.
2. Click Load/Store.
3. From the Automatic Firmware Updates pull-down menu, choose Enable and Store Files to Image.

The Logix Designer application moves the firmware kits from your computer to the controller SD card for Firmware Supervisor to use.

If you disable Firmware Supervisor, you disable only Firmware Supervisor updates. Controller firmware updates that occur when the controller image is reloaded from the SD card are not disabled.

Status Indicators

This section explains how to interpret the status indicators on the Compact GuardLogix® 5370 controllers.



Controller Mode (RUN) Status Indicator

Status	Description
Off	The controller is in Program or Test mode.
Green	The controller is in Run mode.

Force State (FORCE) Status Indicator

Status	Description
Off	No tags contain I/O force values. I/O forces are inactive (disabled).
Yellow	I/O forces are active (enabled). I/O force values can exist.
Flashing yellow	One or more input or output addresses have been forced to an On or Off condition, but the forces have not been enabled.

I/O State (I/O) Status Indicator

Status	Description
Off	One of the following conditions exists: • There are no devices in the I/O configuration of the controller. • The controller does not contain a project.
Green	The controller is communicating with all devices in its I/O configuration.
Flashing green	One or more devices in the I/O configuration of the controller are not responding.
Flashing red	One of the following conditions exists: • The controller is not communicating with any devices. • A fault has occurred on the controller.

Controller Status (OK) Status Indicator

Status	Description
Off	No power is applied.
Green	The controller is OK.
Flashing green	The controller stores or loads a project from the SD card.
Red	The controller detected a nonrecoverable major fault and cleared the project from memory.
Flashing red	One of the following: • The controller requires a firmware update. • A major recoverable fault occurred on the controller. • A nonrecoverable major fault occurred on the controller and cleared the program from memory.

Ethernet Network Status (NS) Status Indicator

Status	Description
Off	The port is not initialized; it does not have an IP address and is operating in BOOTP or DHCP mode.
Green	The port has an IP address and CIP connections are established.
Flashing green	The port has an IP address, but no CIP™ connections are established.
Red	The port has detected that the assigned IP address is already in use.
Flashing red/green	The port is performing its power up self-test.

Ethernet Link Status (LINK 1/LINK 2) Status Indicator

Status	Description
Off	One of the following conditions exists: • No link. • Port administratively disabled. • Port disabled because rapid ring fault condition was detected (LINK2).
Green	One of the following conditions exists: • A 100 Mbps link (half- or full-duplex) exists, no activity. • A 10 Mbps link (half- or full-duplex) exists, no activity. • Ring network is operating normally and the controller is the active supervisor. • Ring network has encountered a rare partial network fault and the controller is the active supervisor.
Flashing green	A 100 Mbps link exists and there is activity.

SD Card Activity (SD) Status Indicator

Status	Description
Off	There is no activity to the SD card.
Flashing green	The controller is reading from or writing to the SD card.
Flashing red	The SD card does not have a file system.

SFTY RUN Status Indicator

Status	Description
Off	The user safety task or safety outputs are disabled. The controller is in the PROG mode, test mode, or the safety task is faulted.
Green	The user safety task and safety outputs are enabled. The safety task is executing. Safety task signature is present.
Flashing Green	The user safety task and safety outputs are enabled. The safety task is executing. Safety task signature is not present.

SFTY TASK Status Indicator

Status	Description
Off	No partnership established.
Green	Safety controller status is OK. The coordinated system time (CST) is synchronized and safety I/O connections are established.
Flashing Green	Safety controller status is OK. The coordinated system time (CST) is not synchronized.
Red	Safety partnership was lost.
Flashing Red	Safety task is inoperable.

SFTY LOCK Status Indicator

Status	Description
Off	Safety task is not locked.
Green	Safety task is locked.

SFTY OK Status Indicator

Status	Description
Off	No power is applied.
Green	The safety partner is OK.
Flashing Green	The safety partner stores or loads a project to or from nonvolatile memory.
Red	The safety partner detected a nonrecoverable major fault, so it cleared the project from its memory.
Flashing Red	The internal safety partner requires a firmware update or a firmware update is in progress.

Notes:

Change Controller Type

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

- Supported features
- The safety partner and Safety I/O (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

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:

- Safety components are created (safety task, safety program, and so on).

  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.
- A time-based safety network number (SNN) is generated for the local chassis.
- Standard controller features, like redundancy, which the safety controller does not support, are removed from the Controller Properties dialog box (if they existed).

Change from a Safety to a Standard Controller

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 modules 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 number (SNN) is deleted.
- Safety-lock and -unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, those new features are visible in the Controller Properties dialog box.

Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions can still reference modules that have been deleted and produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the previously listed changes to the system, safety-specific instructions and safety I/O tags cannot be verified.

If the safety controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

Change Safety Controller Types

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

IMPORTANT 1768 Compact I/O™ modules are not compatible in a (1769) Compact GuardLogix® 5370 controller system.

The representation of the safety partner is updated to appear appropriately for the target controller in these cases:

- The safety partner is created in slot *x* (primary slot + 1) when changing from a Compact GuardLogix 5370 to a GuardLogix 5570 controller.
- When changing to a Compact GuardLogix 5370 controller from a GuardLogix 5570 controller, the safety partner is removed because it is internal to the Compact GuardLogix controller.

Numerics

A

B

C

D

T

U

V

W

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1769-UM022D-EN-P - August 2022
Supersedes 1769-UM022C-EN-P - June 2018