

User Manual

Original Instructions



# Compact GuardLogix Controllers

Catalog Numbers 1768-L43S, 1768-L45S



# Important User Information

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

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

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

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

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

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

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

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



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



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

---

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

---

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



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



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



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

---

	<b>Preface</b> .....	7
	Summary of Changes .....	7
	Understanding Terminology .....	7
	Additional Resources .....	8
	 <b>Chapter 1</b>	
<b>System Overview</b>	Safety Application Requirements .....	9
	Safety Network Number .....	9
	Safety Task Signature .....	10
	Distinguishing Between Standard and Safety Components .....	10
	HMI Devices .....	10
	Controller Data Flow Capabilities .....	11
	Selecting System Hardware .....	12
	Controller .....	12
	Selecting Safety I/O Modules .....	12
	Selecting Communication Networks .....	12
	Programming Requirements .....	13
	 <b>Chapter 2</b>	
<b>Install the Controller</b>	Precautions .....	15
	Environment and Enclosure Information .....	15
	Programmable Electronic Systems (PES) .....	16
	North American Hazardous Location Approval .....	16
	European Hazardous Location Approval .....	17
	Prevent Electrostatic Discharge .....	17
	Required System Components .....	18
	Clearance Requirements .....	18
	Module Placement .....	18
	Mount the Controller .....	20
	Panel Mount the Controller .....	20
	Mount the Controller on a DIN Rail .....	21
	Confirm the Installation .....	23
	Insert or Remove a Memory Card .....	24
	Make Communication Connections .....	24
	Update the Controller .....	26
	Install Firmware via ControlFLASH Software .....	26
	Install Firmware via AutoFlash Software .....	27
	Install Firmware via a CompactFlash Card .....	27
	Faceplate Push Button .....	28
	Remove a 1768 or 1769 Module from the DIN Rail .....	28
	 <b>Chapter 3</b>	
<b>Configure the Controller</b>	Create a Controller Project .....	31
	Set Passwords for Safety-locking and -unlocking .....	33

Protecting the Safety Task Signature in Run Mode .....	34
Handling I/O Module Replacement .....	35
Enable Time Synchronization .....	35
Configure a Peer Safety Controller.....	36

## **Chapter 4**

### **Communicate over Networks**

The Safety Network .....	37
Managing the Safety Network Number (SNN).....	37
Assigning the Safety Network Number (SNN).....	39
Changing the Safety Network Number (SNN).....	39
EtherNet/IP Communication.....	43
Producing and Consuming Data via an EtherNet/IP Network	43
Connections over the EtherNet/IP Network .....	43
EtherNet/IP Communication Example .....	44
EtherNet/IP Connections for CIP Safety I/O Modules.....	45
Standard EtherNet/IP Connections.....	45
ControlNet Communication .....	46
Producing and Consuming Data via a ControlNet Network ..	46
Connections over the ControlNet Network .....	46
ControlNet Communication Example .....	47
ControlNet Connections for Distributed I/O .....	48
Standard DeviceNet Communication.....	49
Serial Communication.....	50
Additional Resources .....	51

## **Chapter 5**

### **Add, Configure, Monitor, and Replace CIP Safety I/O**

Adding CIP Safety I/O Modules .....	53
Configure CIP Safety I/O Modules via RSLogix 5000 Software ...	54
Setting the Safety Network Number (SNN) .....	55
Using Unicast Connections on EtherNet/IP Networks.....	55
Setting the Connection Reaction Time Limit.....	55
Specify the Requested Packet Interval (RPI) .....	56
View the Maximum Observed Network Delay .....	56
Setting the Advanced Connection Reaction Time Limit Parameters	57
Understanding the Configuration Signature.....	59
Configuration via RSLogix 5000 Software .....	59
Different Configuration Owner (listen only connection) ....	60
Reset Safety I/O Module Ownership.....	60
Addressing Safety I/O Data .....	60
Monitor Safety I/O Module Status .....	61
Resetting a Module to Out-of-box Condition.....	63
Replacing a Module.....	63
Replacement with 'Configure Only When No Safety	
Signature Exists' Enabled.....	64
Replacement with 'Configure Always' Enabled.....	68

<b>Develop Safety Applications</b>	<b>Chapter 6</b>	
	The Safety Task .....	72
	Safety Task Period Specification .....	72
	Safety Task Execution.....	73
	Safety Programs .....	74
	Safety Routines .....	74
	Safety Tags .....	74
	Tag Type .....	75
	Data Type .....	76
	Scope.....	77
	Class .....	78
	Constant Value.....	78
	External Access.....	78
	Produced/Consumed Safety Tags.....	79
	Configure the Peer Safety Controllers' Safety	
	Network Numbers.....	79
	Produce a Safety Tag.....	81
	Consume Safety Tag Data.....	82
	Safety Tag Mapping .....	84
	Restrictions .....	84
	Create Tag Mapping Pairs.....	85
	Monitor Tag Mapping Status.....	86
	Safety Application Protection .....	86
	Safety-lock the Controller.....	86
	Generate a Safety Task Signature.....	88
	Software Restrictions .....	89
<b>Go Online with the Controller</b>	<b>Chapter 7</b>	
	Connecting the Controller to the Network.....	91
	Connect the Controller via a Serial Network.....	91
	Connect Your EtherNet/IP Device and Computer.....	92
	Connect Your ControlNet Communication Module	
	and Your Computer .....	92
	Configuring the Network Driver .....	92
	Configure a Serial Communication Driver.....	93
	Configuring an EtherNet/IP or ControlNet Driver .....	93
	Understanding the Factors that Affect Going Online.....	93
	Project to Controller Matching.....	94
	Firmware Revision Matching.....	94
	Safety Status/Faults.....	94
	Safety Task Signature and Safety-locked and -unlocked Status ..	95
	Download .....	96
	Upload.....	98
	Go Online.....	99

	<b>Chapter 8</b>	
<b>Monitor Status and Handle Faults</b>	Viewing Status via the Online Bar .....	101
	Monitoring Connections .....	102
	All Connections .....	102
	Safety Connections .....	103
	Monitoring Status Flags .....	103
	Monitoring Safety Status .....	104
	Controller Faults .....	104
	Nonrecoverable Controller Faults .....	104
	Nonrecoverable Safety Faults in the Safety Application .....	104
	Recoverable Faults in the Safety Application .....	105
	Viewing Faults .....	105
	Fault Codes .....	106
	Developing a Fault Routine .....	106
	Program Fault Routine .....	106
	Controller Fault Handler .....	107
	Use GSV/SSV Instructions .....	107
	<b>Chapter 9</b>	
<b>Store and Load Projects Using Nonvolatile Memory</b>	Using Memory Cards for Nonvolatile Memory .....	111
	Storing a Safety Project .....	113
	Loading a Safety Project .....	113
	Manage Firmware with Firmware Supervisor .....	114
	<b>Appendix A</b>	
<b>Status Indicators</b>	Compact GuardLogix Controller Status Indicators .....	117
	Clear a Major Fault .....	118
	Clear a Nonrecoverable Fault .....	119
	Troubleshoot a Nonresponsive Module .....	119
	Troubleshoot System Power .....	120
	Examine the Power Supply PWR Status Indicator .....	120
	Examine the Controller PWR Indicator .....	121
	Examine the I/O PWR Indicator .....	121
	<b>Appendix B</b>	
<b>Change Controller Type in RSLogix 5000 Projects</b>	Changing from a Standard to a Safety Controller .....	123
	Changing from a Safety to a Standard Controller .....	124
	Changing from a 1756 GuardLogix Controller to a 1768 Compact GuardLogix Controller or Vice Versa .....	125
	Changing from a 1756-L7xS Controller to a 1756-L6xS or 1768-L4xS Controller .....	125
	Additional Resources .....	125
	<b>Index</b> .....	127

This manual is a guide for using Compact GuardLogix™ controllers. It describes the Compact GuardLogix-specific procedures you use to configure, operate, and troubleshoot your controller.

Use this manual if you are responsible for designing, installing, programming, or troubleshooting control systems that use Compact GuardLogix controllers.

You must have a basic understanding of electrical circuitry and familiarity with relay logic. You must also be trained and experienced in the creation, operation, and maintenance of safety systems.

For detailed information on related topics like programming your Compact GuardLogix controller, SIL 3/PLe requirements, or information on standard Logix components, see the list of [Additional Resources](#) on page 8.

## Summary of Changes

This manual contains new and updated information. Since the last release of this publication, we added a section about the recessed push button on the faceplate of the controller.

Topic	Page
Specified up to V20 in footnote	13
Added section on recessed push button on the faceplate of the controller	28

## Understanding Terminology

This table defines terms used in this manual.

**Table 1 - Terms and Definitions**

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 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.
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.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
RPI	Requested Packet Interval	The expected rate in time for production of data when communicating 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
CompactLogix Controllers Specifications Technical Data, publication <a href="#">1769-TD005</a>	Provides specifications, dimensions, and certification information for Compact GuardLogix controllers
GuardLogix Controller Systems Safety Reference Manual, publication <a href="#">1756-RM093</a>	Contains detailed requirements for achieving and maintaining SIL 3/PLe with the GuardLogix controller system
GuardLogix Safety Application Instruction Set Reference Manual, publication <a href="#">1756-RM095</a>	Provides information on the GuardLogix Safety application instruction set
CompactBlock Guard I/O EtherNet/IP™ Safety Modules Installation Instructions, publication <a href="#">1791ES-IN001</a>	Provides information on installing CompactBlock™ Guard I/O™ EtherNet/IP Safety modules
Guard I/O EtherNet/IP Safety Modules User Manual, publication <a href="#">1791ES-UM001</a>	Provides information on using Guard I/O EtherNet/IP Safety modules
CompactLogix Controllers User Manual, publication <a href="#">1768-UM001</a>	Provides information on using CompactLogix™ controllers in standard applications
Logix5000 Controllers General Instruction Set Reference Manual, publication <a href="#">1756-RM003</a>	Provides information on the Logix5000™ instruction set
Logix5000 Controllers Common Procedures Programming Manual, publication <a href="#">1756-PM001</a>	Provides access to the Logix5000 Controllers set of programming manuals, which covers managing project files, organizing tags, ladder logic programming, testing routines, creating Add-On Instructions, controller status data, handling faults, importing and exporting project components and more
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication <a href="#">ENET-UM001</a>	Provides information on using EtherNet/IP communication modules in a Logix5000 control system
ControlNet™ Modules in Logix5000 Control Systems User Manual, publication <a href="#">CNET-UM001</a>	Provides information on using the 1756-CNB module in Logix5000 control systems
Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication <a href="#">1756-RM087</a>	Provides information on estimating the execution time and memory use for instructions
Logix5000 Controllers Import Export Reference Manual, publication <a href="#">1756-RM084</a>	Provides information on using RSLogix 5000® Import/Export utility
PhaseManager User Manual, publication <a href="#">LOGIX-UM001</a>	Provides information on programming the controller to use equipment phases in a standard application
SERCOS and Analog Motion Configuration and Startup Manual, publication <a href="#">MOTION-UM001</a>	Provides information on configuring the controller for motion axes, coordinate system, and motion modules in standard applications
Industrial Automation Wiring and Grounding Guidelines, publication <a href="#">1770-4.1</a>	Provides in-depth information on grounding and wiring programmable controllers

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



## System Overview

Topic	Page
Safety Application Requirements	9
Distinguishing Between Standard and Safety Components	10
Controller Data Flow Capabilities	11
Selecting System Hardware	12
Selecting Safety I/O Modules	12
Selecting Communication Networks	12
Programming Requirements	13

### Safety Application Requirements

The Compact GuardLogix™ controller system is certified for use in safety applications up to and including Safety Integrity Level (SIL) 3 and Performance Level (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 Controller Systems Safety Reference Manual, publication [1756-RM093](#). You must read, understand, and fulfill these requirements prior to operating a Compact GuardLogix SIL 3, PLe safety system.

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.

Refer to the GuardLogix Controller Systems Safety Reference Manual, publication [1756-RM093](#), for details.

### 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 assigning the SNN, see [Managing the Safety Network Number \(SNN\) on page 37](#).

## 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. Creating, recording, and verifying the safety task signature is a mandatory part of the safety-application development process.

See [Generate a Safety Task Signature on page 88](#) for more information.

## Distinguishing Between Standard and Safety Components

Slots in the Compact GuardLogix backplane may be populated with other CompactLogix I/O modules that are certified to the Low Voltage and EMC Directives. Refer to <http://www.ab.com/certification/ce> 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 application. To aid in creating this distinction, RSLogix 5000™ programming software features safety identification icons to identify the safety task, safety programs, safety routines, and safety components. In addition, the RSLogix 5000 software 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 HMI devices or via message instructions from peer controllers. RSLogix 5000 software 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.

The 1768 CompactLogix Controllers User Manual, publication [1768-UM001](#), provides information on using 1768 CompactLogix controllers in standard (non-safety) applications.

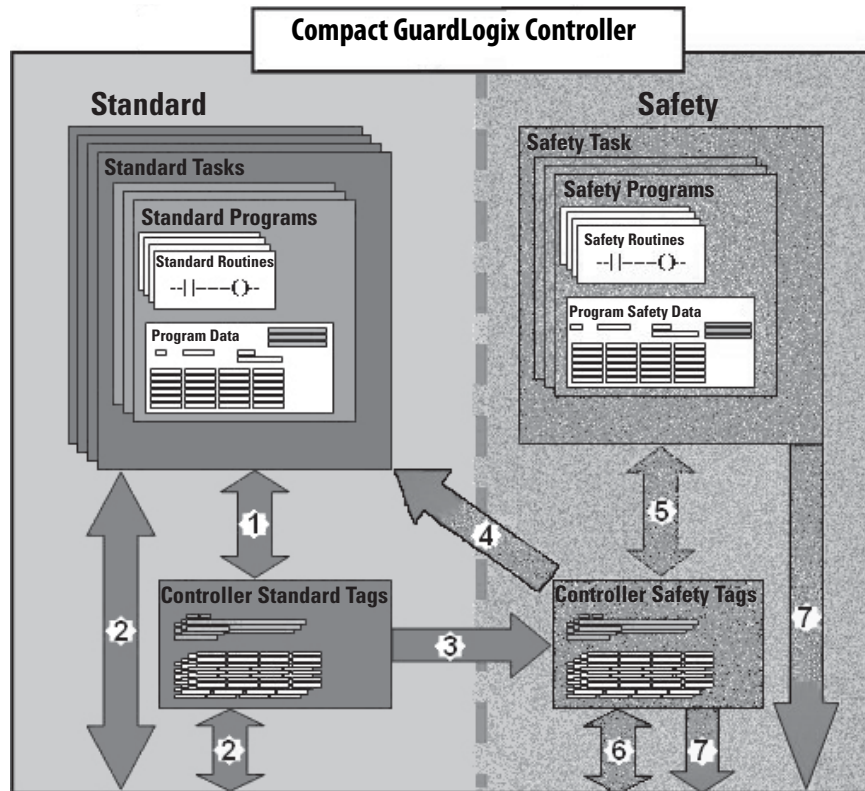
## HMI Devices


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

## Controller Data Flow Capabilities

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

Figure 1 - Data Flow Capabilities



No.	Description
1	Standard tags and logic behave the same way 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.
	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <b>ATTENTION:</b> This data must not be used to directly control a SIL 3/PLc output. </div> </div>
4	Controller-scoped safety tags can be read directly by standard logic.
5	Safety tags can be read or written by safety logic.
6	Safety tags can be exchanged between safety controllers over Ethernet or ControlNet networks, including 1756 and 1768 GuardLogix controllers.
7	Safety tag data, program- or controller-scoped, can be read by external devices, such as HMI devices, personal computers, or other standard controllers.
	<b>IMPORTANT</b> Once this data is read, it is considered standard data, not SIL 3/PLc data.

## Selecting System Hardware

The Compact GuardLogix system supports SIL 3 and PLe safety applications.

### Controller

1768-L43S and 1768-L45S controllers feature one built-in serial port. A keyswitch on the front panel lets you change controller modes: RUN, PROGram and REMote. The 1768 Compact GuardLogix controllers combine a 1768 backplane with a 1769 backplane. This combination includes all the advantages of the 1768 architecture for safety applications while retaining the 1769 I/O support for standard applications.

Controller	Available 1768 Slots	Number of 1768 Communication Modules	Maximum Local 1769 I/O Modules Supported	Number of Connections Supported	Safety Task Memory	Standard Memory
1768-L43S	2	2	16 modules in 3 banks	250	0.5 MB	2 MB
1768-L45S	4	2	30 modules in 3 banks		1 MB	3 MB

In addition, Compact GuardLogix controllers support 1768-M04SE SERCOS modules for motion control in standard (non-safety) applications. For information on developing motion applications, refer to the SERCOS and Analog Motion Configuration and Startup Manual, publication [MOTION-UM001](#).

## Selecting Safety I/O Modules

Safety input and output devices can be connected to CIP Safety I/O on EtherNet/IP networks, allowing output devices to be controlled by a Compact GuardLogix controller system via EtherNet/IP communication.

For the most up-to-date information on available CIP Safety I/O catalog numbers, certified series, and firmware revisions, see <http://www.ab.com/certification/safety>.

## Selecting Communication Networks

The Compact GuardLogix controller supports communication that lets it do the following:

- Distribute and control Safety I/O on EtherNet/IP networks.
- Produce and consume safety tag data between 1756 and 1768 GuardLogix controllers across EtherNet/IP or ControlNet networks.
- Distribute and control standard I/O on EtherNet, ControlNet, or DeviceNet networks.

Use these communication modules to provide an interface between Compact GuardLogix controllers and network devices.

Use this module	To interface between
1768-ENBT, series A, revision 3 <sup>(1)</sup>	The Compact GuardLogix controller and EtherNet/IP devices
1768-CNB, series A, revision 3 <sup>(1)</sup>	Controllers on the ControlNet network

(1) This or later.

The Compact GuardLogix controller can connect to RSLogix 5000 programming software via a serial connection, an 1768-ENBT EtherNet module, or a 1768-CNB ControlNet module.

See the [Additional Resources on page 8](#) for more information on using network communication modules.

## Programming Requirements

RSLogix 5000 software is the programming tool for Compact GuardLogix controller applications.

Use [Table 2](#) to identify the minimum software versions for use with your Compact GuardLogix controllers.

**Table 2 - Software Versions**

Cat. No.	RSLogix 5000 Software Version <sup>(1)</sup>	RSLink <sup>®</sup> Classic Software Version <sup>(1)</sup>
1756-L43S, 1756-L45S	18	Any version <sup>(2)</sup>

(1) This version and up to V20.

(2) RSLink Classic version 2.59 or later is required with RSLogix 5000 software version 20 or later.

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

**Table 3 - Supported Features by RSLogix 5000 Software Version**

Feature	Version 18		Version 19		Version 20	
	Safety Task	Standard Task	Safety Task	Standard Task	Safety Task	Standard Task
Add-On instructions	X	X	X	X	X	X
Alarms and events		X		X		X
Constant value tags	X	X	X	X	X	X
Equipment phase routines		X		X		X
External Access	X	X	X	X	X	X
Event tasks		X		X		X
Firmware Supervisor	X	X	X	X	X	X
Function block diagrams (FBD)		X		X		X
Integrated motion		X		X		X
Ladder logic	X	X	X	X	X	X
Language switching	X	X	X	X	X	X
Online import and export of program components		X		X		X
Sequential function chart (SFC) routines		X		X		X
Structured text		X		X		X
Unicast connections for produced and consumed safety tags			X	X	X	X
Unicast connections for safety I/O modules					X	X

Compact GuardLogix controllers support 1768-M04SE SERCOS modules for motion control in standard (non-safety) applications. For information on developing motion applications, refer to the SERCOS and Analog Motion Configuration and Startup Manual, publication [MOTION-UM001](#).

Compact GuardLogix controllers also support PhaseManager™ programs, which let you add equipment phases to standard controller applications. Refer to the PhaseManager User Manual, publication [LOGIX-UM001](#), for more information.

For information on using these features, refer to the Logix5000 Controllers Common Procedures Programming Manual, publication [1756-PM001](#), the publications listed in the [Additional Resources on page 8](#), and RSLogix 5000 software online help.

## Install the Controller

Topic	Page
Precautions	15
Required System Components	18
Clearance Requirements	18
Module Placement	18
Mount the Controller	20
Insert or Remove a Memory Card	24
Make Communication Connections	24
Update the Controller	26
Faceplate Push Button	28
Remove a 1768 or 1769 Module from the DIN Rail	28

### Precautions

Read and follow these precautions for use.

### Environment and Enclosure Information



**ATTENTION:** This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is considered Group 1, Class A industrial equipment according to IEC/CISPR Publication 11. Without appropriate precautions, there may be difficulties with electromagnetic compatibility in residential and other environments due to conducted as well as radiated disturbances.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if non-metallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication [1770-4.1](#), for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

## Programmable Electronic Systems (PES)



**ATTENTION:** Personnel responsible for the application of safety-related Programmable Electronic Systems (PES) shall be aware of the safety requirements in the application of the system and shall be trained in using the system.

## North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations:	Informations sur l'utilisation de cet équipement en environnements dangereux:
<p>Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.</p>	<p>Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.</p>
<div data-bbox="152 995 245 1079" data-label="Image"> </div> <p><b>WARNING: EXPLOSION HAZARD</b></p> <ul style="list-style-type: none"> <li>Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.</li> <li>Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.</li> <li>Substitution of components may impair suitability for Class I, Division 2.</li> <li>If this product contains batteries, they must only be changed in an area known to be nonhazardous.</li> </ul>	<div data-bbox="823 995 915 1079" data-label="Image"> </div> <p><b>AVERTISSEMENT: RISQUE D'EXPLOSION</b></p> <ul style="list-style-type: none"> <li>Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement.</li> <li>Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit.</li> <li>La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2.</li> <li>S'assurer que l'environnement est classé non dangereux avant de changer les piles.</li> </ul>



---

## European Hazardous Location Approval

---

### The following applies when the product bears the Ex Marking.

This equipment is intended for use in potentially explosive atmospheres as defined by European Union Directive 94/9/EC and has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of Category 3 equipment intended for use in Zone 2 potentially explosive atmospheres, given in Annex II to this Directive.

Compliance with the Essential Health and Safety Requirements has been assured by compliance with EN 60079-15 and EN 60079-0.

---



**ATTENTION:** This equipment is not resistant to sunlight or other sources of UV radiation.

---



### **WARNING:**

- This equipment must be installed in an enclosure providing at least IP54 protection when applied in Zone 2 environments.
  - This equipment shall be used within its specified ratings defined by Rockwell Automation.
  - Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 40% when applied in Zone 2 environments.
  - Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
  - Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.
- 

---

## Prevent Electrostatic Discharge

---



**ATTENTION:** This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
  - Wear an approved grounding wriststrap.
  - Do not touch connectors or pins on component boards.
  - Do not touch circuit components inside the equipment.
  - Use a static-safe workstation, if available.
  - Store the equipment in appropriate static-safe packaging when not in use.
-

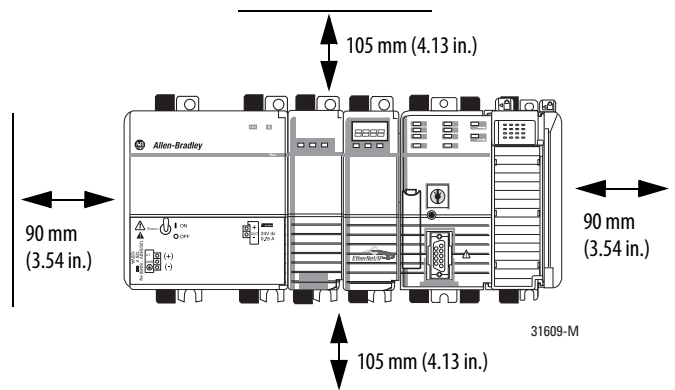
## Required System Components

You need these parts when installing your controller:

- 1768-L43S or 1768-L45S Compact GuardLogix controller
- 1768-PA3 or 1768-PB3 power supply
- 1769-ECR end cap
- Mounting screws (M4 or #8 panhead) or one of these EN 50 022 DIN rails:
  - 35 x 7.5 mm (1.38 x 0.30 in.)
  - 35 x 15 mm (1.38 x 0.59 in.)
- 1756-CP3 serial cable (or make your own)

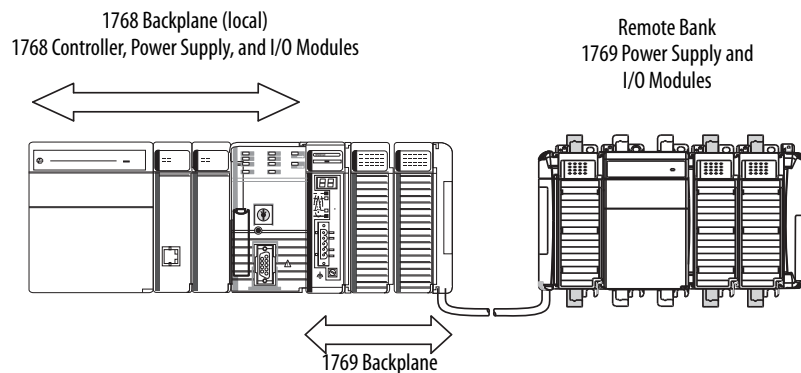
## Clearance Requirements

Allow for the minimum clearance from enclosure walls, wireways, and other equipment.



**IMPORTANT** These minimum clearances keep the modules cool enough in most situations. The operating temperature range is 0...60 °C (32...140 °F).

## Module Placement



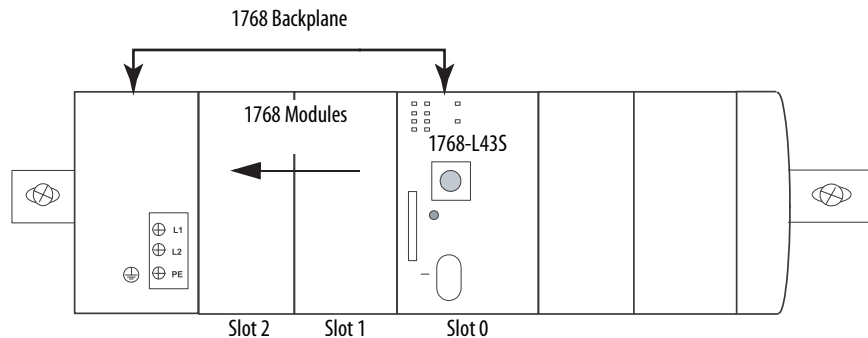
**IMPORTANT CompactLogix System Distance Ratings**

Because the 1768 CompactLogix power supply works with the controller to power a 1768 system, the distance rating in a 1768 CompactLogix system differs from that in a 1769 CompactLogix system.

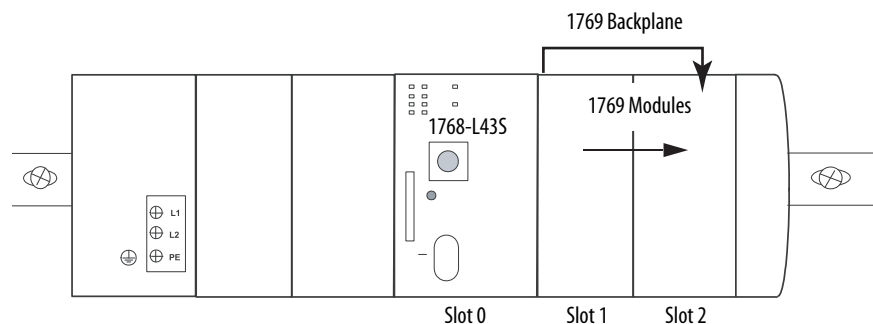
In the 1768 system, the distance rating is the distance between 1769 I/O modules and the controller. In the 1769 system, the distance rating is the distance between 1769 I/O modules and the power supply.

Follow these requirements to determine proper placement of your 1768 controller, power supply, 1768 I/O modules, and 1769 I/O modules:

- Place the 1768-L4xx controller so that it is the last module (furthest away from the power supply) in the 1768 backplane.
- The 1768 CompactLogix power supply distributes power from the right side of the supply and must be the leftmost module in the system.
- The local bank is powered by a 1768 power supply.
- Up to eight 1769 I/O modules can reside in the local bank.
- 1768 slots are numbered right to left, starting with the controller as slot 0.



- Up to two remote banks of 1769 I/O modules may be connected by using 1769-CRLx extension cables.
- Remote banks are powered by a standard 1769 power supply.
- Each I/O bank must have its own 1769 power supply.
- 1769 slots are numbered from left to right, starting with the controller as slot 0.



- Up to eight 1769 Compact I/O™ modules can reside on each side of a 1769 power supply in a remote bank. Consult the module’s specifications for its distance rating.

---

**IMPORTANT**    1769 power supplies must be separated from the 1768 series processor by a bus extension cable. Never put a 1769 power supply in the 1768 backplane or the controller will generate a major fault that cannot be cleared until you remove the 1769 power supply.

---

- The type of controller determines the maximum number of 1768 modules that can reside in the local bank and the maximum number of 1769 I/O modules that can reside in one local and up to two remote banks.

Controller	Max Local 1768 Modules	Max 1769 I/O Modules (local and remote)
1768-L43S	2	16
1768-L45S	4	30

## Mount the Controller

You can mount the controller to a panel or on a DIN rail.

---

**IMPORTANT**    Do not use screws if using a DIN rail to mount the controller. You can break the mounting tabs if you screw the controller to a panel while it is on a DIN rail.


---

### Panel Mount the Controller

Follow these steps to mount your controller by using the panhead screws.

1. Connect the CompactLogix modules together as shown in [Mount the Controller on a DIN Rail on page 21](#).
2. Use the controller as a template and mark pilot holes on your panel.
3. Drill the pilot holes for M4 or #8 screws.

---

 **ATTENTION:** During mounting of all devices, be sure that all debris (such as metal chips or wire strands) is kept from falling into the controller or I/O modules. Debris that falls into the controller or modules could cause damage while the controller is energized.

---

4. Use M4 or #8 screws to mount the controller to your panel with 1.16 N•m (10 lb•in) of torque.
5. Ground the module on a ground bus with a dedicated earth ground stake.
6. Connect the ground bus to a functional earth ground on the panel or a DIN rail.

## Mount the Controller on a DIN Rail

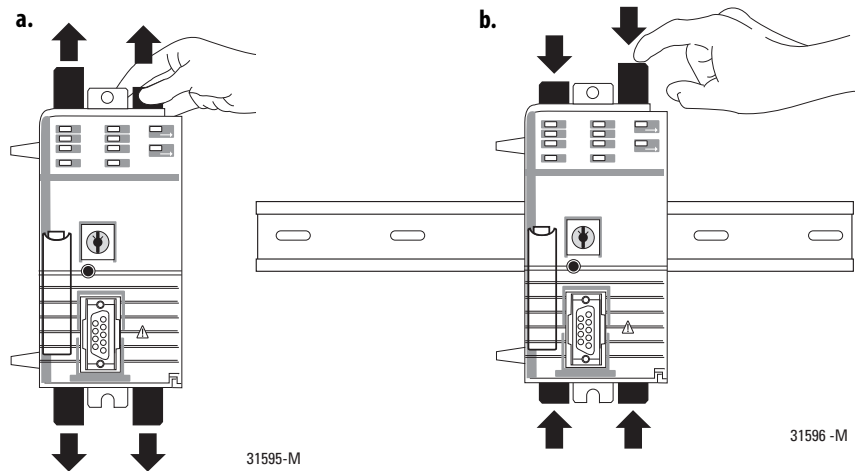


**ATTENTION:** This product is grounded through the DIN rail to chassis ground. Use zinc plated yellow-chromate steel DIN rail to assure proper grounding. The use of other DIN rail materials (for example, aluminum and plastic) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding. Secure DIN rail to the mounting surface approximately every 200 mm (7.87 in.) and use end anchors appropriately.

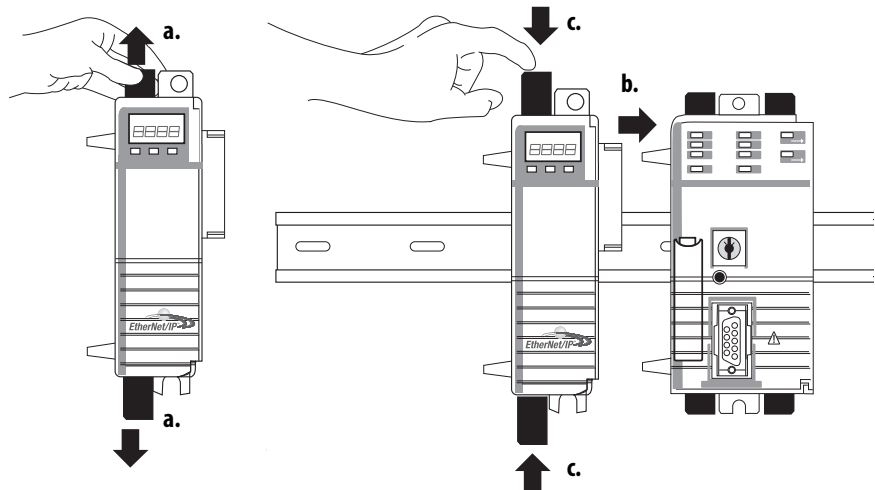
### Mount 1768 Components

Follow these steps to mount the controller.

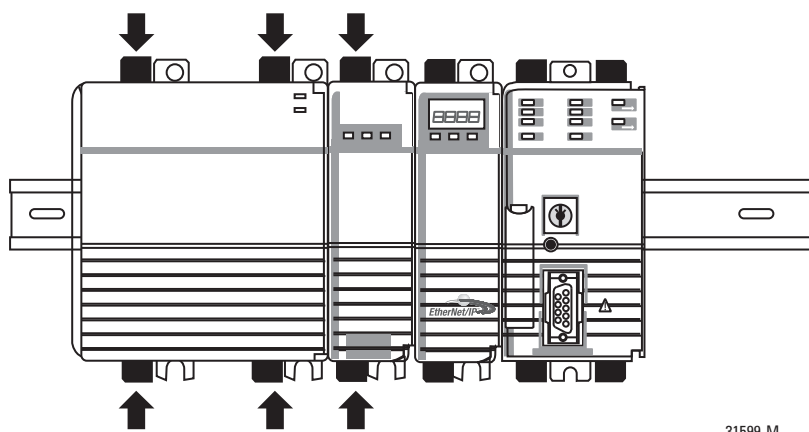
1. Mount the controller on the DIN rail.



2. Mount additional 1768 modules to the left of the controller.



3. Mount the 1768 power supply and other 1768 modules.

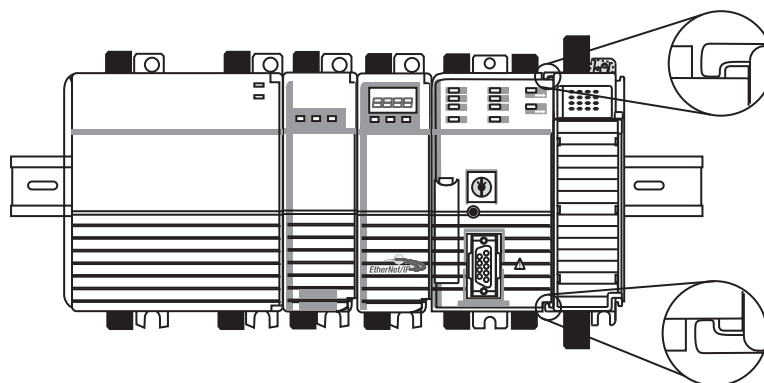


31599-M

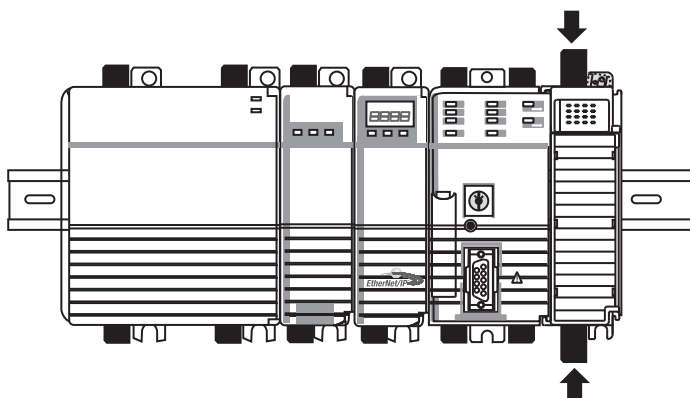
### Mount 1769 I/O Modules

Follow these steps to mount 1769 I/O modules to the right of the controller.

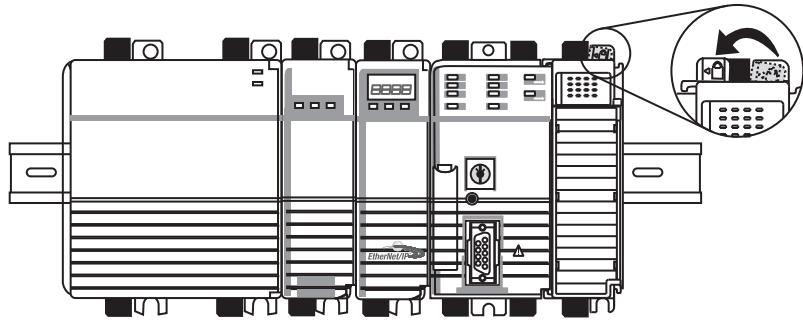
1. Align the upper and lower tongue-and-groove slots and slide the module back toward the DIN rail until the bus levers line up.



2. Close the DIN rail latches.

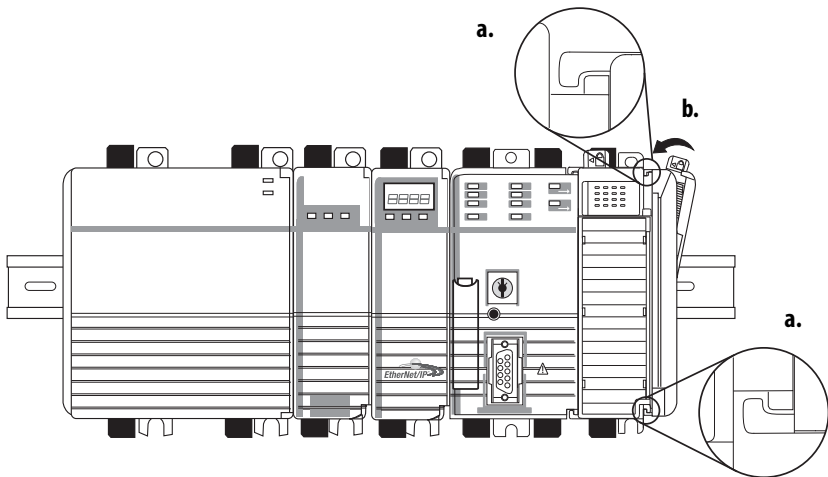


- Slide the bus lever to the left to lock the modules together.



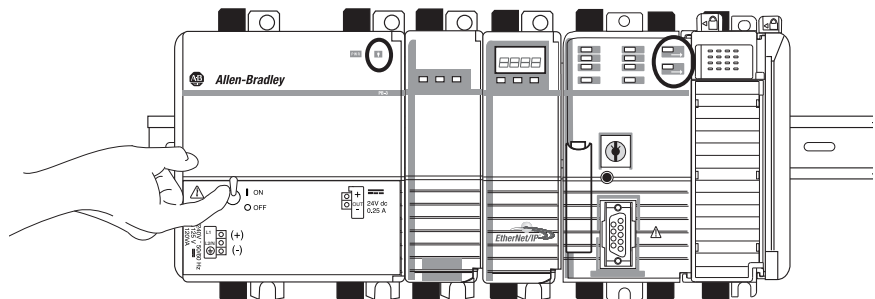
**ATTENTION:** When attaching I/O modules, it is very important that the bus connectors are securely locked together for proper electrical connection.

- Attach the end cap by using the tongue and groove slots (a) and locking the bus lever (b).



## Confirm the Installation

After you have installed the controller and applied power, check that the PWR and I/O PWR status indicators are solid green.



If the indicators are in any other state, see [Troubleshoot System Power on page 120](#).

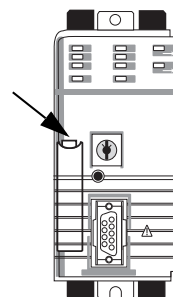
## Insert or Remove a Memory Card



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

Follow these steps to insert or remove a CompactFlash card.

1. Press the memory-card door latch on the controller front panel and pivot the door down toward you.
2. Insert or remove the card from the slot.
3. Close the memory card door.



## Make Communication Connections



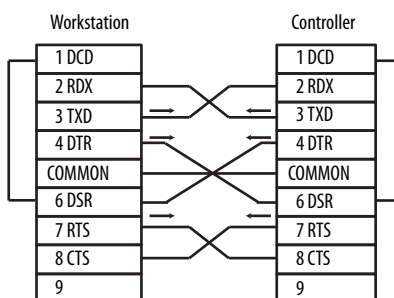
**WARNING:** If you connect or disconnect the serial cable with power applied to this module or the serial device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Make sure that power is removed or the area is nonhazardous before proceeding.

Connect the 1756-CP3 serial cable to the controller's serial port and to your workstation.

If you make your own cable, follow these guidelines.

- Wire the connectors as shown.

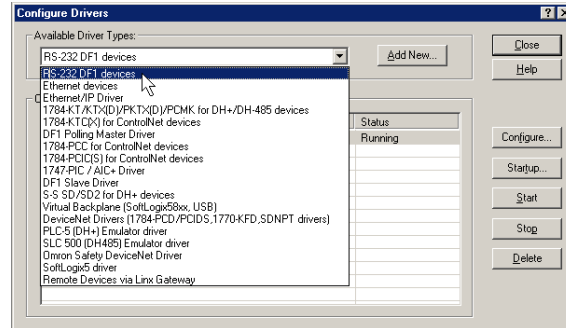


- Limit the cable length to 15.2 m (50 ft).
- Attach the shield to both connectors.

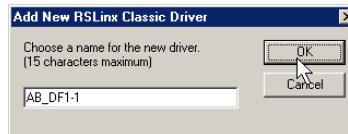


Use RSLinx software to configure the driver for serial communication.

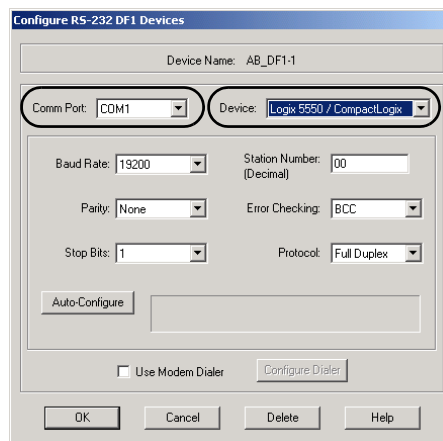
1. From the Communications menu, choose Configure Drivers.
2. From the Available Driver Types pull-down menu, choose the RS-232 DF1 devices driver.



3. Click Add New.
4. Type a name for the driver and click OK.



5. From the Comm Port pull-down menu on the Configure Devices dialog box, choose the serial port on the workstation to which your cable is connected.



6. From the Device pull-down menu, choose Logix5550/CompactLogix.
7. Click Auto-Configure.
  - a. Click OK if the Auto Configuration Successful dialog box appears.
  - b. If the dialog box does not appear, go back to [step 5](#) and verify that you selected the correct comm port.
8. Click Close.

## Update the Controller

The controllers ship without firmware. Controller firmware is packaged with RSLogix 5000 programming software. In addition, controller firmware is also available for download from the Rockwell Automation Technical Support website at: <http://www.rockwellautomation.com/support/>.

---

**IMPORTANT** When installing or updating controller firmware, do not interrupt the update process in any way. Interrupting the firmware update may result in an inoperable controller. Inoperable controllers must be returned to Rockwell Automation.

---

To install firmware, you can use any of the following.

Method	Page
ControlFLASH, version 8 or later, software that ships with RSLogix 5000 software	26
AutoFlash software that runs within RSLogix 5000 software	27
A 1784-CF64 or 1784-CF128 CompactFlash card with valid firmware already loaded	27

Updating your controller firmware via ControlFLASH™ or AutoFlash software requires either a serial or other network connection to the controller.

Updating via an Ethernet connection is faster, but you must first install a 1768-ENBT Ethernet module to connect to the controller via the Ethernet network.

For information on installing, configuring, and operating a 1768-ENBT module, refer to the EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication [ENET-UM001](#).

### Install Firmware via ControlFLASH Software

1. Make sure the network is connected.
2. Start ControlFLASH software.
3. When the Welcome dialog box appears, click Next.
4. Select the catalog number of the controller and click Next.
5. Expand the network until you see the controller.

**TIP** If the required network is not shown, first configure a driver for that network in RSLinx software.

6. Select the controller and click OK.
7. Select the desired revision level and click Next.
8. To start the update, click Finish and then Yes.
9. The OK status indicator flashes red to show that the update is in progress. The status box indicates when the update is complete and the OK status indicator is solid green.
10. Click OK.

11. Click Cancel and then Yes to close ControlFLASH software.

## Install Firmware via AutoFlash Software

1. Make sure the network is connected.
2. Using RSLogix 5000 software, attempt a download to a controller project.
3. AutoFlash software launches if the required firmware is not loaded on the controller.
4. Select the catalog number of the controller and click Next.
5. Expand the network until you see the controller.

**TIP** If the required network is not shown, first configure a driver for that network in RSLinx software.

6. Select the controller and click OK.
7. Select the desired revision level and click Next.
8. To start the update, click Finish and then Yes.
9. The OK status indicator flashes red to show that the update is in progress. The status box indicates when the update is complete and the OK status indicator is solid green.
10. Click OK.
11. Click Cancel and then Yes to close AutoFlash software.

## Install Firmware via a CompactFlash Card

Follow these steps to use RSLogix 5000 software to store the controller program and firmware of an already-configured controller to the CompactFlash card. The firmware is automatically stored on your CompactFlash card when you store the program.

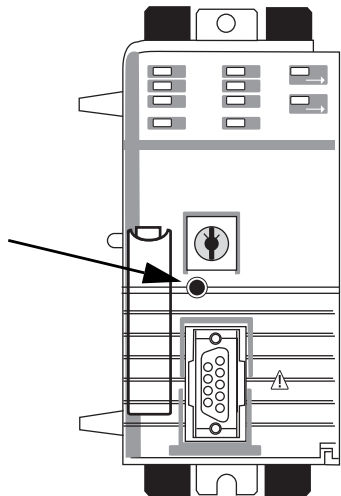
1. With the CompactFlash card installed on the configured controller, on the Controller Properties dialog box, click the Nonvolatile Memory tab.
2. Click Load Image On Powerup to save to the card.
3. Remove the card and insert it into the controller onto which you want to load the firmware and user program.
4. Start the new controller and the image stored on the CompactFlash card loads.

## Faceplate Push Button

On the faceplate of the controller, there is a recessed push button.

**Table 4 - Push Button Actions**

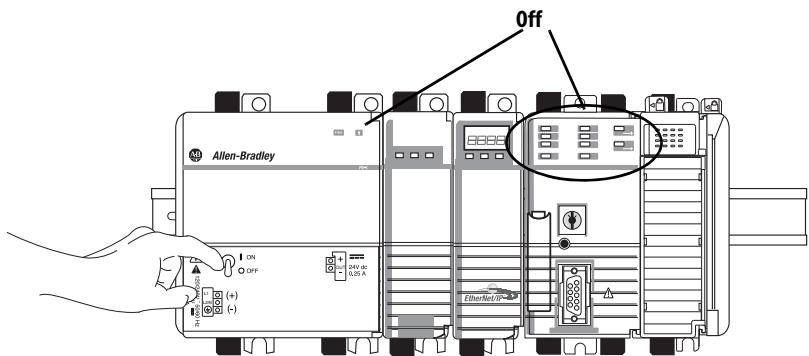
If you access the push button	The action
After power is applied to the controller	Resets the RS-232 configuration setting to the defaults
While the controller is powering up	Clears the user program from controller memory



## Remove a 1768 or 1769 Module from the DIN Rail

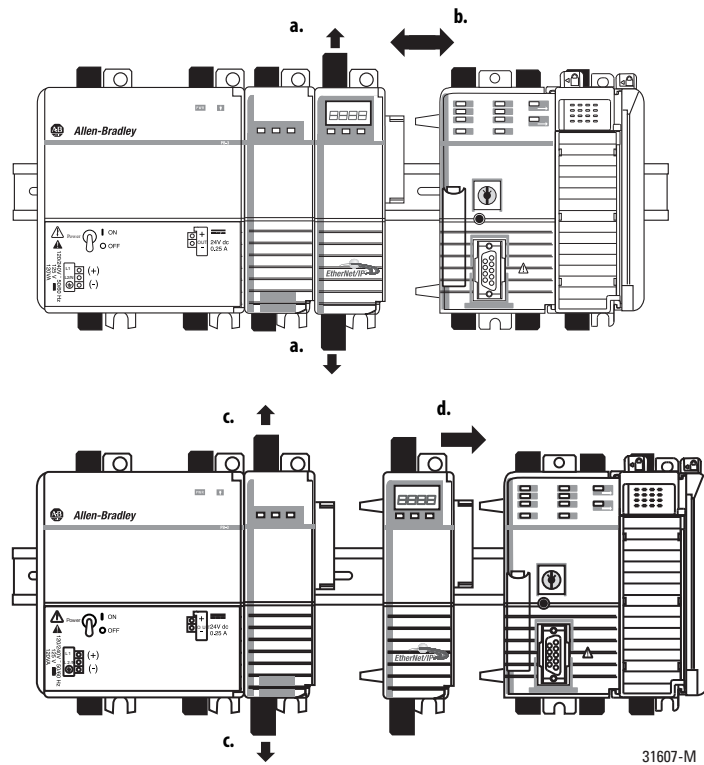
If you need to remove a module from the DIN rail, follow these steps.

1. Remove power from the controller and wait for all status indicators on the power supply and controller to turn off.

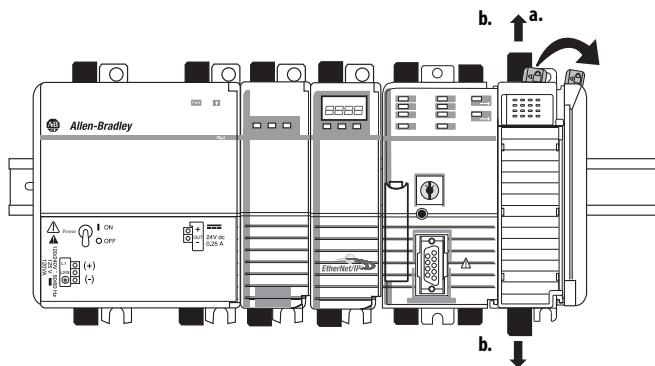


**IMPORTANT** If you disconnect any part of the system while the controller is still writing its program to memory, you will lose your program.

2. Remove the 1768 module.



3. Remove the 1769 module by unlocking the bus lever (a) and DIN rail latches (b).



4. Slide the module away from the DIN rail along the tongue and groove slots.

## **Notes:**

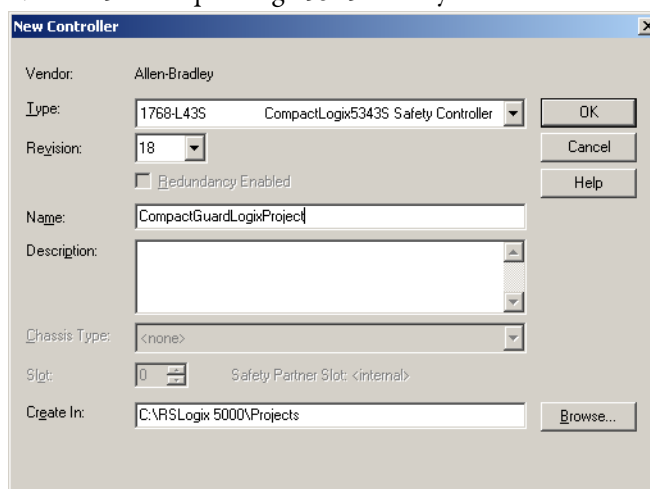
## Configure the Controller

Topic	Page
Create a Controller Project	31
Set Passwords for Safety-locking and -unlocking	33
Handling I/O Module Replacement	35
Enable Time Synchronization	35
Configure a Peer Safety Controller	36

### Create a Controller Project

To configure and program your controller, use RSLogix 5000 software to create and manage a project for the controller.

1. Create a project in RSLogix 5000 software by clicking the New button on the main toolbar.
2. From the Type pull-down menu, choose a Compact GuardLogix controller:
  - 1768-L43S CompactLogix5343S Safety Controller
  - 1768-L45S CompactLogix5345S Safety Controller



3. Enter the major revision of firmware for the controller.
4. Type a name for the controller.

When you create a project, the project name is the same as the name of the controller. However, you can rename either the project or the controller.

5. Specify the folder in which to store the safety controller project.
6. For RSLogix 5000, version 20 or later, choose a Security Authority option.

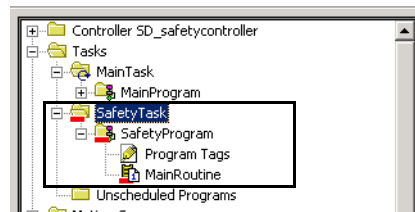
For detailed information on security, refer to the Logix5000 Controllers Security Programming Manual, publication [1756-PM016](#).

7. Click OK.

RSLogix 5000 software automatically creates a safety task and a safety program.

A main ladder logic safety routine called MainRoutine is also created within the safety program.

**Figure 2 - Safety Task in the Controller Organizer**



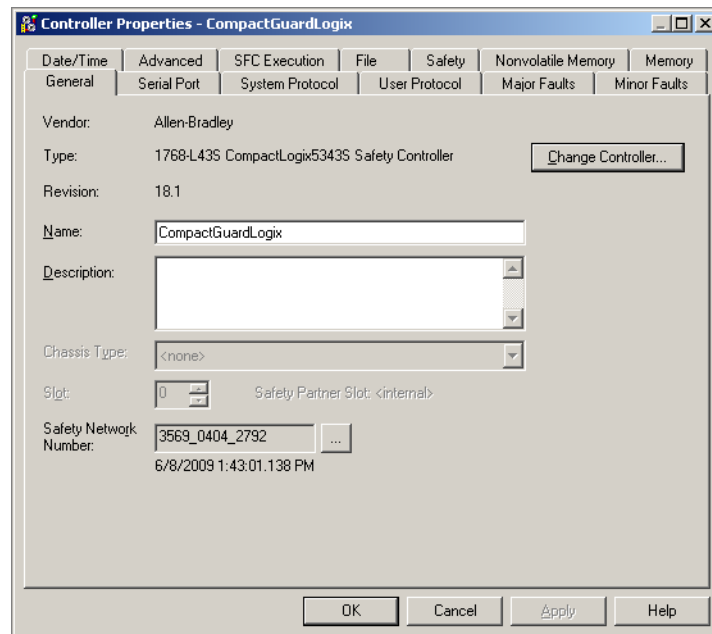
A red bar under the icon distinguishes safety programs and routines from standard project components in the RSLogix 5000 Controller Organizer.

When a new safety project is created, RSLogix 5000 software also automatically creates a time-based safety network number (SNN).

This SNN defines the Compact GuardLogix controller 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 in which you might want to enter a specific SNN.



**Figure 3 - Safety Network Number**

**TIP** You can use the Controller Properties dialog box to change the controller from standard to safety or vice versa by clicking Change Controller. However, standard and safety projects are substantially affected.

See [Appendix B, Change Controller Type in RSLogix 5000 Projects](#), for details on the ramifications of changing controllers.

**Table 5 - Additional Resources**

Resource	Description
<a href="#">Chapter 6, Develop Safety Applications.</a>	Contains more information on the safety task, safety programs, and safety routines
<a href="#">Chapter 4, Communicate over Networks</a>	Provides more information on managing the SNN

## Set Passwords for Safety-locking and -unlocking

Safety-locking the controller helps 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. Choose Tools > Safety > Change Password.
2. From the What Password pull-down menu, choose either Safety Lock or Safety Unlock.

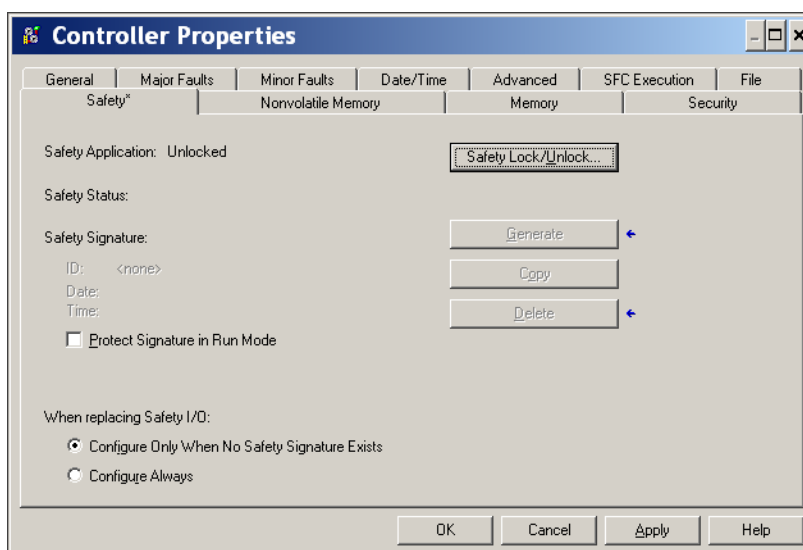


3. Type the old password, if one exists.
4. Type and confirm the new password.
5. Click OK.

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

## Protecting the Safety Task Signature in Run Mode

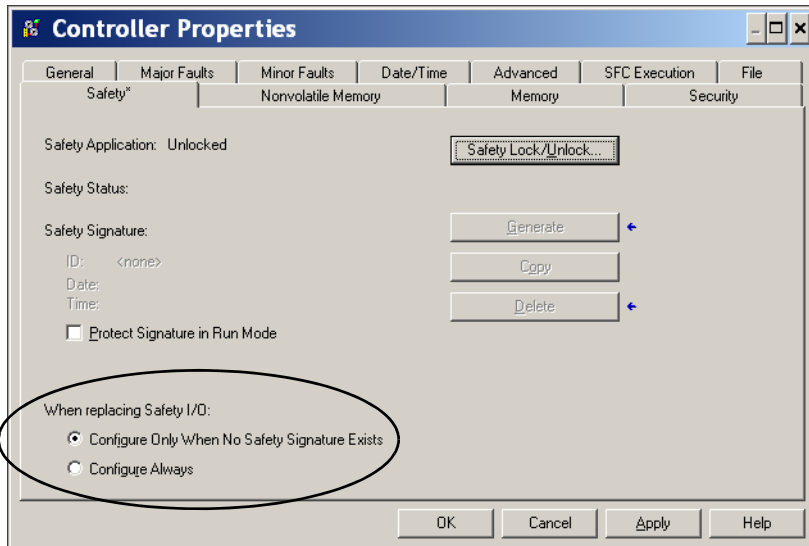
You can prevent the safety task signature from being either generated or deleted while the controller is in Run or Remote Run mode, regardless of whether the safety application is locked or unlocked, by checking Protect Signature in Run Mode on the Safety tab of the Controller Properties dialog box.



## Handling I/O Module Replacement

The Safety tab of the Controller Properties dialog box lets you define how the controller handles the replacement of an I/O module in the system. This option determines whether the controller sets the safety network number (SNN) of an I/O module to which it has a connection and for which it has configuration data when a safety task signature<sup>(1)</sup> exists.

**Figure 4 - I/O Module Replacement Options**



**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 module.

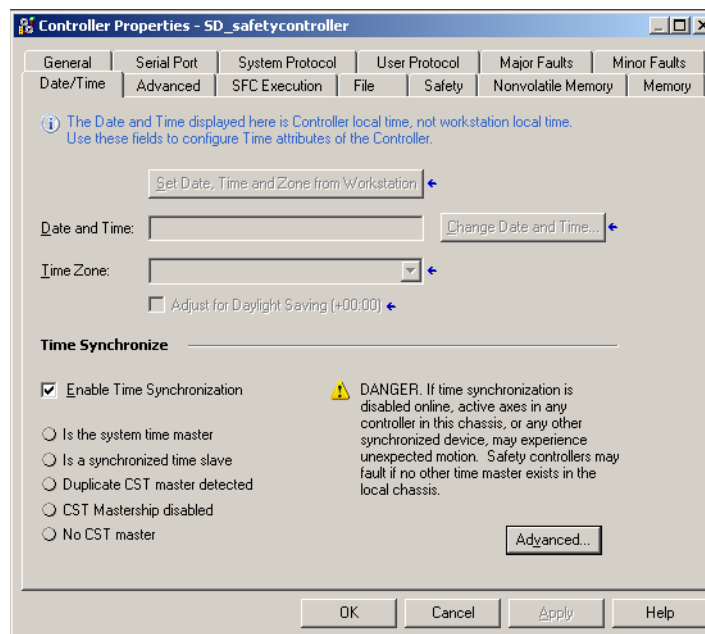
See [Chapter 5, Add, Configure, Monitor, and Replace CIP Safety I/O](#) for more information.

## Enable Time Synchronization

In a Compact GuardLogix controller system, Time Synchronization must be enabled for the controller. To allow the controller to become the CST master, enable Time Synchronization on the Date/Time tab of the Controller Properties dialog box. Time Synchronization provides a standard mechanism to synchronize clocks across a network of distributed devices.

(1) The safety task signature is a number used to uniquely identify each project's logic, data, and configuration, thereby protecting the system's safety integrity level (SIL). See [Safety Task Signature on page 10](#) and [Generate a Safety Task Signature on page 88](#) for more information.

Figure 5 - Date/Time Tab



For more information on Time Synchronization, refer to the Integrated Architecture™ and CIP Sync™ Configuration Application Solution, publication [IA-AT003](#).

## Configure a Peer Safety Controller

You can add a remote 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 details on configuring the peer safety controllers and producing and consuming safety tags, see [Produced/Consumed Safety Tags on page 79](#).

## Communicate over Networks

Topic	Page
The Safety Network	37
EtherNet/IP Communication	43
ControlNet Communication	46
Standard DeviceNet Communication	49
Serial Communication	50
Additional Resources	51

### 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.

### Managing 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.

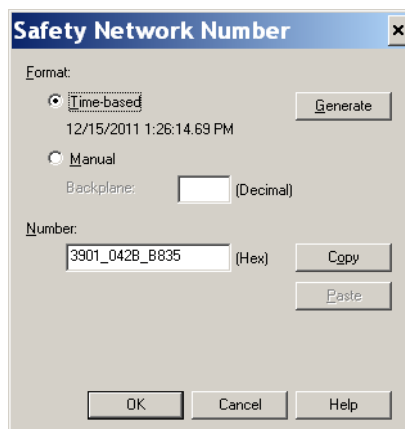
**TIP** Multiple safety network numbers can be assigned to a CIP Safety subnet or a ControlBus chassis that contains more than one safety device. **However, for simplicity, we recommend that each CIP Safety subnet have one, and only one, unique SNN.**

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 Safety Network Number*

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 personal computer running the configuration software.

**Figure 6 - Time-based Format**

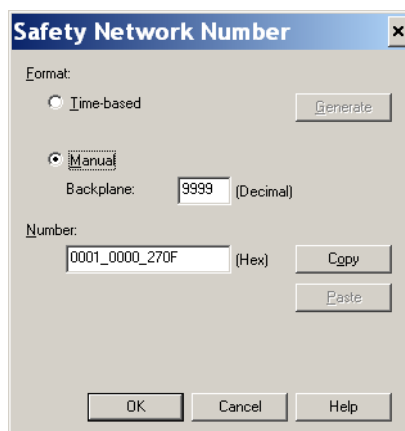


The screenshot shows a dialog box titled "Safety Network Number". Under the "Format:" section, the "Time-based" radio button is selected. Below it, the date and time "12/15/2011 1:26:14.69 PM" are displayed. To the right of this is a "Generate" button. The "Manual" radio button is unselected. Below it, there is a "Backplane:" label followed by an empty text box and the label "(Decimal)". Under the "Number:" section, there is a text box containing "3901\_042B\_B835" followed by the label "(Hex)". To the right of this text box are "Copy" and "Paste" buttons. At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

### *Manual Safety Network Number*

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

**Figure 7 - Manual Entry**



The screenshot shows the same "Safety Network Number" dialog box, but now the "Manual" radio button is selected. The date and time display is gone. The "Backplane:" text box now contains the value "9999" followed by the label "(Decimal)". The "Number:" text box now contains the value "0001\_0000\_270F" followed by the label "(Hex)". The "Generate" button is still present next to the "Time-based" option. The "Copy" and "Paste" buttons are still next to the "Number:" text box. The "OK", "Cancel", and "Help" buttons are at the bottom.

## Assigning the Safety Network Number (SNN)

You can allow RSLogix 5000 software to automatically assign an SNN, 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 interconnecting networks is small, and where users might like to manage and assign the SNN in a logical manner pertaining to their specific application.

See [Changing the Safety Network Number \(SNN\) on page 39](#).

---

**IMPORTANT** If you assign an SNN manually, make sure that system expansion does not result in duplication of SNN and node address combinations.

---

### *Automatic Versus Manual*

For typical users, 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 whose configuration is owned by some other device.
- A safety project is copied to another hardware installation within the same routable CIP Safety system.

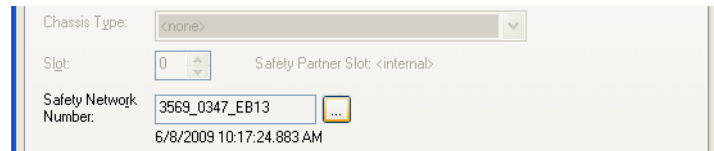
## Changing the Safety Network Number (SNN)

Before changing the SNN you must do the following:

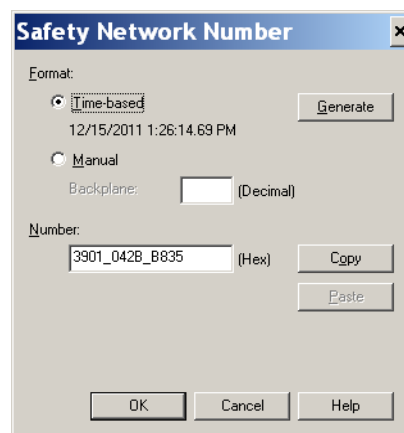
- Unlock the project, if it is safety-locked.  
See [Safety-lock the Controller on page 86](#).
- Delete the safety task signature, if one exists.  
See [Delete the Safety Task Signature on page 89](#).

### *Change the Safety Network Number (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.

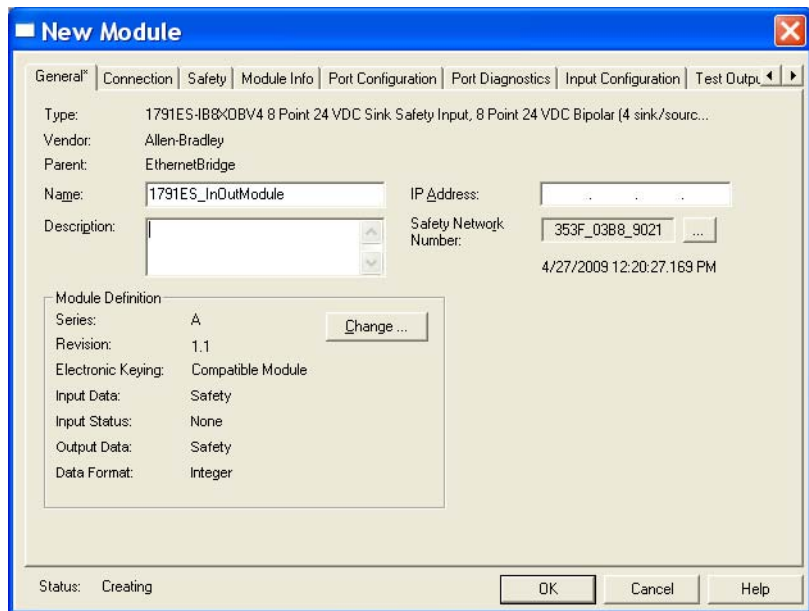
### *Change the Safety Network Number (SNN) of Safety I/O Modules on the CIP Safety Network*



This example uses an EtherNet/IP network.

1. Find the first EtherNet/IP communication module in the I/O Configuration tree.
2. Expand the safety I/O modules available through the EtherNet/IP communication module.



3. Double-click the first safety I/O module to view the General tab.

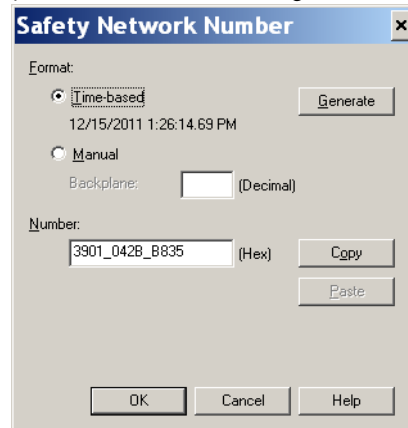



4. Click  to the right of the safety network number to open the Safety Network Number dialog box.
5. Choose Time-based and click Generate to generate a new SNN for that EtherNet/IP network.
6. Click OK.
7. Click Copy to copy the new SNN to the Windows Clipboard.
8. Open the General Tab of the Module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

### *Copy and Paste a Safety Network Number (SNN)*

If the module's configuration is owned by another controller, you may need to copy and paste the SNN from the configuration owner into the module in your I/O configuration tree.

1. In the software configuration tool of the module's configuration owner, 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. Click  to the right of the safety network number to open the Safety Network Number dialog box.
5. Click Paste.
6. Click OK.

## EtherNet/IP Communication

For CIP Safety communication, including Safety I/O module control, choose a 1768-ENBT module, series A, revision 3 or later.

For standard EtherNet/IP communication, choose a 1768-ENBT or 1768-EWEB communication module, series A, revision 3 or later.

EtherNet/IP communication modules provide the following features:

- Support for messaging, produced/consumed tags, HMI, and distributed I/O.
- Encapsulated messages within standard TCP/UDP/IP protocol
- A common application layer with ControlNet and DeviceNet™ networks
- Interface via RJ45, category 5, unshielded, twisted-pair cable
- Support for half/full duplex 10 M or 100 M operation
- Work with standard switches
- No network scheduling required
- No routing tables required

These software products are available for EtherNet/IP networks.

**Table 6 - Software for EtherNet/IP Modules**

Software	Purpose	Required
RSLogix 5000 programming software	This software is required to configure the controller project and define EtherNet/IP communication.	Yes
BOOTP/DHCP utility	This utility comes with RSLogix 5000 software. You can use this utility to assign IP addresses to devices on an EtherNet/IP network.	No
RSNetWorx™ for EtherNet/IP software	You can use this software to configure EtherNet/IP devices by IP addresses and/or host names.	No
RSLinx software	You can use this software to configure devices, establish communication between devices, and provide diagnostics.	Yes

## Producing and Consuming Data via an EtherNet/IP Network

The controller supports the ability to produce (send) and consume (receive) tags over an EtherNet/IP network. Produced and consumed tags each require connections. The total number of tags that can be produced or consumed is limited by the number of available connections.

## Connections over the EtherNet/IP Network

You indirectly determine the number of connections the safety controller uses by configuring the controller to communicate with other devices in the system. Connections are allocations of resources that provide more reliable communication between devices compared to unconnected messages (message instructions).

EtherNet/IP connections are unscheduled. An unscheduled connection is triggered by the requested packet interval (RPI) for I/O control or the program (such as a MSG instruction). Unscheduled messaging lets you send and receive data when needed.

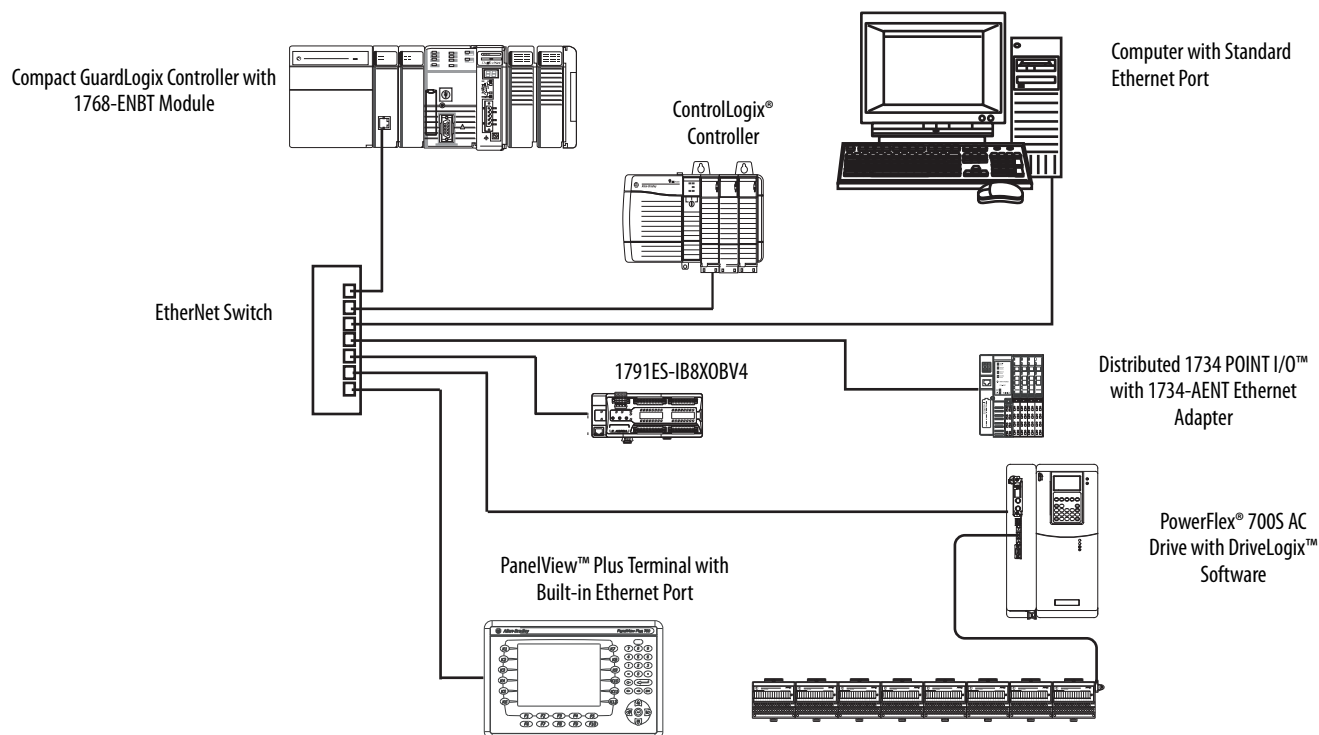
The EtherNet/IP communication modules support 64 Common Industrial Protocol (CIP) connections over an EtherNet/IP network.

## EtherNet/IP Communication Example

This example illustrates the following:

- The controllers can produce and consume standard or safety tags between each other.
- The controllers can initiate MSG instructions that send/receive standard data or configure devices.<sup>(1)</sup>
- The EtherNet/IP communication module is used as a bridge, letting the safety controller produce and consume standard and safety data.
- The personal computer can upload/download projects to the controllers.
- The personal computer can configure devices on the EtherNet/IP network.

**Figure 8 - EtherNet/IP Communication Example**

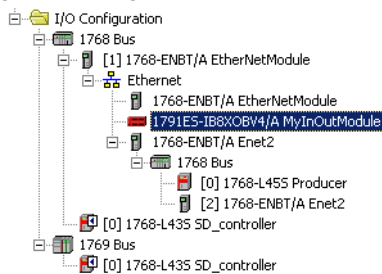


(1) Compact GuardLogix controllers do not support MSG instructions for safety data.

## EtherNet/IP Connections for CIP Safety I/O Modules

CIP Safety I/O modules on EtherNet/IP networks are added to the project under the EtherNet/IP communication module as described in [Chapter 5, Add, Configure, Monitor, and Replace CIP Safety I/O](#). When you add a CIP Safety I/O module, RSLogix 5000 software automatically creates controller-scoped safety data tags for that module.

Figure 9 - Adding EtherNet/IP Modules to the Project



## Standard EtherNet/IP Connections

To use a standard EtherNet/IP module with the safety controller, add the module to the safety controller project and download the project to the Compact GuardLogix controller.

1. To configure the module, define the IP address, subnet mask, and gateway.

EtherNet/IP Parameter	Description
IP Address	The IP address uniquely identifies the module. The IP address is in the form <code>xxx.xxx.xxx.xxx</code> , where each <code>xxx</code> is a number between 0 and 255. However, there are some values that you cannot use as the first octet in the address: <ul style="list-style-type: none"><li>• <code>000.xxx.xxx.xxx</code></li><li>• <code>127.xxx.xxx.xxx</code></li><li>• <code>223...255.xxx.xxx.xxx</code></li></ul>
Subnet Mask	Subnet addressing is an extension of the IP address scheme that allows a site to use one network ID for multiple physical networks. Routing outside of the site continues by dividing the IP address into a net ID and a host ID via the class. Inside a site, the subnet mask is used to redivide the IP address into a custom network ID portion and host ID portion. This field is set to 0.0.0.0 by default.  If you change the subnet mask of an already-configured module, you must cycle power for the change to take effect.
Gateway	A gateway connects individual physical networks into a system of networks. When a node needs to communicate with a node on another network, a gateway transfers the data between the two networks. This field is set to 0.0.0.0 by default.

2. After you physically install an EtherNet/IP module and set its IP address, add the module to the Controller Organizer in your Compact GuardLogix controller project.  
Use RSLogix 5000 software to download the project.

## ControlNet Communication

For ControlNet communication, choose a 1768-CNB module, series A, revision 3 or later.

These software products are available for ControlNet networks.

**Table 7 - Software for ControlNet Modules**

Software	Purpose	Required
RSLogix 5000 programming software	This software is required to configure the GuardLogix project and define ControlNet communication.	Yes
RSNetWorx for ControlNet software	This software is required to configure the ControlNet network, define the network update time (NUT), and schedule the ControlNet network.	Yes
RSLinx software	You can use this software to configure devices, establish communication between devices, and provide diagnostics.	Yes

The ControlNet communication modules provide the following:

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

## Producing and Consuming Data via a ControlNet Network

The Compact GuardLogix controller supports the ability to produce (send) and consume (receive) tags over ControlNet networks. The total number of tags that can be produced or consumed is limited by the number of available connections in the Compact GuardLogix controller.

## Connections over the ControlNet Network

The number of connections the controller uses is determined by how you configure the controller to communicate with other devices in the system. Connections are allocations of resources that provide more reliable communication between devices compared to unconnected messages.

ControlNet connections can be scheduled or unscheduled.

**Table 8 - ControlNet Connections**

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

The 1768-CNB communication modules support 64 CIP connections over a ControlNet network.

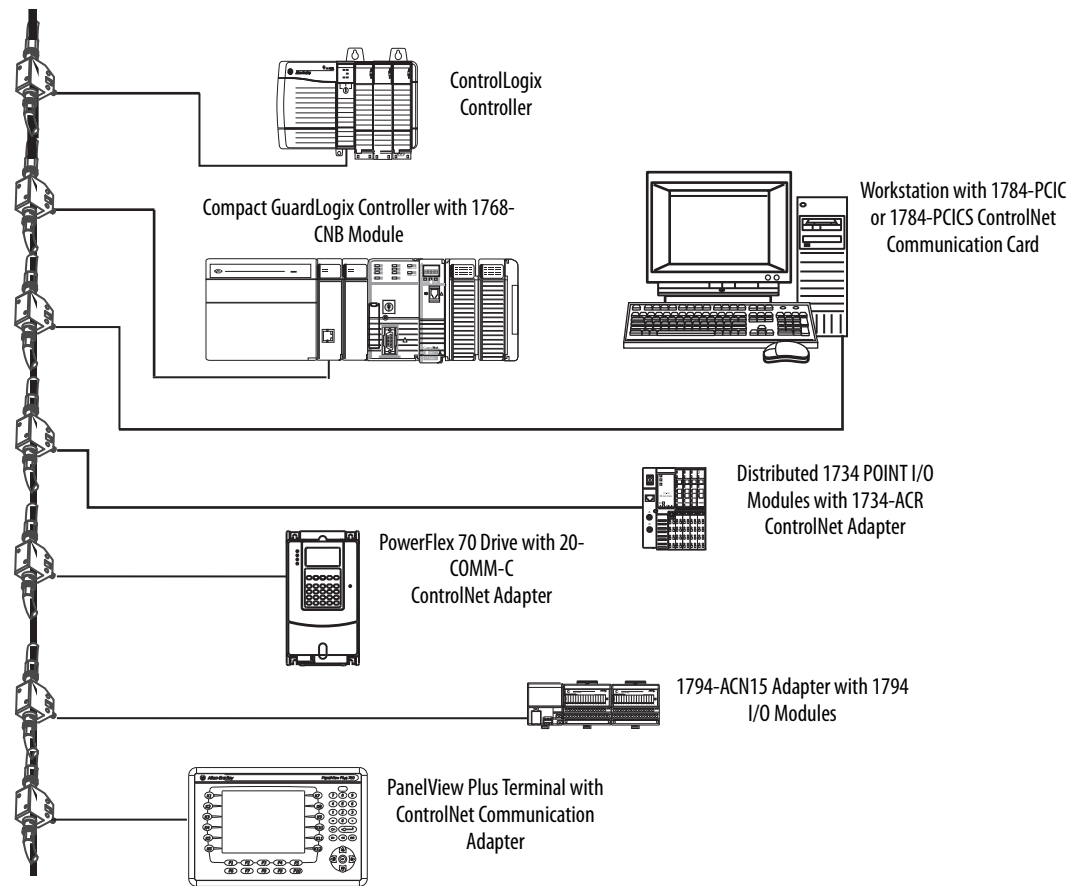
## ControlNet Communication Example

This example illustrates the following:

- Compact GuardLogix controllers can produce and consume standard or safety tags between each other.
- Compact GuardLogix controllers can initiate MSG instructions that send/receive standard data or configure devices.<sup>(1)</sup>
- The 1768-CNB module can be used as a bridge, letting the Compact GuardLogix controller produce and consume standard and safety data to and from I/O devices.
- The personal computer can upload/download projects to the controllers.
- The personal computer can configure devices on the ControlNet network, and it can configure the network itself.

(1) Compact GuardLogix controllers do not support MSG instructions for safety data.

**Figure 10 - ControlNet Communication Example**



## ControlNet Connections for Distributed I/O

To communicate with distributed I/O modules over a ControlNet network, add a 1768-CNB ControlNet bridge, a ControlNet adapter, and I/O modules to the controller's I/O Configuration folder.



## Standard DeviceNet Communication

The DeviceNet network uses the Common Industrial Protocol (CIP) to provide the control, configuration, and data collection capabilities for industrial devices.

A DeviceNet network lets you connect devices directly to plant-floor controllers without having to hardwire each device to an I/O module.

**Table 9 - DeviceNet Interfaces**

Application	Required Interface
<ul style="list-style-type: none"> <li>Communicates with other DeviceNet devices</li> <li>Uses the controller as a master on a DeviceNet network</li> </ul>	1769-SDN DeviceNet scanner
<ul style="list-style-type: none"> <li>Accesses remote Compact I/O™ modules over a DeviceNet network</li> <li>Sends remote I/O data for as many as 30 modules back to a scanner or controller</li> </ul>	1769-ADN DeviceNet adapter <sup>(1)</sup>

(1) This table specifically describes using the 1769-ADN adapter to access remote Compact I/O modules over the DeviceNet network. However, CompactLogix controllers can access other Allen-Bradley remote I/O modules over the DeviceNet network. In those cases, you must select the appropriate interface. For example, if accessing remote POINT I/O modules, you must select the 1734-ADN adapter.

In addition to communication hardware for DeviceNet networks, these software products are available.

**Table 10 - Required Software for DeviceNet Communication**

Software	Functions	Requirement
RSLogix 5000	<ul style="list-style-type: none"> <li>Configure CompactLogix projects.</li> <li>Define DeviceNet communication.</li> </ul>	Yes
RSNetWorx for DeviceNet	<ul style="list-style-type: none"> <li>Configure DeviceNet devices.</li> <li>Define the scan list for those devices.</li> </ul>	
RSLinx	<ul style="list-style-type: none"> <li>Configure communication devices.</li> <li>Provide diagnostics.</li> <li>Establish communication between devices.</li> </ul>	

The DeviceNet communication modules provide the following:

- support messaging to a device, not controller to controller.
- offer diagnostics for improved data collection and fault detection.
- require less wiring than traditional, hardwired systems.

Figure 11 - Standard DeviceNet Communication Example

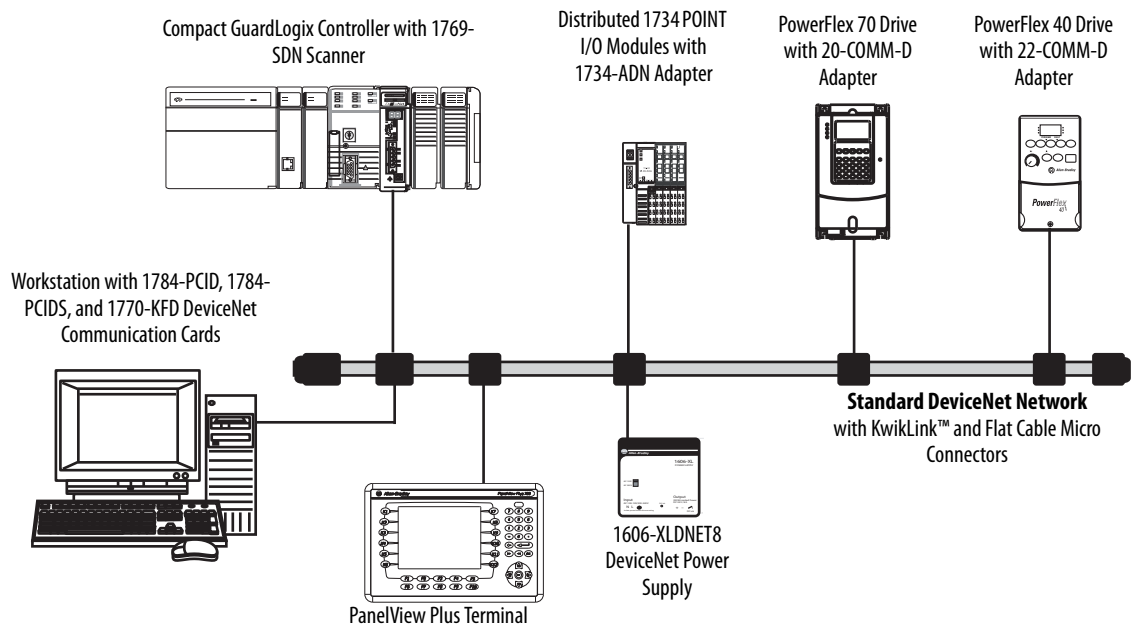


Table 11 - Additional Resources

Resource	Description
Logix5000 Controllers Design Considerations Reference Manual, publication <a href="#">1756-RM094</a>	Provides information pertinent to the design of Logix5000 systems.
DeviceNet Modules in Logix5000 Control Systems User Manual, publication <a href="#">DNET-UM004</a>	Explains how to use DeviceNet modules with Logix5000 controllers.
Logix5000 Controllers Common Procedures Programming Manual, publication <a href="#">1756-PM001</a>	Provides guidelines for the development of programs for Logix5000 controllers.

Serial Communication

To operate the Compact GuardLogix controller on a serial network, you need the following:

- A workstation with a serial port
- RSLinx software to configure the serial communication driver
- RSLogix 5000 software to configure the serial port of the controller

For the controller to communicate to a workstation or other device over the serial network, you must follow these steps.

1. Configure the serial communication driver for the workstation.
2. Configure the serial port of the controller.

**IMPORTANT**    Limit the length of serial (RS-232) cables to 15.2 m (50 ft).

**Table 12 - DF1 Modes for Logix5000 Controllers**

Mode	Functions
DF1 Point-to-Point	<p>Communication between a controller and one other DF1-protocol-compatible device. This is the Default System mode. These are the default parameters:</p> <ul style="list-style-type: none"> <li>• Communication Rate: 19,200 bps</li> <li>• Data Bits: 8</li> <li>• Parity: None</li> <li>• Stop Bits: 1</li> <li>• Control Line: No Handshake</li> <li>• RTS send Delay: 0</li> <li>• RTS Off Delay: 0</li> </ul> <p>This mode is typically used to program a controller through its serial port.</p>
DF1 Master	<ul style="list-style-type: none"> <li>• Control of polling and message transmission between the master and slave nodes.</li> <li>• The master/slave network includes one controller configured as the master node and up to 254 slave nodes. Link slave nodes using modems or line drivers.</li> <li>• A master/slave network can have node numbers from 0...254. Each node must have a unique node address. Also, for your link to be a network, it must consist of one master and one slave station.</li> </ul>
DF1 Slave	<ul style="list-style-type: none"> <li>• A controller to operate as a slave station in a master/slave serial communication network.</li> <li>• When there are multiple slave stations on the network, link slave stations by using modems or line drivers to the master. When you have a single slave station on the network, you do not need a modem to connect the slave station to the master. You can configure the control parameters for no handshaking. You can connect 2...255 nodes to a single link. In DF1 Slave mode, a controller uses DF1 half-duplex protocol.</li> <li>• One node is designated as the master and controls who has access to the link. All of the other nodes are slave stations and must wait for permission from the master before transmitting.</li> </ul>
DF1 Radio Modem	<ul style="list-style-type: none"> <li>• Compatible with SLC 500 and MicroLogix™ 1500 controllers.</li> <li>• This mode supports Master and Slave, and Store and Forward modes.</li> </ul>
User	<ul style="list-style-type: none"> <li>• Communication with ASCII devices.</li> <li>• This requires your program to use ASCII instructions to read and write data from and to an ASCII device.</li> </ul>
DH-485	<ul style="list-style-type: none"> <li>• Communication with other DH-485 devices.</li> <li>• This multi-master, token-passing network permits programming and peer-to-peer messaging.</li> </ul>

## Additional Resources

Resource	Description
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication <a href="#">ENET-UM001</a>	Contains detailed information on configuring and using EtherNet/IP communication modules in a Logix5000 control system
ControlNet Modules in Logix5000 Control Systems User Manual, publication <a href="#">CNET-UM001</a>	Contains detailed information on configuring and using ControlNet communication modules in a Logix5000 control system
DeviceNet Modules in Logix5000 Control Systems User Manual, publication <a href="#">DNET-UM004</a>	Contains detailed information on configuring and using the 1756-DNB in a Logix5000 control system

## **Notes:**

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

Topic	Page
Adding CIP Safety I/O Modules	53
Configure CIP Safety I/O Modules via RSLogix 5000 Software	54
Setting the Safety Network Number (SNN)	55
Using Unicast Connections on EtherNet/IP Networks	55
Setting the Connection Reaction Time Limit	55
Understanding the Configuration Signature	59
Reset Safety I/O Module Ownership	60
Addressing Safety I/O Data	60
Monitor Safety I/O Module Status	61
Resetting a Module to Out-of-box Condition	63
Replacing a Module	63

For more information on installation, configuration, and operation of CIP Safety I/O modules, refer to these resources:

- Guard I/O EtherNet/IP Safety Modules User Manual, publication [1791ES-UM001](#)
- POINT Guard I/O™ Safety Modules Installation and User Manual, publication [1734-UM013](#)
- RSLogix 5000 software online help

### Adding CIP Safety I/O Modules

When you add a module to the system, you must define a configuration for the module, including the following:

- IP address for EtherNet/IP networks  
To set the IP address, you can adjust the rotary switches on the module, use DHCP software, available from Rockwell Automation, or retrieve the default address from nonvolatile memory.
- Safety network number (SNN)  
See page [55](#) for information on setting the SNN.

- Configuration signature

See page [59](#) for information on when the configuration signature is set automatically and when you need to set it.

- Reaction time limit

See page [55](#) for information on setting the reaction time limit.

- Safety input, output, and test parameters

You can configure CIP Safety I/O modules via the Compact GuardLogix controller by using RSLogix 5000 software.

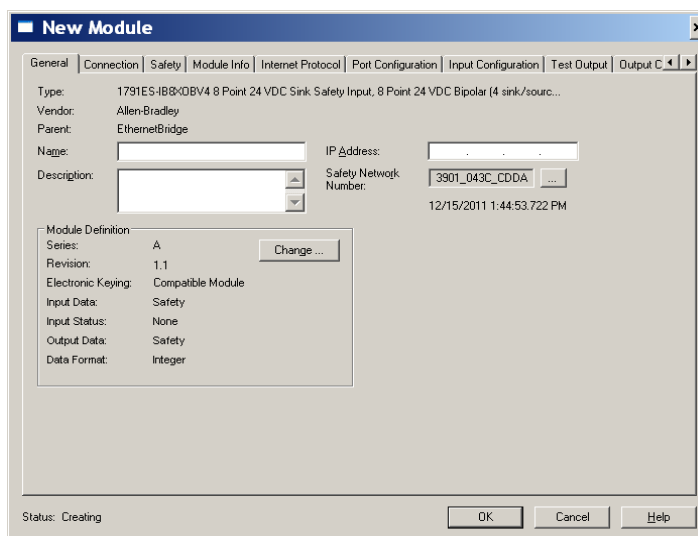
**TIP** Safety I/O modules support standard and safety data. Module configuration defines what data is available.

## Configure CIP Safety I/O Modules via RSLogix 5000 Software

Add the CIP Safety I/O module to the communication module under the I/O Configuration folder of the RSLogix 5000 project. Use a 1768-ENBT module, revision 3 or later, for EtherNet/IP modules.

**TIP** You cannot add or delete a CIP Safety I/O module while online.

1. Right-click the network and choose New Module.
2. Expand the Safety category and choose a CIP Safety I/O module.
3. Specify the module properties.



- a. Modify the Module Definition settings, if required, by clicking Change.
- b. Type a name for the new module.
- c. Enter the IP address of the module on its connecting network.
- d. Modify the safety network number (SNN), if required, by clicking the button.

See page [55](#) for details.

- e. Set module configuration parameters by using the Input Configuration, Test Output, and Output Configuration tabs.

Refer to RSLogix 5000 online help for more information on CIP Safety I/O module configuration.

- f. Set the Connection Reaction Time Limit by using the Safety tab.

See page [55](#) for details.

## Setting the Safety Network Number (SNN)

The assignment of a time-based SNN is automatic when adding new Safety I/O modules. Subsequent safety-module 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 in which manipulation of an SNN is required.

See [Assigning the Safety Network Number \(SNN\) on page 39](#).

## Using Unicast Connections on EtherNet/IP Networks

In RSLogix 5000 software, version 20 or later, you can configure EtherNet/IP I/O modules to use unicast connections. 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.

## Setting the Connection Reaction Time Limit

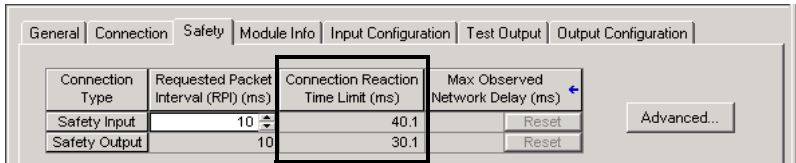
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. The Connection Reaction Time Limit is determined by the following equations:

$$\text{Input Connection Reaction Time Limit} = \text{Input RPI} \times [\text{Timeout Multiplier} + \text{Network Delay Multiplier}]$$

$$\text{Output Connection Reaction Time Limit} = \text{Safety Task Period} \times [\text{Timeout Multiplier} + \text{Network Delay Multiplier} - 1]$$

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

Figure 12 - Connection Reaction Time Limit



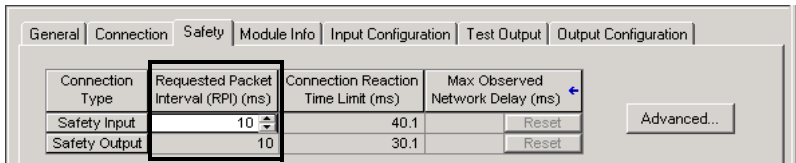
Specify the Requested Packet Interval (RPI)

The RPI specifies the period at which 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 RSLogix 5000 software.

Figure 13 - 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 72](#) 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 57.

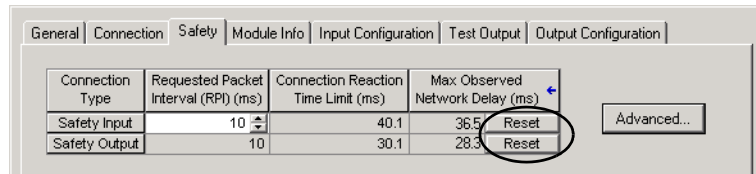
View the Maximum Observed Network Delay

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, you can reset the Maximum Observed Network Delay by clicking Reset.

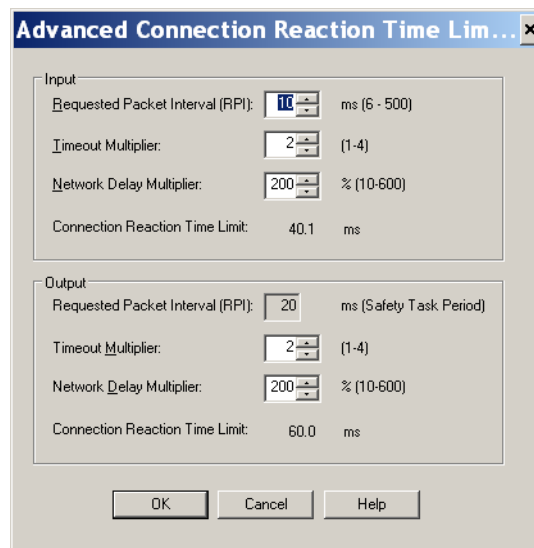
**Figure 14 - Resetting the Max Observed Network Delay**



**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.

## Setting the Advanced Connection Reaction Time Limit Parameters

**Figure 15 - Advanced Configuration**



### *Timeout Multiplier*

The 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 may be lost before a connection error is declared.

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

### *Network Delay Multiplier*

The Network Delay Multiplier defines the message transport time that is enforced by the CIP Safety protocol. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and 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, adjusting the Network Delay Multiplier may be helpful 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 under all of the following conditions:

- 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:

$200\% \times [10 \div 20] = 100\%$

---

**Method 2:** Use the Maximum Observed Network Delay. If the system is run for an extended period of 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 period of time through its worst-case loading conditions, record the Maximum Observed Network Delay.

The Network Delay Multiplier can be approximated by the following equation:

$$[\text{Maximum Observed Network Delay} + \text{Margin\_Factor}] \div \text{RPI}$$

---

**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:

$$[20 + 10] \div 50 = 60\%$$


---

**Table 13 - Additional Resources**

Resource	Description
GuardLogix Controllers Systems Safety Reference Manual, publication <a href="#">1756-RM093</a>	Provides information on calculating reaction times.
Guard I/O EtherNet/IP Safety Modules User Manual, publication <a href="#">1791ES-UM001</a>	

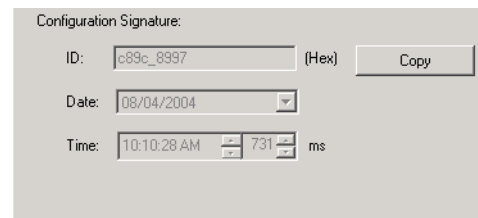
## Understanding the Configuration Signature

Each safety device has a unique configuration signature, which 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 RSLogix 5000 Software

When the I/O module is configured by using RSLogix 5000 software, the configuration signature is generated automatically. You can view and copy the configuration signature via the Safety tab on the Module Properties dialog box.

**Figure 16 - View and Copy the Configuration Signature**



## Different Configuration Owner (listen only connection)

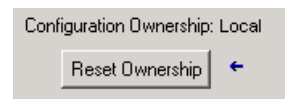
When the I/O module configuration is owned by another controller, you need to copy the module configuration signature from its owner's project and paste it into the Safety tab of the Module Properties dialog box.

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

## Reset Safety I/O Module Ownership

When RSLogix 5000 software 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.

When online, you can reset the module to its out-of-box configuration by clicking Reset Ownership.



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

## Addressing Safety I/O Data

When you add a module to the I/O configuration folder, RSLogix 5000 software automatically creates controller-scoped tags for the module.

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 module. The name of a tag is based on the module's name in the system.

A CIP Safety I/O device address follows this format:

Modulename:Type.Member

**Table 14 - CIP Safety I/O Module Address Format**

Where	Is
Modulename	The name of the CIP Safety I/O module
Type	Type of data
	Input: I
	Output: O
Member	Specific data from the I/O module
	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

**Table 15 - Additional Resources**

Resource	Description
<a href="#">Chapter 8, Monitor Status and Handle Faults</a>	Contains information on monitoring safety tag data
Logix5000 Controllers I/O and Tag Data Programming Manual, publication <a href="#">1756-PM004</a>	Provides information on addressing standard I/O modules

## Monitor Safety I/O Module Status

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

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](#)

**Table 16 - Status Indicator Operation**

Indicator	Status	Description
		<b>EtherNet/IP Modules</b>
Module Status (MS)	Off	No power.
	Green, On	Operating under normal conditions.
	Green, Flashing	Device is idle.
	Red, Flashing	A recoverable fault exists or a firmware update is in progress.
	Red, On	An unrecoverable fault exists.
	Red/Green, Flashing	Self-tests are in progress or the module is not configured properly. See the network status indicator for more information.
Network Status (NS)	Off	Device is not online or may not have power.
	Green, On	Device is online; connections are established.
	Green, Flashing	Device is online; no connections established.
	Red, Flashing	Communication timeout or a firmware update is in progress.
	Red, On	Communication failure. The device has detected an error that has prevented network communication.
	Red/Green, Flashing	Self-test in progress.
Input Points (INx)	Off	Safety input is OFF.
	Yellow, On	Safety input is ON.
	Red, On	An error has occurred in the input circuit.
	Red, Flashing	When dual-channel operation is selected, an error has occurred in the partner input circuit.
Output Points (Ox)	Off	Safety output is OFF.
	Yellow, On	Safety output is ON.
	Red, On	An error has occurred in the output circuit.
	Red, Flashing	When dual-channel operation is selected, an error has occurred in the partner output circuit.
IN PWR	Green, Off	No input power.
	Green, On	Input power voltage is within specification.
	Yellow, On	Input power voltage is out of specification.
OUT PWR	Green, Off	No output power.
	Green, On	Output power voltage is within specification.
	Yellow, On	Output power voltage is out of specification.
Test Output Points (Tx)	Off	The output is OFF.
	Yellow, On	The output is ON.
	Red, On	An error has occurred in the output circuit.

## Resetting a Module to Out-of-box Condition

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

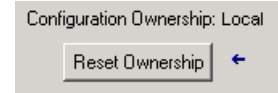
When RSLogix 5000 software is online, the Safety tab of the Module Properties dialog box displays the current configuration ownership. When the opened project owns the configuration, Local is displayed. When a second device owns the configuration, Remote is displayed, along with the safety network number (SNN), and node address or slot number of the configuration owner. Communication error is displayed if the module read fails.

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

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

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

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



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

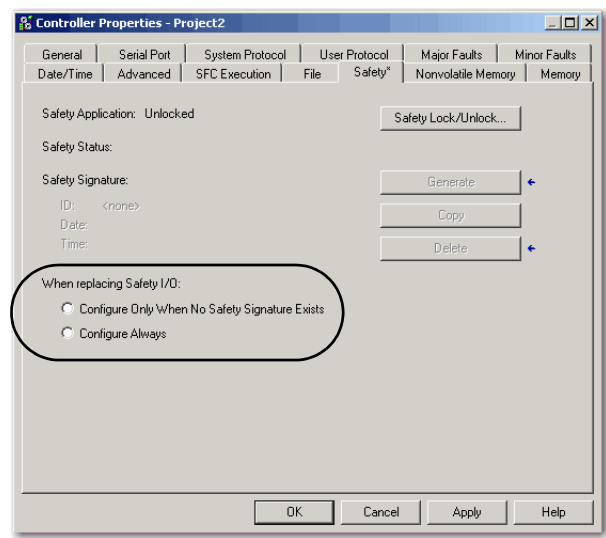
## Replacing a Module

If you are relying on a portion of the CIP Safety system to maintain SIL 3 behavior during module replacement and functional testing, the Configure Always feature may not be used. Go to [Replacement with 'Configure Only' When No Safety Signature Exists' Enabled on page 64](#).

If the entire routable CIP Safety control system is not being relied on to maintain SIL 3/PLC during the replacement and functional testing of a module, the Configure Always feature may be used. Go to [Replacement with 'Configure Always' Enabled on page 68](#).

Module replacement is configured on the Safety tab of the Compact GuardLogix controller.

Figure 17 - Safety I/O Module Replacement



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

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


If the project is configured as ‘Configure Only When No Safety Signature Exists’, follow the appropriate steps in [Table 17](#) to replace a POINT Guard I/O module based on your scenario. Once you have completed the steps correctly, the DeviceID will match the original, enabling the safety controller to download the proper module configuration, and re-establish the safety connection.

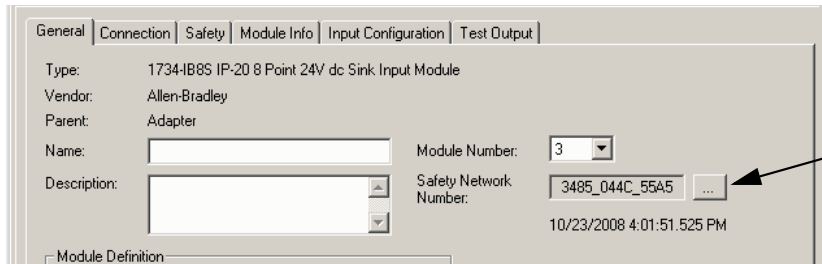
Table 17 - Replacing a Module

GuardLogix Safety Signature Exists	Replacement Module Condition	Action Required
No	No SNN (Out-of-box)	None. The module is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The module is ready for use.
Yes	No SNN (Out-of-box)	<a href="#">See Scenario 1 - Replacement Module is Out-of-box and Safety Signature Exists on page 65.</a>
Yes	Different SNN from original safety task configuration	<a href="#">See Scenario 2 - Replacement Module SNN is Different from Original and Safety Signature Exists on page 66.</a>
No		<a href="#">See Scenario 3 - Replacement Module SNN is Different from Original and No Safety Signature Exists on page 68.</a>

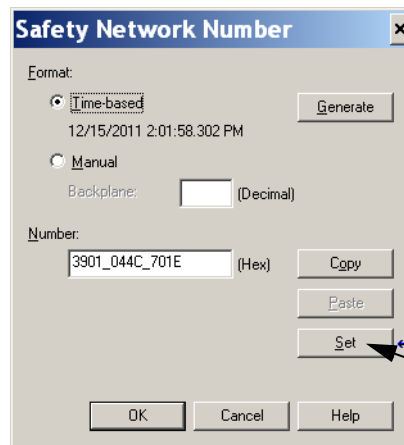


*Scenario 1 - Replacement Module is Out-of-box and Safety Signature Exists*

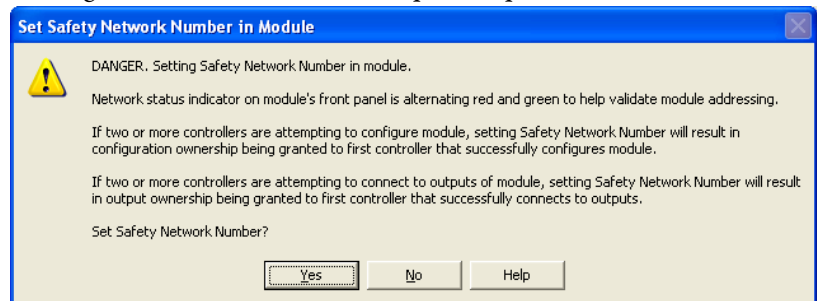
1. Remove the old I/O module and install the new module.
2. Right-click the replacement POINT Guard I/O module and choose Properties.
3. Click  to the right of the safety network number to open the Safety Network Number dialog box.



4. Click Set.



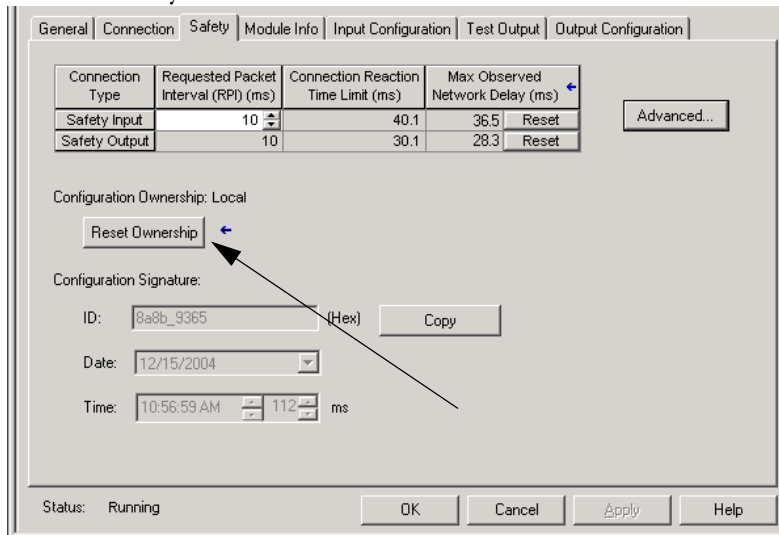
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct module before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement module.



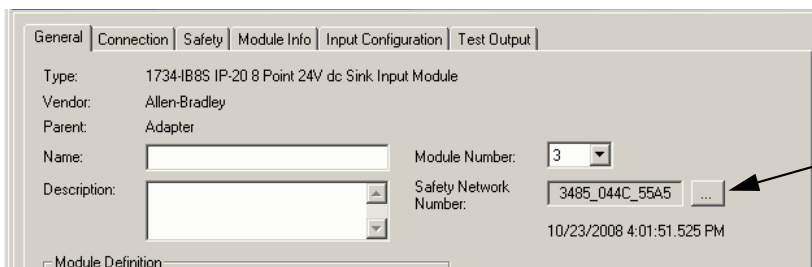
6. Follow your company-prescribed procedures to functionally test the replaced I/O module and system and to authorize the system for use.

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

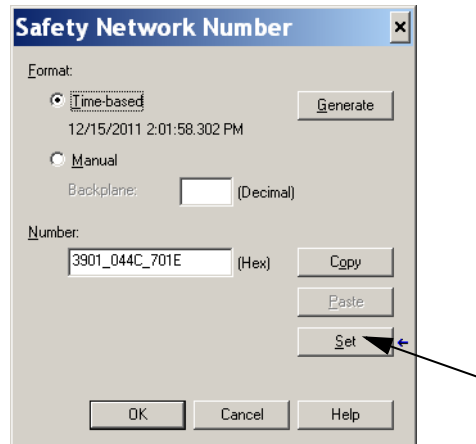
1. Remove the old I/O module and install the new module.
2. Right-click your POINT Guard I/O module and choose Properties.
3. Click the Safety tab.



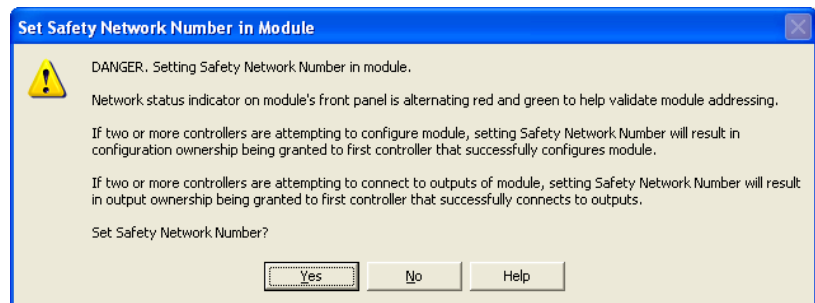
4. Click Reset Ownership.
5. Click OK.
6. Right-click your controller and choose Properties.
7. Click ... to the right of the safety network number to open the Safety Network Number dialog box.



8. Click Set.



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



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

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

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

The screenshot shows the 'Safety' tab of the 'Properties' dialog for a POINT Guard I/O module. The 'General' tab is selected, showing a table with the following data:

Connection Type	Requested Packet Interval (RPI) (ms)	Connection Reaction Time Limit (ms)	Max Observed Network Delay (ms)	
Safety Input	10	40.1	36.5	Reset
Safety Output	10	30.1	28.3	Reset

Below the table, there is a 'Reset Ownership' button. An arrow points to this button. The 'Configuration Signature' section shows the ID as '8a8b\_9365' (Hex), the Date as '12/15/2004', and the Time as '10:56:59 AM' with a '112' ms delay. The 'Status' is 'Running'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

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

### Replacement with 'Configure Always' Enabled



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

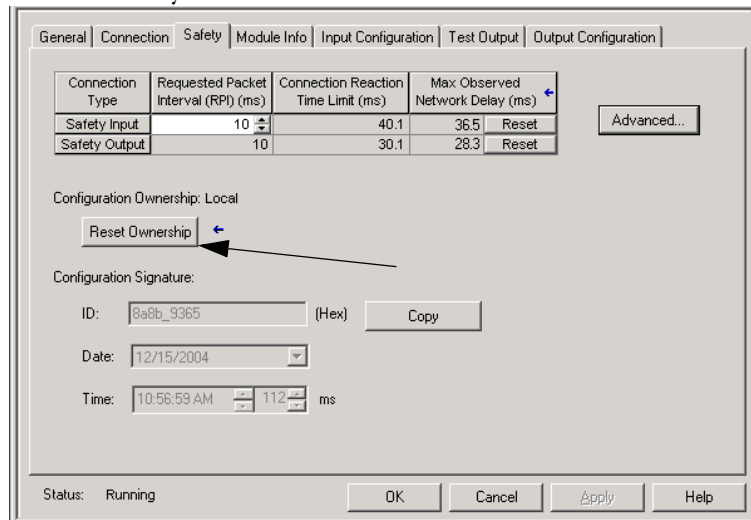
Do not place modules that are in the out-of-box condition on a CIP Safety network when the Configure Always feature is enabled, except while following this replacement procedure.

When the 'Configure Always' feature is enabled in RSLogix 5000 software, the controller automatically checks for and connects to a replacement module that meets all of the following requirements:

- The controller has configuration data for a compatible module at that network address.
- The module 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 POINT Guard I/O module.

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



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

## **Notes:**

## Develop Safety Applications

Topic	Page
The Safety Task	72
Safety Programs	74
Safety Routines	74
Safety Tags	74
Produced/Consumed Safety Tags	79
Safety Tag Mapping	84
Safety Application Protection	86
Software Restrictions	89

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

For guidelines and requirements for developing and commissioning SIL 3 and PLe safety applications, refer to the GuardLogix Controller Systems Safety Reference Manual, publication [1756-RM093](#).

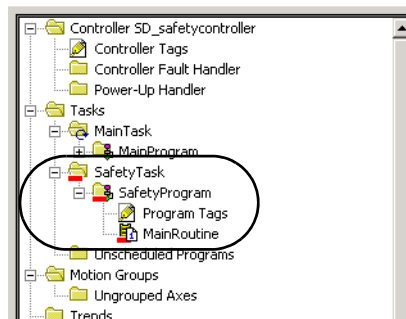
The Safety Reference Manual addresses the following:

- Creating a detailed project specification
- Writing, documenting, and testing the application
- Generating the safety task signature to identify and protect the project
- Confirming the project by printing or displaying the uploaded project and manually comparing the configurations, safety data, and safety program logic
- Verifying the project through test cases, simulations, functional verification tests, and an independent safety review, if required
- Locking the safety application
- Calculating system reaction time

## The Safety Task

When you create a safety controller project, RSLogix 5000 software automatically creates a safety task with a safety program and a main (safety) routine.

**Figure 18 - Safety Task in the Controller Organizer**



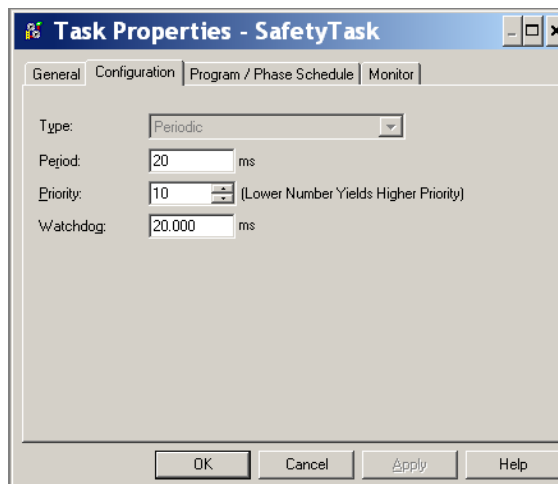
Within the safety task, you can use multiple safety programs, composed of multiple safety routines. The Compact GuardLogix controller supports one safety task. The safety task cannot be deleted.

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. You select the task priority and watchdog time via the Task Properties - Safety Task dialog box. Open the dialog box by right-clicking the Safety Task and choosing Properties.

**Figure 19 - Configuring the Safety Task Period**





The safety task should be 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 at which the safety task executes. The safety task watchdog is the maximum time allowed from the start of safety task execution to its completion.

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

The safety task period directly affects system reaction time.

The GuardLogix Controller Systems Safety Reference Manual, publication [1756-RM093](#), provides detailed information on calculating system reaction time.

## 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 internal 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 [84](#) for information on safety tag mapping.

- Safety output tag (output and produced) values are updated at the conclusion of safety task execution.

## Safety Programs

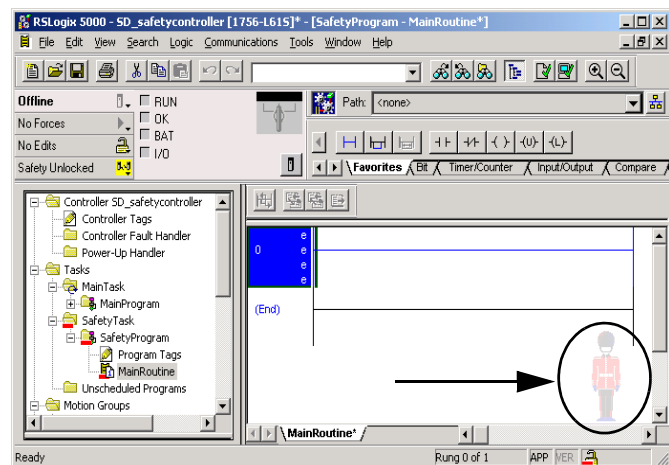
Safety programs have all the attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines, one of which must be designated as the main routine, and one of which may be designated as 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. At this time, only ladder diagram is supported for safety routines.

**TIP** RSLogix 5000 software uses a watermark feature to visually distinguish 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 for allocating memory, referencing data from logic, and monitoring data. Safety tags have all the attributes of standard tags with the addition of mechanisms 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 should be a constant.

To create a safety tag, open the New Tag dialog box by right-clicking Controller Tags or Program Tags and choosing New Tag.

**Figure 20 - Creating a New Tag**

## Tag Type

[Table 18](#) defines the four types of tags: base, alias, produced, and consumed.

**Table 18 - Four Tag Types**

Tag Type	Description
Base	These tags store values for use by logic within the project.
Alias	<p>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.</p> <p><b>IMPORTANT:</b> Aliasing between standard and safety tags is prohibited in safety applications. Instead, standard tags can be mapped to safety tags using safety tag mapping. See <a href="#">Safety Tag Mapping on page 84</a>.</p>
Produced	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 using logic. Produced tag data is sent at the RPI of the consuming tag.
Consumed	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 at which 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.

Only these data types are permitted for safety tags.

**Table 19 - 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

---

**IMPORTANT** This restriction includes user-defined data types that contain predefined data types.

---

## 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:

- More than one program in the project
  - To produce or consume data
  - To communicate with a PanelView/HMI terminal
  - In safety tag mapping
- See [Safety Tag Mapping on page 84](#) 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 associated with Safety I/O and produced or consumed safety data must be controller-scoped safety tags. For produced/consumed safety tags, you must create a user-defined data type with the first member of the tag structure reserved for the status of the connection. This member is a predefined data type called CONNECTION\_STATUS.

**Table 20 - Additional Resources**

Resource	Description
<a href="#">Safety Connections</a> on page <a href="#">103</a>	Provides more information on the CONNECTION_STATUS member
Logix5000 Controllers I/O and Tag Data Programming Manual, publication <a href="#">1756-PM004</a>	Provides instructions for creating user-defined data types

### *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.

Safety-program-scoped safety tags can only be read by or written to via a safety routine scoped in the same safety program.

## 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

When you designate a tag as a constant value, it cannot be modified by logic in the controller, or by an external application such as an HMI. Constant value tags cannot be forced.

RSLogix 5000 software 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 RSLogix 5000 software is not affected by this setting. The default value is read/write.

**Table 21 - External Access Levels**

External Access Setting	Description
None	Tags are not accessible from outside the controller.
Read Only	Tags may be browsed or read, but not written to from outside the controller.
Read/Write	Standard tags may 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 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 in version 19 and later of RSLogix 5000 software.

**Table 22 - Produced and Consumed Connections**

Tag	Connection Description
Produced	A Compact GuardLogix controller can produce (send) safety tags to other 1756 or 1768 GuardLogix controllers. The producing controller uses a single connection for each consumer.
Consumed	Compact GuardLogix controllers can consume (receive) safety tags from other 1756 or 1768 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 properly configure produced and consumed safety tags to share data between peer safety controllers, you must properly configure the peer safety controllers, produce a safety tag, and consume a safety tag, as described below.

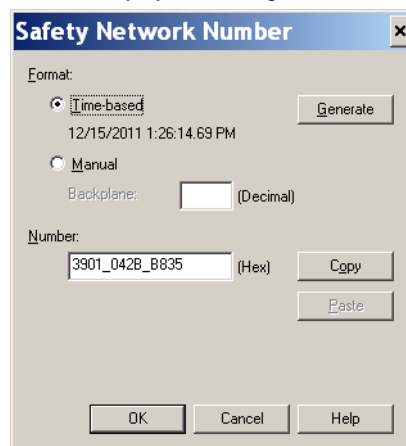
### Configure the Peer Safety Controllers' Safety Network Numbers

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.

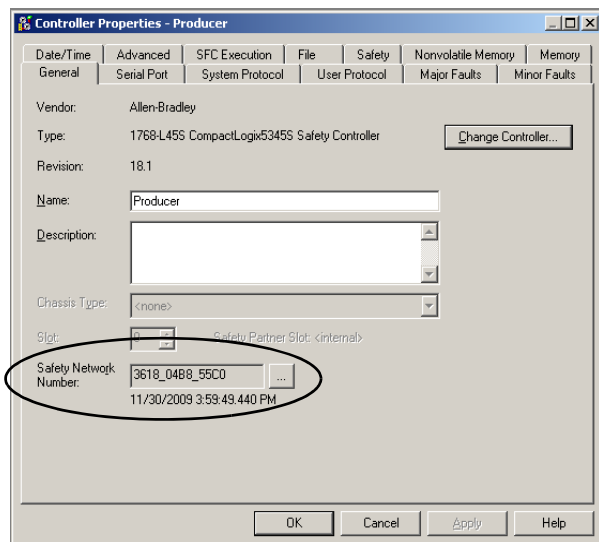
1. Add the producer controller to the consumer controller's I/O tree.
2. In the producer controller's project, right-click the producer controller and choose Controller Properties.
3. Copy the producer controller's SNN.

**TIP** An SNN can be copied and pasted by using the buttons on the Safety Network Number dialog box. Open the respective Safety Network Number dialog boxes by clicking  to the right of the SNN fields in the properties dialog boxes.

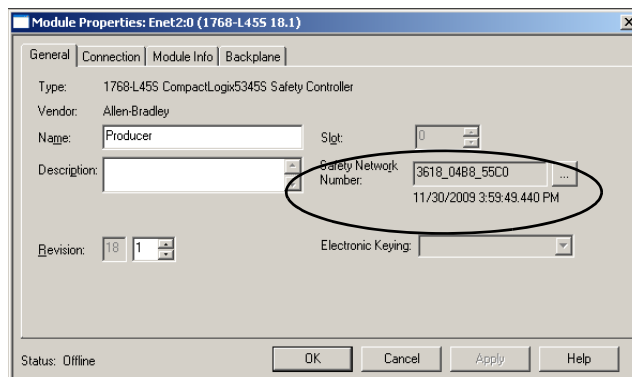


4. In the consumer controller's project, right-click the producer controller and choose Module Properties.
5. Paste the producer controller's SNN into the SNN field.

Producer Controller Properties Dialog Box in Producer Project



Module Properties Dialog Box in Consumer Project

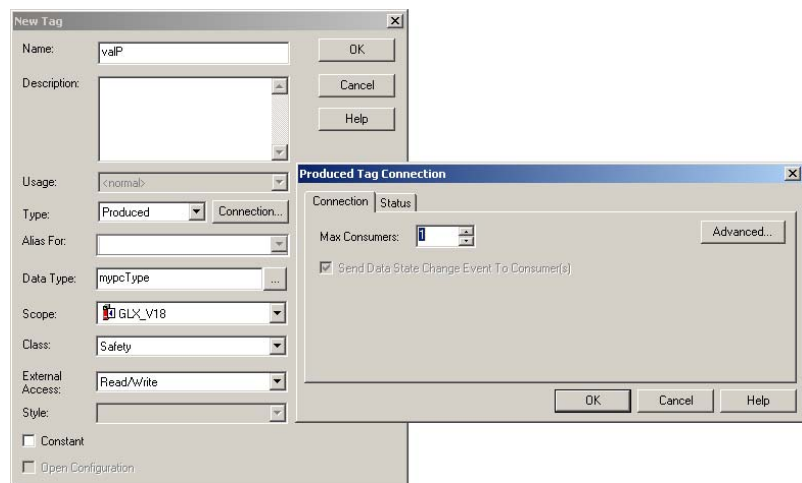




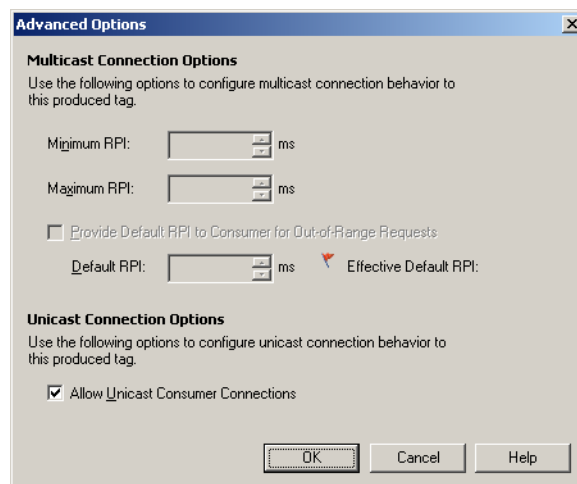
## Produce a Safety Tag

Follow this procedure to produce a safety tag.

1. In the producing controllers project, create a user-defined data type defining the structure of the data to be produced.  
Make sure that the first data member is of the CONNECTION\_STATUS data type.
2. Right-click Controller Tags and choose New Tag.
3. Set the type as Produced, the class as Safety, and the Data Type to the user-defined type you created in step 1.
4. Click Connection and enter the number of consumers.



5. Click Advanced if you want to change the type of connection by unchecking 'Allow Unicast Consumer Connections'.



6. Click OK.

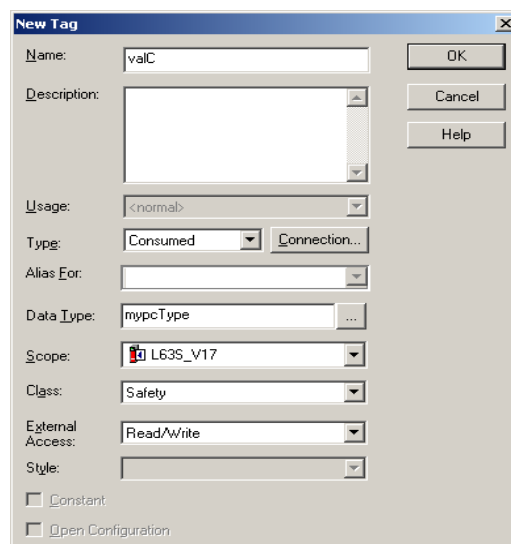
## Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

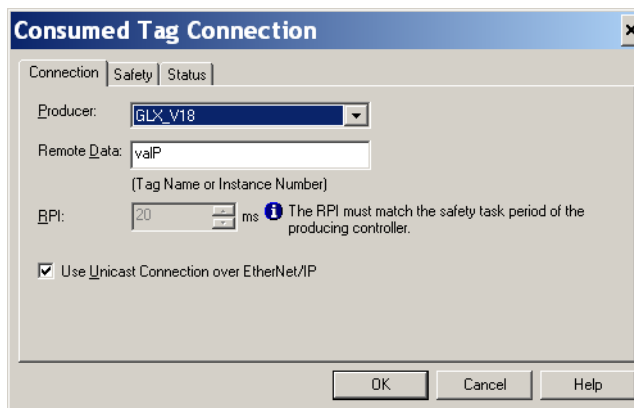
1. In the consumer controller's project, create a user-defined data type identical to the one created in the producer project.

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

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



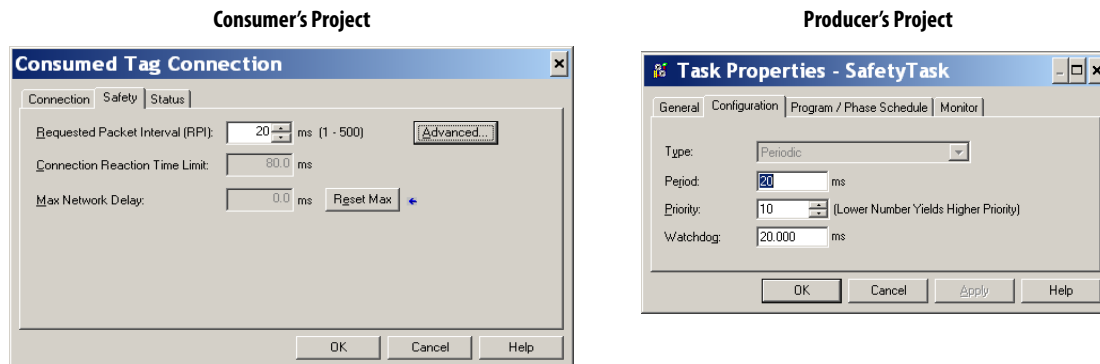
4. Click Connection to open the Consumed Tag Connection dialog box.



5. Select the controller that produces the data.
6. Enter the name of the produced tag.
7. Click the Safety tab.

8. Enter the requested packet interval (RPI) for the connection in 1 ms increments.

The default is 20 ms.

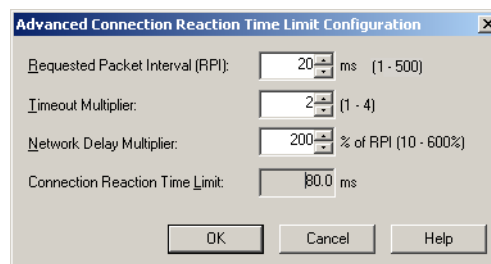


The RPI specifies the period at which data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.

The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, an acceptable Connection Reaction Time Limit can be achieved 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. When online, you can reset the Max Network Delay by clicking Reset Max.

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 is enforced by the CIP Safety protocol. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and back to the producer. You can use the Network Delay Multiplier to increase or decrease the Connection Reaction Time Limit.

**Table 23 - Additional Resources**

Resource	Description
Pages <a href="#">55</a> ... <a href="#">59</a>	Provides more information on setting the RPI and understanding how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time
<a href="#">Chapter 8</a>	Contains information on the CONNECTION_STATUS predefined data type
Logix5000 Controllers Produced and Consumed Tags Programming Manual, publication <a href="#">1756-PM011</a>	Provides detailed information on using produced and consumed tags

## Safety Tag Mapping

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

### Restrictions

Safety tag mapping is subject to these restrictions:

- The safety tag and standard tag pair must be controller-scoped.
- The data types of the safety and standard tag pair must match.
- Alias tags are not allowed.
- Mapping must take place at the whole tag level. For example, myTimer.pre is not allowed if myTimer is a TIMER tag.
- A mapping pair is one standard tag mapped to one safety tag.
- You may not 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.

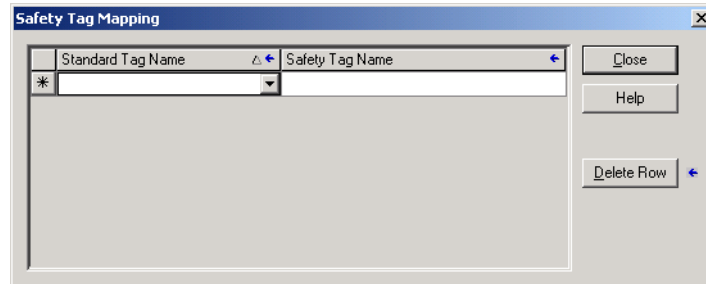


**ATTENTION:** When using standard data in a safety routine, you are responsible for providing a reliable means of ensuring that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 3/PL safety output with standard tag data.

Refer to the GuardLogix Controller Systems Safety Reference Manual, publication [1756-RM093](#), for more information.

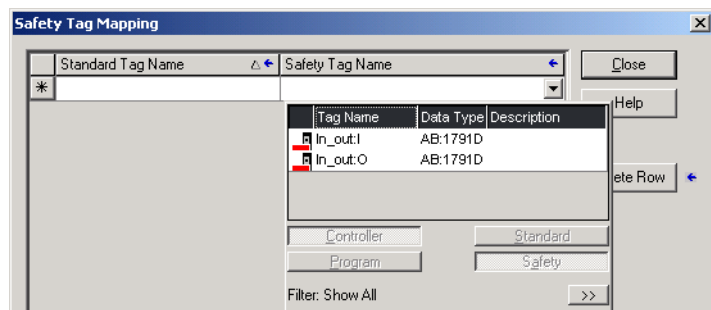
## Create Tag Mapping Pairs

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



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

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







3. Add a new tag to the Standard Tag Name or Safety Tag Name column by right-clicking in the empty cell and selecting New Tag and typing the tag name into the cell.
4. Right-click in the cell and choose New tagname, where tagname is the text you entered in the cell.

## Monitor Tag Mapping Status

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

**Table 24 - 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. <sup>(1)</sup> When online, an invalid tag map results in an error message explaining why the mapping is invalid. You cannot move to another row or close the Safety Tag Mapping dialog box if a tag mapping error exists.
	Indicates the row that currently has the focus.
	Represents the Create New Mapped Tag row.
	Represents a pending edit.

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

For more information, see the tag mapping restrictions on page [84](#).

## Safety Application Protection

You can protect your application program from unauthorized changes by safety-locking the controller and by generating and recording the safety task signature.

### Safety-lock the Controller

The Compact GuardLogix controller can be Safety-locked to 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:

- Online/offline programming or editing (including safety Add-On Instructions)
- Forcing Safety I/O
- Changing the inhibit state of Safety I/O or produced connections
- Safety data manipulation (except by safety routine logic)
- Generating or deleting the safety task signature

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



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

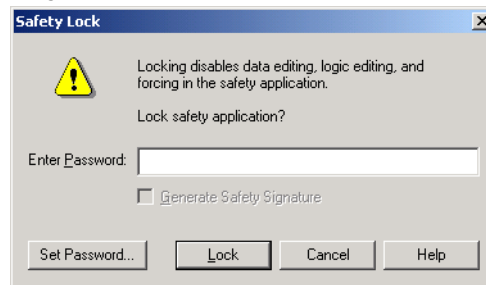
-  = controller safety-locked
-  = controller safety-unlocked

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 may be present.

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

You can Safety-lock and -unlock the controller from the Safety tab of the Controller Properties dialog box or by choosing Tools>Safety>Safety Lock/Unlock.

**Figure 21 - Safety-locking the Controller**



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 page [33](#).

The safety-lock feature, described in this section, and standard RSLogix™-security measures are applicable to Compact GuardLogix controller applications.

Refer to the Logix5000 Controllers Security Programming Manual, publication [1756-PM016](#), for information on RSLogix 5000 Security features.

## Generate a Safety Task Signature

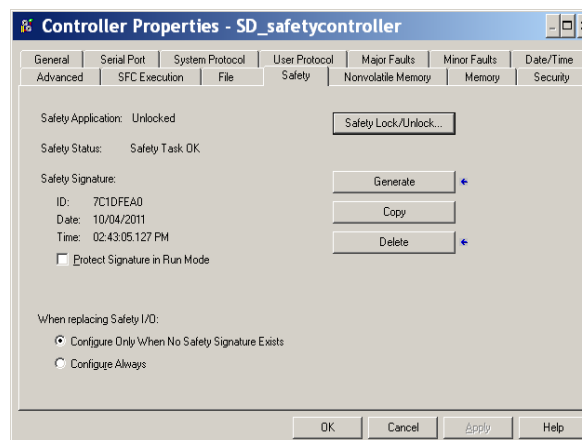
Before verification testing, you must generate the safety task signature. You can generate the safety task signature only when online with the safety-unlocked Compact GuardLogix controller in Program mode, and with no safety forces, pending online safety edits, or safety faults. The safety status must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

**TIP** You can view the safety status via the safety status button on the online bar (see page 102) or on the Safety tab of the Controller Properties dialog box, as shown on page 88.

You can generate the safety task signature from the Safety tab of the Controller Properties dialog box by clicking Generate. You can also choose Tools>Safety>Generate Signature.

**Figure 22 - Safety Tab**



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

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

- Online/offline programming or editing (including safety Add-On Instructions)
- Forcing Safety I/O
- Changing 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.

Refer to the GuardLogix Controller Systems Safety Reference Manual, publication [1756-RM093](#), for more information on SIL 3/PLe requirements.

---

## Software Restrictions

Restrictions limiting the availability of some menu items and features (that is, cut, paste, delete, search and replace) are imposed by the programming software to protect safety components from being modified whenever the following is true:

- The controller is safety-locked.
- A safety task signature exists.
- Safety faults are present.
- A non-recoverable safety fault is present.

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

- Create or modify safety objects, including safety programs, safety routines, safety tags, safety Add-On Instructions, and Safety I/O modules.

---

**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, slot, and safety network number.
- Modify or delete the safety task signature, when safety-locked.

## **Notes:**

## Go Online with the Controller

Topic	Page
Connecting the Controller to the Network	91
Configuring the Network Driver	92
Understanding the Factors that Affect Going Online	93
Download	96
Upload	98
Go Online	99

### Connecting the Controller to the Network

If you have not done so, connect the controller to the network.

**Table 25 - Network Connections**

For this network	Connect the controller via a
Serial	1756-CP3 or 1747-CP3 cable
EtherNet/IP	1768-ENBT module to the left of the Compact GuardLogix controller
ControlNet	1768-CNB module to the left of the Compact GuardLogix controller

### Connect the Controller via a Serial Network

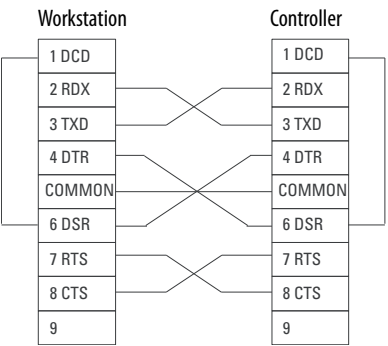
The 1756-CP3 or 1747-CP3 cable attaches the serial port of the workstation directly to the controller.



**WARNING:** If you connect or disconnect the serial cable with power applied to this module or the serial device at the end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

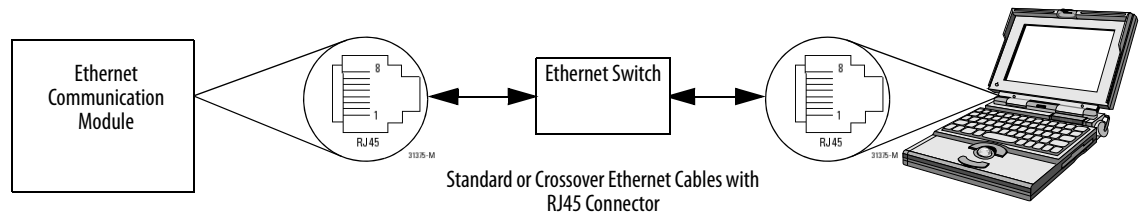
- TIP** If you make your own cable, do the following:
- Limit the length to 15.2 m (50 ft).
  - Wire the connectors as shown below.
  - Attach the shield to both connectors.



Connect Your EtherNet/IP Device and Computer

Connect your EtherNet/IP device and computer by using an Ethernet cable.

Figure 23 - Ethernet Connections



Connect Your ControlNet Communication Module and Your Computer

- To access the ControlNet network, you can do either of the following:
- Connect directly to the network.
  - Connect to a serial or EtherNet/IP network and browse (bridge) to the desired network. This requires no additional programming.

Configuring the Network Driver

RSLinx software handles communication between Compact GuardLogix controllers and RSLogix 5000 software. To communicate with the controller, configure RSLinx software for the required communication network.

Table 26 - Network Drivers

For this network	Configure this driver
Serial	RS-232 DF1 devices
EtherNet/IP	EtherNet/IP driver or Ethernet devices
ControlNet	ControlNet drivers

## Configure a Serial Communication Driver

1. Start RSLinx software.
2. From the Communication menu, choose Configure Drivers.
3. From the Available Driver Types pull-down menu, choose the driver.
4. Click Add New.
5. Click OK to accept the default name for the driver.
6. From the Comm Port pull-down menu, choose the serial port (on the workstation) to which the cable is connected.
7. From the Device pull-down menu, choose CompactLogix Serial Port.
8. Click Auto-Configure.
9. Does the dialog box display the following message?

Auto Configuration Successful!

If	Then
Yes	Click OK.
No	Go to Step 6 and verify that you selected the correct comm port.

10. Click Close.

## Configuring an EtherNet/IP or ControlNet Driver

For information on configuring a driver, refer to the appropriate publication:

- EtherNet/IP Modules in Logix5000 Control Systems, publication [ENET-UM001](#)
- ControlNet Modules in Logix5000 Control Systems User Manual, publication [CNET-UM001](#)

## Understanding the Factors that Affect Going Online

RSLogix 5000 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 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 Matching

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, RSLogix 5000 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 Matching

Firmware revision matching affects the download process. If the revision of the controller does not match the revision of the project, you are prompted to update the firmware of the controller. RSLogix 5000 software lets you update the firmware as part of the download sequence.

---

<b>IMPORTANT</b>	To update the firmware of the controller, first install a firmware upgrade kit. An upgrade kit ships on a supplemental CD along with RSLogix 5000 software.
------------------	---

---

<b>TIP</b>	You can also upgrade the firmware by choosing ControlFLASH™ from the Tools menu in RSLogix 5000 software.
------------	---

## Safety Status/Faults

Uploading program logic and going online is allowed 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 prior to 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 or not a download can proceed.

**Table 27 - 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 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.

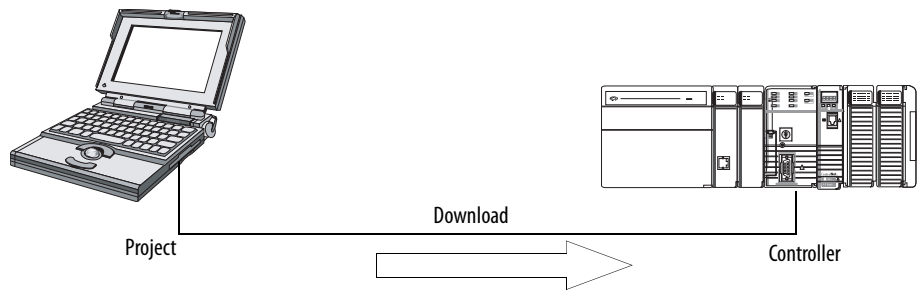
**IMPORTANT** During a download to a controller that is safety-unlocked, if firmware in the controller is different than in the offline project, do one of the following:


- 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 RSLogix 5000 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



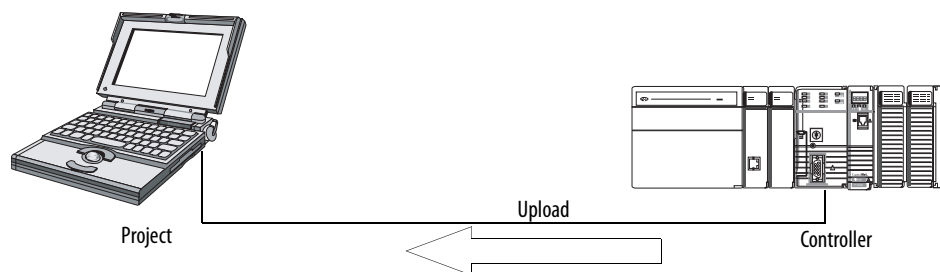
5. Follow the directions in this table to complete the download based on the software's response.


If the software indicates	Then
Download to the controller.	Choose Download. The project downloads to the controller and RSLogix 5000 software 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. 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. 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. <b>IMPORTANT:</b> 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.	<ul style="list-style-type: none"> <li>If the firmware minor revision is incompatible, to preserve the safety task signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project.</li> <li>To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted.</li> </ul> <b>IMPORTANT:</b> 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) master exists.	Check Enable Time Synchronization and click Download to proceed.

Following 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, choose File>Select>Yes.
4. If the project file exists, select it.

If the project to controller match is enabled, RSLogix 5000 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.
  - Update the project serial number to match the controller by checking the Update Project Serial Number checkbox and choosing 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.

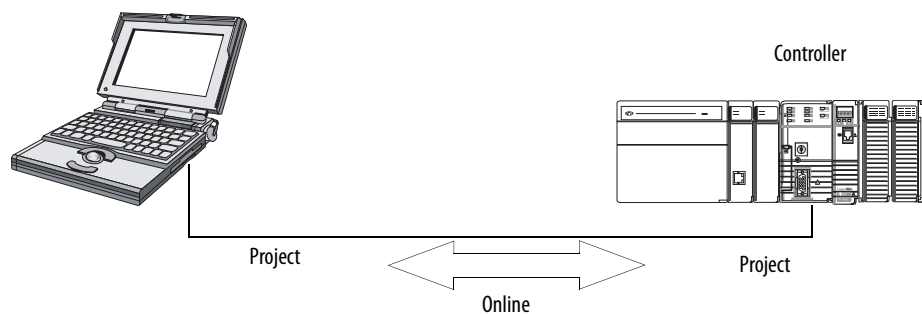
If you choose Upload, the standard and safety applications are uploaded. If a safety task signature exists, it is also uploaded. The safety-lock status

of the project reflects the original status of the online (controller) project.


**TIP** Prior to 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 offline safety task signature and safety-locked state are replaced by 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. Follow the directions in the table below to connect to the controller.

**Table 28 - Connect to the Controller**

If the software indicates	Then
Unable to connect to controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller, select another project file, or choose the Update project serial number checkbox and choose Go Online... to connect to the controller and update the offline project serial number to match the controller.
Unable to connect to controller. The revision of the offline project and the controller's firmware are not compatible.	Choose one of the following options: <ul style="list-style-type: none"> <li>Choose Update Firmware. Choose the required revision and click Update. Confirm your selection by clicking Yes.</li> <li><b>IMPORTANT:</b> The online project is deleted.</li> <li>To preserve the online project, cancel the online process and install a version of RSLogix 5000 software that is compatible with the firmware revision of your controller.</li> </ul>
You need to upload or download to go online by using the open project.	Choose one of the following options: <ul style="list-style-type: none"> <li>Upload to update the offline project.</li> <li>Download to update the controller project.</li> <li>Choose File to select another offline project.</li> </ul>
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.	<ul style="list-style-type: none"> <li>To preserve the safety task signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller.</li> <li>To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted.</li> <li><b>IMPORTANT:</b> The safety system requires revalidation.</li> </ul>
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 RSLogix 5000 software are online, the safety-locked status and safety task signature of the controller match the controller's project. The safety-lock status and safety task signature of the offline project are overwritten by the controller. If you do not want the changes to the offline project to be permanent, do not save the project file following the go online process.

## Monitor Status and Handle Faults

Topic	Page
Viewing Status via the Online Bar	101
Monitoring Connections	102
Monitoring Safety Status	104
Controller Faults	104
Developing a Fault Routine	106

See [Appendix B, Status Indicators](#) for information on interpreting the controller's status indicators.

### Viewing 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.

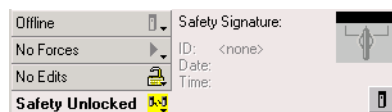
**Figure 24 - Status Buttons**



When the Controller Status button is selected as shown above, 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 below, the online bar displays the safety task signature.


**Figure 25 - Safety Signature Online Display**



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

Table 29 - Safety Status Icon

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 checkmark. 

## Monitoring 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:

- 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 need to monitor for connection faults to be sure that the safety system maintains SIL 3/PL e integrity.

See [Safety Connections](#).

## Safety Connections

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

The RunMode value indicates if consumed data is actively being updated by a device that is in the Run Mode (1) or Idle State (0). Idle state is indicated if the connection is closed, the safety task is faulted, or the remote controller or device is in Program mode or Test mode.

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.

**Table 30 - Safety Connection Status**

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	Data is actively being controlled by the producing device. 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.

## Monitoring 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 Logix5000 Controllers Controller Information and Status Programming Manual, publication [1756-PM015](#).

## Monitoring 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.

**Figure 26 - Safety Task Status**



These are the possible values for safety status:

- Safety partner is unavailable.
- Safety firmware is incompatible.
- Safety task inoperable.
- Safety task OK.

With the exception of safety task OK, the descriptions indicate that nonrecoverable safety faults exist.

See [Major Safety Faults \(Type 14\) on page 106](#) 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 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 terminated. 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:** Overriding the safety fault does not clear it! If you override the safety fault, it is your responsibility to prove that doing so maintains safe operation.

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 or not the fault is handled by the Program Fault Handler in the safety application.

When a recoverable fault is cleared programmatically, the safety task 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 re-initialize them. Safety outputs are placed in the safe state and the producer of safety-consumed tags commands the consumers to place them in a safe state, as well.

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.

## Viewing Faults

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

## Fault Codes

[Table 31](#) shows the fault codes specific to Compact GuardLogix controllers. The type and code correspond to the type and code displayed on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

**Table 31 - 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 re-initialized and the safety task begins executing. If a safety task signature does not exist, you must re-download 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 re-initialized 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 master.

The Logix5000 Controllers Major and Minor Faults Programming Manual, publication [1756-PM014](#), contains descriptions of the fault codes common to Logix controllers.

## Developing 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 [107](#).

## 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.

The Logix5000 Controllers Major and Minor Faults Programming Manual, publication [1756-PM014](#), provides details on creating and testing a fault routine.

## 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. Note that SSV instructions in safety and standard tasks cannot set bit 0 (major fault on error) in the mode attribute of a Safety I/O module.

For safety objects, the [Table 32](#) shows which attributes you can get values for 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. Making changes to objects can cause unexpected controller operation or injury to personnel.

---

Table 32 - GSV/SSV Accessibility

Safety Object	Attribute Name	Data Type	Attribute Description	Accessible from the Safety Task		Accessible from Standard Tasks	
				GSV	SSV	GSV <sup>(4)</sup>	SSV
Safety Task	Instance	DINT	Provides instance number of this task object. Valid values are 0...31.	?		?	
	MaximumInterval	DINT[2]	The max time interval between successive executions of this task.			?	?
	MaximumScanTime	DINT	Max recorded execution time (ms) for this task.			?	?
	MinimumInterval	DINT[2]	The min time interval between successive executions of this task.			?	?
	Priority	INT	Relative priority of this task as compared to other tasks. Valid values are 0...15.	?		?	
	Rate	DINT	Period for the task (in ms), or timeout value for the task (in ms).	?		?	
	Watchdog	DINT	Time limit (in ms) for execution of all programs associated with this task.	?		?	
Safety Program	Instance	DINT	Provides the instance number of the program object.	?		?	
	MajorFaultRecord <sup>(1)</sup>	DINT[11]	Records major faults for this program.	?	?	?	
	MaximumScanTime	DINT	Max recorded execution time (ms) for this program.			?	?
Safety Routine	Instance	DINT	Provides the instance number for this routine object. Valid values are 0...65,535.	?			
Safety Controller	SafetyLocked	SINT	Indicates whether the controller is safety-locked or -unlocked.	?		?	
	SafetyStatus <sup>(2)</sup>	INT	Specifies the safety status as the following: <ul style="list-style-type: none"> <li>• Safety task OK. (1000000000000000)</li> <li>• Safety task inoperable. (1000000000000001)</li> <li>• Firmware incompatible. (0000000000000011)</li> </ul>			?	
	SafetySignatureExists	SINT	Indicates whether the safety task signature is present.	?		?	
	SafetySignatureID	DINT	32-bit identification number.			?	
	SafetySignature	String <sup>(3)</sup>	32-bit identification number.			?	
	SafetyTaskFaultRecord <sup>(1)(2)</sup>	DINT[11]	Records safety task faults.			?	
AOI (Safety)	LastEditDate	LINT	Date and time stamp of the last edit to an Add-On Instruction definition.			?	
	SignatureID	DINT	ID number.			?	
	SafetySignatureID	DINT	32-bit identification number.			?	

(1) See [Access FaultRecord Attributes on page 109](#) for information on how to access this attribute.

(2) See [Capture Fault Information on page 109](#) 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.

**Table 33 - Parameters for Accessing FaultRecord Attributes**

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

For more information on using the GSV and SSV instructions, refer to the Input/Output Instructions chapter of the Logix5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

*Capture Fault Information*

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

## **Notes:**

## Store and Load Projects Using Nonvolatile Memory

Topic	Page
Using Memory Cards for Nonvolatile Memory	111
Storing a Safety Project	113
Loading a Safety Project	113
Manage Firmware with Firmware Supervisor	114

### Using Memory Cards for Nonvolatile Memory

Compact GuardLogix controllers, revision 18 or later, support a 1784-CF128 CompactFlash card for nonvolatile 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.

**TIP** The Compact GuardLogix controller does not require a battery. When it is being shut down, the controller uses internal nonvolatile memory to store its program. Energy stored in the 1768 power supply maintains controller power long enough to store the program to internal nonvolatile memory, not the external CompactFlash card.

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

- On every powerup
- Whenever there is no project in the controller and it powers up
- Anytime through RSLogix 5000 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 you make changes to 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, tag values, or a ControlNet network schedule, store the project again after you make the changes.

---



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

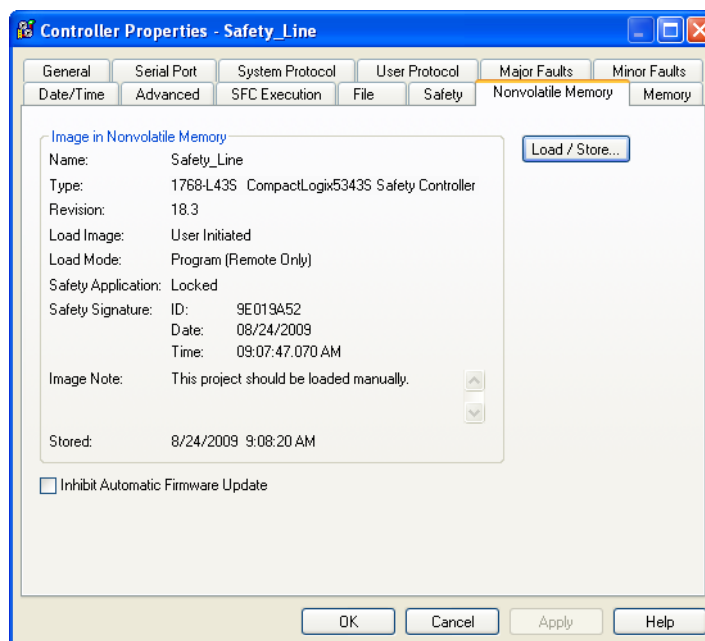


**WARNING:** When you insert or remove the CompactFlash card while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

If a memory 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.

**Figure 27 - Nonvolatile Memory Tab**



For detailed information on using nonvolatile memory, refer to the Logix5000 Controllers Nonvolatile Memory Programming Manual, publication [1756-PM017](#).



## Storing a Safety Project

You cannot store a safety project if the safety task status is Safety Task Inoperable. When you store a safety project, controller firmware is saved to the memory 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 will 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 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 a memory card, we recommend you select Program (Remote Only) as the Load mode, that is, the mode the controller should enter following the load.

## Loading a Safety Project

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

- The controller type specified by the project stored in nonvolatile memory matches the controller type.
- The major and minor revisions of the project in nonvolatile memory matches 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.

**Table 34 - Options for Loading a Project**

If you want to load the project	Then select this Load Image option	Notes
Whenever you turn on or cycle power	On Power Up	<ul style="list-style-type: none"> <li>During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory.</li> <li>The controller loads the stored project and firmware at every powerup regardless of the firmware or application on the controller. The load occurs whether or not the controller is safety-locked or has a safety task signature.</li> <li>You can always use RSLogix 5000 software to load the project.</li> </ul>
Whenever there is no project in the controller and you turn on or cycle power	On Corrupt Memory	<ul style="list-style-type: none"> <li>The controller updates the firmware on the controller, if required. The application stored in nonvolatile memory is also loaded and the controller enters the selected mode, either Program or Run.</li> <li>You can always use RSLogix 5000 software to load the project.</li> </ul>
Only through RSLogix 5000 software	User Initiated	<ul style="list-style-type: none"> <li>If the controller type as well as the major and minor revisions of the project in nonvolatile memory match the controller type and major and minor revisions of the controller, you can initiate a load, regardless of the Safety Task status.</li> <li>Loading a project to a safety-locked controller is allowed only when the safety task signature of the project stored in nonvolatile memory matches the project on the controller.</li> <li>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.</li> </ul> <p><b>IMPORTANT:</b> 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.</p> <ul style="list-style-type: none"> <li>If the firmware on the controller matches the revision in nonvolatile memory, the internal safety partner firmware is updated, if required, the application stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the selected mode, either Program or Run.</li> </ul>

## Manage Firmware with Firmware Supervisor

Beginning with RSLogix 5000 software, version 18, you can use the Firmware Supervisor feature to manage firmware on Compact GuardLogix 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 memory card.
- The device must support firmware upgrades via the ControlFLASH utility.

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. CIP Safety I/O modules on DeviceNet networks and POINT Guard I/O modules are not yet supported.

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.

RSLogix 5000 software moves the firmware kits from your computer to the controller memory card for Firmware Supervisor to use.

**TIP** If you disable Firmware Supervisor, you disable only firmware supervisor updates. This does not include the controller firmware updates that occur when the controller image is reloaded from the memory card.

## **Notes:**

## Status Indicators

Topic	Page
Compact GuardLogix Controller Status Indicators	117
Clear a Major Fault	118
Clear a Nonrecoverable Fault	119
Troubleshoot a Nonresponsive Module	119
Troubleshoot System Power	120

### Compact GuardLogix Controller Status Indicators

This table describes the controller's status indicators.

**Table 35 - Status Indicator Descriptions**

Indicator	Status	Description
PWR	Green	The controller is providing power to 1768 modules in the system.
	Red	The power supply is not producing valid 24V power to the 1768 modules. See <a href="#">Troubleshoot System Power on page 120</a> .
	Off	The power supply is turned off, lacks adequate input power, or has failed. See <a href="#">Troubleshoot System Power on page 120</a> .
I/O PWR	Off	Either the controller or the power supply is not operating properly.
	Green	The controller is operating properly.
	Flashing Red/Green or Solid Red	An endcap or 1769 I/O module is not properly attached. See <a href="#">Troubleshoot System Power on page 120</a> .
RUN	Off	The controller is in Program or Test mode.
	Green	The controller is in Run mode.
FORCE	Off	No tags contain I/O force values or I/O forces are inactive (disabled).
	Amber	I/O forces are active (enabled). I/O force values may or may not exist.
	Flashing Amber	One or more of input or output addresses have been forces to an On or Off state, but the forces have not been enabled. Enable forces or remove the individual I/O from being forced.
MEM SAVE	Off	The user program and configuration data are not actively being saved to nonvolatile memory.
	Green	The use program and configuration data are being saved to nonvolatile memory.
I/O	Off	There are no devices in the I/O configuration of the controller or the controller does not contain a project.
	Green	The controller is communicating with all of the devices in its I/O configuration.
	Flashing Green	One or more devices in the controller's I/O configuration are not responding. See <a href="#">Troubleshoot a Nonresponsive Module on page 119</a> .
	Flashing Red	The controller is not communicating with any of the devices in its I/O configuration. See <a href="#">Troubleshoot a Nonresponsive Module on page 119</a> .

Table 35 - Status Indicator Descriptions

Indicator	Status	Description
OK	Off	No power is applied. If MEM SAVE indicator is green, the user program and configuration data are being saved to nonvolatile memory.
	Flashing Red	The controller requires a firmware update or a firmware update is in progress. A recoverable major fault occurred on the controller. A non-recoverable major fault occurred on the controller. See <a href="#">Clear a Major Fault on page 118</a> .
	Red	The controller detected a nonrecoverable major fault so it cleared the project from memory. See <a href="#">Clear a Nonrecoverable Fault on page 119</a> .
	Green	Controller is OK.
	Flashing Green	The controller is storing or loading a project to or from nonvolatile memory.
CF	Off	There is no CompactFlash card activity.
	Flashing Green	The controller is reading from or writing to the CompactFlash card. <b>IMPORTANT:</b> Do not remove the CompactFlash card while the controller is reading from or writing to the card. Removing the card during a read or write could corrupt data on the card, data in the controller, and firmware installed on the controller.
	Flashing Red	The CompactFlash card does not have a valid file system and must be replaced.
DCH0	Off	Channel 0 is configured differently than the default serial configuration.
	Green	Channel 0 has the default serial configuration.
CH0	Off	No RS-232 activity.
	Green	RS-232 activity.
SAFE RUN	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.
SAFETY TASK	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.
SAFETY LOCK	Off	Safety task is not locked.
	Green	Safety task is locked.
SAFETY OK	Off	No power is applied.
	Green	The safety partner is OK.
	Flashing Green	The safety partner is storing or loading 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. A recoverable major fault occurred on the safety partner. A nonrecoverable major fault occurred on the safety partner.

## Clear a Major Fault

If the OK status indicator flashes red because of a recoverable major fault, clear the fault by following these steps.

1. Turn the controller keyswitch from PROG to RUN and back to PROG.
2. Go online with RSLogix 5000 software.
3. On the Controller Properties dialog box, click the Major Faults tab to find information about the fault.

If the OK status indicator is flashing red because of a nonrecoverable major fault, the controller:

- initially displayed a solid red OK indicator.
- reset itself.
- cleared the project from its memory.
- set the OK indicator to flashing red.
- produced a major recoverable fault and generated a corresponding fault code in the RSLogix 5000 project.
  - Fault code 60 means the CompactFlash card is not installed.
  - Fault code 61 means the CompactFlash card is installed.

Follow these steps to recover from fault code 60 or 61.

1. Turn the controller keyswitch from PROG to RUN and back to PROG.
2. Go online with RSLogix 5000 software and download the project.
3. Change to REM RUN or RUN mode.

If the issue persists, record the status of the OK and RS-232 indicators before cycling power and contacting Rockwell Automation support.

## **Clear a Nonrecoverable Fault**

If the OK status indicator is solid red, follow these steps to clear the fault.

1. Cycle power.
2. Download the project.
3. Change to REM RUN or RUN mode.

If the issue persists, record the status of the OK and RS-232 indicators before cycling power and contacting Rockwell Automation support.

## **Troubleshoot a Nonresponsive Module**

Follow these steps to determine why a device may not be responding.

1. Verify that all I/O modules in your project are installed in the same order.
2. Verify that all devices have been updated to the latest major and minor firmware revisions.
3. Use RSLogix 5000 software's online help to determine which module is not responding.

## Troubleshoot System Power

The CompactLogix power supply works with the CompactLogix controller to provide power to the system. You must consider both when attempting to troubleshoot system power.

---

**IMPORTANT** Before you disconnect, reconnect, or replace any component, make sure you have turned off power and allowed all system status indicators to turn off.

---

To troubleshoot system power issues, use the CompactLogix power supply PWR status indicator and the CompactLogix controller PWR and I/O PWR indicators. If the power supply is not operating properly, the controller will not operate properly either. You must first diagnose and correct any issues with the power supply before troubleshooting the controller.

1. Examine the power supply PWR status indicator.
2. If the power supply is operating properly and the power supply PWR status indicator is green, examine the controller PWR indicator.
3. If the controller PWR status indicator is green, examine the I/O PWR status indicator.

### Examine the Power Supply PWR Status Indicator

Power Supply PWR Indicator Status	Recommended Action
Off	Verify that the power supply is turned on and that adequate input power is properly connected. Replace the power supply.
Green	The power supply is operating properly. Check the controller PWR and I/O PWR status indicators to make sure the entire system is operating properly.
Red	The power supply is not producing valid 24V power to the 1768 modules. Follow the corrective action below.

1. Remove power and wait for all status indicators to turn off.
2. Disconnect all modules from the system, including the controller.
3. Reapply power.
4. Check the PWR status indicator on the power supply.
  - a. If the status indicator remains red, replace the power supply.
  - b. If the status indicator is green, one of the other modules in the system is causing the red indicator.
5. Remove power and wait for all status indicators to turn off.
6. Reinstall the controller and check the power supply's PWR indicator.
  - a. If green, remove power, wait for all status indicators to turn off and reinstall 1768 modules one at a time until you identify the module causing the red indicator.
  - b. If red, replace the controller.



## Examine the Controller PWR Indicator

This task assumes that the power supply PWR indicator is green.

Controller PWR Indicator Status	Recommended Action
Off	Make sure all of the modules in the system are installed properly and are fully engaged with one another. If the indicator remains off, follow the corrective action below.
Green	The controller is providing power to 1768 modules in the system. Check the controller I/O PWR status indicator to make sure the entire system is operating properly.
Red	Either the controller or 1768 modules in the system need to be replaced. Follow the corrective action below.

1. Remove power and wait for all status indicators to turn off.
2. Disconnect all 1768 modules from the system, except for the controller.
3. Reapply power.
4. Check the controller PWR indicator.
  - a. If the status indicator remains red, replace the controller.
  - b. If the status indicator is green, one of the 1768 modules is causing the red indicator.
5. Remove power.
6. Reinstall the 1768 modules one at a time, removing and reapplying power and checking the controller PWR indicator each time.
7. If the controller PWR indicator turns red, the most-recently installed module is causing the red indicator.

To troubleshoot 1768 modules, see their respective installation instructions.

## Examine the I/O PWR Indicator

This task assumes that the power supply and controller PWR indicators are green and that you have 1769 I/O modules in your system.

Controller I/O PWR Indicator Status <sup>(1)</sup>	Recommended Action
Off	Replace the controller.
Green	The controller is operating properly. No action required.
Flashing red and green	Make sure the 1769 I/O modules or end cap are properly attached and cycle power.
Red	A 1769 power supply may be installed in the local bank, or there may be an issue with the controller or 1769 I/O in the system. Follow the corrective action below.

(1) When the controller powers up, the I/O PWR status indicator is momentarily red and then changes to green if there are no issues. If the indicator remains red, use the table above to troubleshoot the issue.

1. If there is a 1769 power supply installed in the local bank, remove it and reapply power.

If the I/O PWR indicator remains red, go to the next step.

2. Remove power and wait for all status indicators to turn off.
3. Disconnect the 1769 I/O modules from the system.
4. Reapply power.
5. Check the controller I/O PWR indicator.
  - a. If the indicator is red, replace the controller.
  - b. If the indicator is green, one of the 1769 I/O modules is causing the red indicator.

To troubleshoot 1769 I/O modules, see their respective installation instructions.

## Change Controller Type in RSLogix 5000 Projects

Topic	Page
Changing from a Standard to a Safety Controller	123
Changing from a Safety to a Standard Controller	124
Changing from a 1756 GuardLogix Controller to a 1768 Compact GuardLogix Controller or Vice Versa	125
Changing from a 1756-L7xS Controller to a 1756-L6xS or 1768-L4xS Controller	125
Additional Resources	125

Because safety controllers have special requirements and do not support certain standard features, you must understand the behavior of the system when changing the controller type from standard to safety or from safety to standard in your RSLogix 5000 project. Changing controller type affects the following:

- Supported features
- Physical configuration of the project, that is the safety partner and Safety I/O
- Controller properties
- Project components such as tasks, programs, routines, and tags
- Safety Add-On Instructions

### Changing 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:

- 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.
- Safety components are created (that is safety task, safety program, and so forth).
- A time-based safety network number (SNN) is generated for the local chassis.
- Standard controller features that are not supported by the safety controller, such as redundancy, are removed from the Controller Properties dialog box (if they existed).

## Changing 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, as described below:

- 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.

**TIP** Peer safety controllers are not deleted, even if they have no connections remaining.

- Instructions may still reference modules that have been deleted and will produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and Safety I/O tags will not verify.

If the safety controller project contains safety Add-On Instructions, you must remove them from the project or change their class to standard before changing the controller type.

## Changing from a 1756 GuardLogix Controller to a 1768 Compact GuardLogix Controller or Vice Versa

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.

The representation of the safety partner is updated to appear appropriately for the target controller:

- The safety partner is created in slot  $x$  (primary slot + 1) when changing to a 1756 GuardLogix controller.
- When changing to a 1768 Compact GuardLogix controller, the safety partner is removed because it is internal to the Compact GuardLogix controller.

**TIP** A 1756 GuardLogix controller supports 100 safety programs in the safety task while a 1768 Compact GuardLogix controller supports 32.

## Changing from a 1756-L7xS Controller to a 1756-L6xS or 1768-L4xS Controller

Floating-point instructions, such as FAL, FLL, FSC, SIZE, CMP, SWPB, and CPT are supported in 1756-L7xS controllers, but not in 1756-L6xS and 1768-L4xS controllers. If your safety program contains these instructions, verification errors will occur when changing from a 1756-L7xS controller to a 1756-L6xS or 1768-L4xS controller.

## Additional Resources

Refer to the Logix5000 Controllers Add-On Instructions Programming Manual, publication [1756-PM010](#), for more information on Add-On Instructions.

## **Notes:**

## Numerics

**1747-CP3 cable** 91  
**1756-CP3** 18, 24  
     cable 91  
**1768 Compact GuardLogix controller** 125  
**1768-PA3** 18  
**1768-PB3** 18  
**1769-ECR** 18

## A

**Add-On Instructions** 124  
**address**  
     CIP Safety I/O module 61  
**advanced connection reaction time** 57  
**alert symbol** 102  
**alias tags** 75  
**attributes**  
     safety object 107  
**AutoFlash software** 26, 27  
**automatic firmware updates** 115

## B

**bank**  
     local 19, 20  
     remote 19, 20  
**base tags** 75  
**bus extension cable** 20

## C

**cable**  
     serial 24  
**cable length** 24  
**Change Controller button** 33  
**changing controllers** 123 ... 124  
**CIP Safety** 7, 37, 69  
**CIP Safety I/O**  
     adding 53  
     configuration signature 59  
     monitor status 61  
     reset ownership 60  
     status data 61  
**class** 78  
**clear**  
     faults 105  
**clear a major fault** 118  
**clearance** 18  
**communication** 12  
     ControlNet 46  
     DeviceNet network 49  
     EtherNet/IP network 43  
     serial network 50  
**communication driver** 25  
**Compact GuardLogix controller** 125

**CompactFlash card** 24  
     update firmware 27  
**CompactLogix**  
     DeviceNet network 49  
     serial network DF1 modes 51  
**configuration owner** 60  
     identifying 60  
     resetting 60, 63  
**configuration signature**  
     components 59  
     copy 59  
     definition 59  
**configure**  
     communication driver 25  
**configure always** 68  
     checkbox 35  
**connect**  
     1768 components 21  
     1769 components 22  
     ControlNet 46  
     serial cable 24  
**connection**  
     ControlNet network 46  
     EtherNet/IP network 43  
     monitor 102  
     scheduled 47  
     status 103  
     unscheduled 47  
**connection reaction time limit** 55, 83  
**CONNECTION\_STATUS** 79, 103  
**ConnectionFaulted bit** 103  
**constant value tag** 78  
**consume tag data** 82  
**consumed tag** 75, 79  
**control and information protocol**  
     definition 7  
**ControlFLASH software** 26, 94, 114  
**controller**  
     change type 123 ... 125  
     configuration 31  
     fault handler 107  
     match 94  
     properties 32  
     serial number 94  
     serial number mismatch 97, 100  
**controller-scoped tags** 77  
**ControlNet**  
     configure driver 93  
     connections 46, 92  
     example 47  
     module 46  
     overview 46  
     scheduled 47  
     software 46  
     unscheduled 47  
**coordinated system time** 97  
**copy**  
     safety network number 42  
     safety task signature 88  
**create a project** 31

**D****data types**

- CONNECTION\_STATUS 79

**delete**

- safety task signature 89

**DeviceNet network 49**

- communication 49
- module capability 49
- required interfaces 49
- required software for communication 49

**DeviceNet network example 50****diagnostic coverage 7****DIN rail 20, 28****distance rating 19****download**

- effect of controller match 94
- effect of firmware revision match 94
- effect of safety status 94
- effect of safety task signature 95
- effect of safety-lock 95
- process 96 ... 97

**driver**

- ControlNet 93
- EtherNet/IP 93

**E****editing 88****electronic keying 114****electrostatic discharge 17****enclosure 15****end cap 18**

- attach 23

**environment 15****EtherNet/IP**

- CIP Safety I/O modules 45
- configure driver 93
- connection use 43
- connections 44, 92
- example 44
- example configuration 44
- module capability 43
- network parameters 45
- overview 43
- software 43
- standard I/O modules 45

**EtherNet/IP network**

- configure driver 92

**extension cable 20****external access 74, 78****F****faceplate**

- push button 28

**fault**

- clear 105
- nonrecoverable controller 104
- nonrecoverable safety 104
- recoverable 105
- routines 106 ... 108

**fault codes**

- major safety faults 106

**firmware**

- update 26

**firmware revision**

- management 114
- match 94
- mismatch 95, 97, 100
- update 26

**Firmware Supervisor 114****firmware upgrade kit 94, 114****forcing 88****G****gateway 45****get system value (GSV)**

- accessibility 108
- definition 7
- using 107

**go online 99**

- factors 93

**grounding**

- DIN rail 21
- panel mounted 20

**H****hazardous location approval**

- Europe 17
- North America 16

**HMI devices 10****I****I/O**

- indicator 102
- module replacement 35

**IP address 45, 53****L****listen only connection 60****load a project 113**

- on corrupt memory 114
- on power up 114
- user initiated 114

**local bank 19, 20****lock**

- See safety-lock.

**Logix5000 controllers**

- DF1 modes 51



## M

**major fault**  
     clear 118  
**major faults tab** 105, 106  
**major safety faults** 106  
**MajorFaultRecord** 109  
**maximum observed network delay** 56  
     reset 83  
**memory card** 111, 112, 114  
     installation 24  
     removal 24  
**minor faults tab** 106  
**module**  
     properties  
         connection tab 60  
**module placement** 18  
**monitor**  
     connections 102  
     status 61  
**morphing**  
     See changing controllers.  
**mount**  
     1768 components 21  
     1769 components 22  
     panel 20  
**mount the controller** 20  
**mounting screws** 18  
**multicast** 7

## N

**network delay multiplier** 58, 83  
**network status**  
     indicator 65, 67  
**nonrecoverable controller fault** 104  
**nonrecoverable safety fault** 104  
     re-starting the safety task 105  
**nonvolatile memory** 111 ... 115  
     tab 112

## O

**online bar** 101  
**out-of-box** 65  
     reset module 63  
**ownership**  
     configuration 60  
     resetting 60

## P

**panel mount** 20  
**parts** 18  
**password**  
     set 33  
     valid characters 34  
**paste**  
     safety network number 42

**peer safety controller**  
     configuration 36  
     location 79  
     sharing data 79  
     SNN 79, 80  
**Performance Level** 7, 9  
**placement** 18  
**power supply** 18, 19  
**probability of failure on demand (PFD)**  
     definition 7  
**probability of failure per hour (PFH)**  
     definition 7  
**produce a tag** 81  
**produce and consume tags** 43, 46, 79  
**produced tag** 75, 79  
**program fault routine** 106  
**programmable electronic systems (PES)** 16  
**programming** 88  
**program-scoped tags** 77  
**project to controller match** 94  
**protect signature in run mode** 34  
**protecting the safety application** 86 ... 89  
     RSLogix Security 87  
     safety task signature 88  
     safety-lock 86  
**push button** 28

## R

**reaction time** 73  
**reaction time limit**  
     CIP Safety I/O 55  
**recoverable fault** 105  
     clear 105  
**remote bank** 19, 20  
**remove a module** 28  
**replace**  
     configure always enabled 68  
     configure only... enabled 64  
**requested packet interval** 79  
     CIP Safety I/O 56  
     consumed tag 83  
     consumed tags 75  
     definition 7  
     produced tag data 75  
**reset**  
     module 63  
     ownership 60, 63  
**restrictions**  
     programming 89  
     safety tag mapping 84  
     software 89  
     when safety signature exists 88  
     when safety-locked 86  
**RPI**  
     See requested packet interval  
**RSLinx Classic software**  
     version 13

**RSLogix 5000 software**

- reset module 63
- restrictions 89
- versions 13

**RSLogix Security** 87**run mode protection** 88, 89**RunMode bit** 103

## S

**safe state** 9**safety network number** 37

- assignment 37
- automatic assignment 39
- changing controller SNN 40
- changing I/O SNN 40
- copy 42
- copy and paste 42
- definition 7
- description 9
- formats 37
- managing 37
- manual 38
- manual assignment 39
- modification 39
- paste 42
- set 55
- time-based 38
- view 32

**safety object**

- attributes 107

**safety programs** 74**safety projects**

- features not supported 14

**safety routine** 74

- using standard data 84

**safety status**

- button 88, 102
- effect on download 94
- safety task signature 88
- view 94, 101, 104

**safety tab** 87, 88, 104

- configuration signature 59
- connection data 56
- generate safety task signature 88
- module replacement 63
- safety-lock 87
- safety-lock controller 87
- unlock 87
- view safety status 94, 104

**safety tags**

- controller-scoped 77
- create 75
- description 74
- mapping 84 . . . 86
- safety-program-scoped 77
- valid data types 76

**safety task** 72

- execution 73
- priority 72
- watchdog time 72

**safety task period** 56, 73, 79**safety task signature** 78

- copy 88
- delete 89
- description 10
- effect on download 95
- effect on upload 95
- generate 88
- restricted operations 88
- restrictions 89
- storing a project 113
- view 101

**safety-lock** 86

- controller 87
- effect on download 95
- effect on upload 95
- icon 87
- password 87

**SafetyTaskFaultRecord** 109**safety-unlock**

- controller 87
- icon 87

**scan times**

- reset 89

**scheduled connections** 47**screw torque** 20**serial**

- communication 50
- network 50
  - software 50
- network driver 92
- port
  - configuration 50

**serial cable** 18, 24**serial driver** 25**serial network**

- DF1 modes for Logix5000 controllers 51

**serial number** 94**serial port**

- connections 91

**set system value (SSV)**

- accessibility 108
- using 107

**slot numbering** 19**SNN**

- See safety network number

**software**

- ControlNet network 46
- EtherNet/IP network 43
- restrictions 89

**standard data in a safety routine** 84**status flags** 103**store a project** 113**subnet mask** 45

## T

### tags

- alias 75
- base 75
- class 78
- constant value 78
- consumed 75, 79
- controller-scoped 77
- data type 76
- external access 74, 78
- naming 60
- overview 74
- produced 75, 79
- produced/consumed safety data 76, 77
- program-scoped 77
- safety I/O 76, 77
- scope 77
- See also, safety tags.
- type 75

### temperature range 18

### terminology 7

### time synchronization 35, 97

### timeout multiplier 57, 83

### torque 20

### troubleshoot

- module 119
- system power 120

## U

### unicast 7

- connections 55, 79, 81

### unlock controller 87

### unscheduled connections 47

### update

- firmware 26

### upload

- effect of controller match 94
- effect of safety task signature 95
- effect of safety-lock 95
- process 98

### UV radiation 17

## V

### verification errors

- changing controller type 125

### view

- safety status 94

## W

### watchdog time 72

## Notes:



## Rockwell Automation Support

Use the following resources to access support information.

<b>Technical Support Center</b>	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	<a href="https://rockwellautomation.custhelp.com/">https://rockwellautomation.custhelp.com/</a>
<b>Local Technical Support Phone Numbers</b>	Locate the phone number for your country.	<a href="http://www.rockwellautomation.com/global/support/get-support-now.page">http://www.rockwellautomation.com/global/support/get-support-now.page</a>
<b>Direct Dial Codes</b>	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	<a href="http://www.rockwellautomation.com/global/support/direct-dial.page">http://www.rockwellautomation.com/global/support/direct-dial.page</a>
<b>Literature Library</b>	Installation Instructions, Manuals, Brochures, and Technical Data.	<a href="http://www.rockwellautomation.com/global/literature-library/overview.page">http://www.rockwellautomation.com/global/literature-library/overview.page</a>
<b>Product Compatibility and Download Center (PCDC)</b>	Get help determining how products interact, check features and capabilities, and find associated firmware.	<a href="http://www.rockwellautomation.com/global/support/pcdc.page">http://www.rockwellautomation.com/global/support/pcdc.page</a>

## Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at [http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002\\_-en-e.pdf](http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf).

Rockwell Automation maintains current product environmental information on its website at <http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>.

Allen-Bradley, Compact I/O, CompactBlock Guard I/O, CompactLogix, ControlFLASH, ControlLogix, DriveLogix, GuardLogix, Integrated Architecture, KwikLink, Logix5000, MicroLogix, PanelView, PhaseManager, POINT Guard I/O, POINT I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLinx, RSLogix 5000, RSLogix, RSNetWorx, and SLC are trademarks of Rockwell Automation, Inc.

CIP Safety, CIP Sync, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

**[www.rockwellautomation.com](http://www.rockwellautomation.com)**

### Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1768-UM002D-EN-P - September 2016

Supersedes Publication 1768-UM002C-EN-P - April 2012

Copyright © 2016 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.