User Manual

Allen-Bradley

# GuardLogix 5570 Controllers

Catalog Numbers 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT, 1756-L72EROMS

Studio 5000 Automation Engineering & Design Environment

Original Instructions

# Important User Information

Read this document and the documents that are 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, and requirements of all applicable codes, laws, and standards.

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

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

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

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

No patent liability is assumed by Rockwell Automation, Inc. for use of information, circuits, equipment, or software that is 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 can 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). |

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

## New and Updated Information

This table contains the changes that are made to this revision.

| Topic | Page |
|---|---|
| Changed section title from More Resources to For More Information. | 13 |
| Changed resource column description from Kinetix® servo drives to Drives. | 14 |
| Added the Kinetix 5700 Servo Drives User Manual and the PowerFlex® 527 Adjustable Frequency AC Drive User Manual to the Drives resource material. | 14 |
| Removed previous versions information from Supported Features table. | 21 |
| Changed column title from Version 24 to Version 24 and Later. | 21 |
| Added introductory sentence and Figure 10. | 50 |
| Added SNN assignment content to Important table. | 50 |
| Revised Figure 14 to include PowerFlex 527 and Kinetix 5700 drives. | 58 |
| Added Kinetix 5700 and PowerFlex 527 drives to drive address information. | 75 |
| Revised Table 20 title and table information to include more drives. | 75 |
| Added Kinetix 5700 and PowerFlex 527 drives to reference for more information. | 76 |

## Notes:

## Chapter 3

## Configure the Controller



## Chapter 4

## Communicate over Networks

## Chapter 5

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



## Chapter 6

### Develop Safety Applications

## Chapter 7

### Go Online with the Controller



## Chapter 8

### Store and Load Projects Using Nonvolatile Memory

## Chapter 9

**Monitor Status and Handle Faults**



## Appendix A

**Status Indicators**



## Appendix B

**Change Controller Type**



**Index**

## Notes:

This manual is a guide for when a GuardLogix® 5570 controller is used in a Studio 5000 Logix Designer™ application. It describes the GuardLogix-specific procedures that you use to configure, operate, and troubleshoot your controller.

Use this manual if you are responsible to design, install, program, or troubleshoot control systems with GuardLogix 5570 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 for GuardLogix controller, Safety Integrity Level (SIL) 3 and Performance Level (e) (SIL 3/PLe) requirements, or information on standard Logix components, see the list of For More Information on page 13.

## About GuardLogix Controllers

Two lines of 1756 GuardLogix controllers are available. These controllers share many features but also have some differences. Table 1 provides a brief overview of those differences.

**Table 1 - Differences between GuardLogix 5570 and GuardLogix 5560 Controllers**

| Feature | GuardLogix 5570 Controllers (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT) | GuardLogix 5560 Controllers (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP) |
|---|---|---|
| Clock support and backup that is used for memory retention at powerdown | Energy storage module (ESM) | Battery |
| Communication ports (built-in) | USB | Serial |
| Connections, controller | 500 | 250 |
| Memory, nonvolatile | Secure Digital (SD) card | CompactFlash (CF) card |
| Status indicators | Scrolling status display and status indicators | Status indicators |
| Programming tool | Studio 5000 environment, version 21 or later<br>RSLogix™ 5000 software, version 20 or later | RSLogix 5000 software, version 14<br>RSLogix 5000 software, version 16 or later |
| User manual | • Studio 5000 environment: this manual<br>• RSLogix 5000 software: 1756-UM020 | 1756-UM020 |
| Safety reference manual | • Studio 5000 environment: 1756-RM099<br>• RSLogix 5000 software: 1756-RM093 | 1756-RM093 |

### Extreme Environment Controllers

The extreme environment GuardLogix controller, catalog numbers 1756-L73SXT and 1756-L7SPXT, provide the same functionality as the 1756-L73S controller, but is designed to withstand temperatures of -25...70 °C (-13...158 °F).

| IMPORTANT | Logix-XT system components are rated for extreme environmental conditions only when used properly with other Logix-XT system components. The use of Logix-XT components with traditional Logix system components nullifies extreme-environment ratings. |
|---|---|

### Armor GuardLogix Controllers

The Armor™ GuardLogix controller (catalog number 1756-L72EROMS) combines a 1756-L72S GuardLogix controller and safety partner with two EtherNet/IP™, DLR-capable communication channels in an IP67-rated housing for mounting on a machine. For more information on the Armor GuardLogix controller, refer to the Armor GuardLogix Controller Installation Instructions, publication 1756-IN060.

## Studio 5000 Environment

The Studio 5000 Automation Engineering & Design Environment™ combines engineering and design elements into a common environment. The first element is the Studio 5000 Logix Designer application. The Logix Designer application is the rebranding of RSLogix 5000 software and continues to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.


The Studio 5000 environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. The Studio 5000 environment is the one place for design engineers to develop all elements of their control system.

## Terminology

This table defines terms that are used in this manual.

**Table 2 - 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 that is designed for industrial automation applications. |
| CIP safety | Common Industrial Protocol – Safety Certified | SIL 3/PLe-rated version of CIP. |
| DC | Diagnostic Coverage | The ratio of the detected failure rate to the total failure rate. |
| EN | European Norm | The official European standard. |
| ESM | Energy Storage Module | Used for clock support and backup for memory retention at powerdown on GuardLogix 5570 controllers. |
| GSV | Get System Value | An instruction that retrieves specified controller-status information and places it in a destination tag. |
| — | Multicast | The transmission of information from one sender to multiple receivers. |
| NAT | Network Address Translation | The translation of an Internet Protocol (IP) address to another IP address on another network. |
| PFD | Probability of 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. |

## For More Information

These documents contain more information about related products from Rockwell Automation.

**Table 3 - Publications Related to GuardLogix Controllers and Systems**

| Resource | | Description |
|---|---|---|
| Safety application requirements | GuardLogix 5570 Controller Systems Safety Reference Manual, publication 1756-RM099 | Contains detailed requirements for achieving and maintaining SIL 3/PLe with the GuardLogix 5570 controller system, using the Studio 5000 Logix Designer application. |
| | GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093 | Contains detailed requirements for achieving and maintaining SIL 3/PLe with the GuardLogix 5560 or 5570 controller system, using RSLogix 5000 software. |
| CIP Sync (time synchronization) | Integrated Architecture® and CIP Sync Configuration Application Technique, publication IA-AT003 | Provides detailed and comprehensive information about how to apply CIP Sync technology to synchronize clocks in a Logix control system. |
| Guard I/O™ modules | Guard I/O DeviceNet™ Safety Modules User Manual, publication 1791DS-UM001 | Provides information on using Guard I/O DeviceNet Safety modules. |
| | Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001 | Provides information on using Guard I/O EtherNet/IP Safety modules. |
| | POINT Guard I/O™ Safety Modules User Manual, publication 1734-UM013 | Provides information on installing, configuring, and using POINT Guard I/O modules. |
| | Armor GuardLogix Controller Installation Instructions, publication 1756-IN060 | Provides information on installing and using Armor GuardLogix controllers. |

**Table 3 - Publications Related to GuardLogix Controllers and Systems (Continued)**

| Resource | | Description |
|---|---|---|
| Drives | Kinetix 5500 Servo Drives User Manual, publication 2198-UM001 | Provides information to install, configure, start up, and troubleshoot your Kinetix 5500 servo drive system. Also includes requirements for using Kinetix 5500 drives in safety applications. |
| | Kinetix 5700 Servo Drives User Manual, publication 2198-UM002 | Provides information to install, configure, start up, and troubleshoot your Kinetix 5700 servo drive system. Also includes requirements for using Kinetix 5700 drives in safety applications. |
| | PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002 | Provides information to install, start up, and troubleshoot the PowerFlex 520-series adjustable frequency AC drive. |
| Hardware installation | ControlLogix® Chassis and Power Supplies Installation Instructions, publication 1756-IN005 | Describes how to install and ground ControlLogix chassis and power supplies. |
| | Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1 | Provides in-depth information on how to ground and wire programmable controllers. |
| Instructions (programming) | GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095 | Provides information on the GuardLogix Safety application instruction set. |
| | Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003 | Provides programmers with details about each available instruction for a Logix5000 controller. |
| | Logix5000 Controllers Motion Instructions Reference Manual, publication MOTION-RM002 | Provides programmers with details about the motion instructions that are available for a Logix5000 controller. |
| Motion | Sercos Motion Configuration and Startup User Manual, publication MOTION-UM001 | Details how to configure a sercos motion application system. |
| | Motion Coordinated Systems User Manual, publication MOTION-UM002 | Details how to create and configure a coordinated motion application system. |
| | Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, publication MOTION-UM003 | Details how to configure an Integrated Motion on EtherNet/IP networks application system. |
| | Integrated Motion on the EtherNet/IP Network Reference Manual, publication MOTION-RM003 | Detailed information on axis control modes and attributes for Integrated Motion on EtherNet/IP networks. |
| Networks (ControlNet™, DeviceNet, EtherNet/IP) | EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication ENET-UM001 | Describes how to configure and operate EtherNet/IP modules in a Logix5000 control system. |
| | ControlNet Modules in Logix5000 Control Systems User Manual, publication CNET-UM001 | Describes how to configure and operate ControlNet modules in a Logix5000 control system. |
| | DeviceNet Modules in Logix5000 Control Systems User Manual, publication DNET-UM004 | Describes how to configure and operate DeviceNet modules in a Logix5000 control system. |
| PhaseManager™ | PhaseManager User Manual, publication LOGIX-UM001 | Provides steps, guidance, and examples on how to set up and program a Logix5000 controller to use equipment phases. |
| Programming tasks and procedures | Logix5000 Controllers Common Procedures Programming Manual, publication 1756-PM001 | Provides access to the Logix5000 Controllers set of programming manuals, which cover such topics as how to manage project files, organize tags, program logic, test routines, handle faults, and more. |
| | Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087 | Helps with how to estimate memory use and execution time of programmed logic, and how to select different programming options. |

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



## Safety Application Requirements

The GuardLogix 5570 controller system is certified for use in safety applications up to and including Safety Integrity Level Claim Limit (SIL CL) 3 and Performance Level (e) where the de-energized state is the safe state. Safety application requirements include probability of failure rates evaluation, such as:

- Probability of failure on demand (PFD)
- Probability of failure per hour (PFH)
- System reaction-time settings
- Functional-verification tests that fulfill SIL 3/PLe criteria

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

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

### 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 safety I/O device must also be configured with the SNN of the safety subnet. The SNN can be assigned automatically or manually.

For information on how to assign the SNN, see Manage the Safety Network Number (SNN) on page 49.

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

See Generate a Safety Task Signature on page 104 for more information.

## Distinguish between Standard and Safety Components

Slots of a GuardLogix system chassis that are not used by the safety function can be populated with other ControlLogix modules that are certified to the Low Voltage and EMC Directives. See http://www.rockwellautomation.com/rockwellautomation/certification/ce.page to find the CE certificate for the Programmable Control>ControlLogix Product Family and determine the modules that are certified.

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

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

The ControlLogix Controllers User Manual, publication 1756-UM001, provides information on using ControlLogix devices in standard (nonsafety) applications.

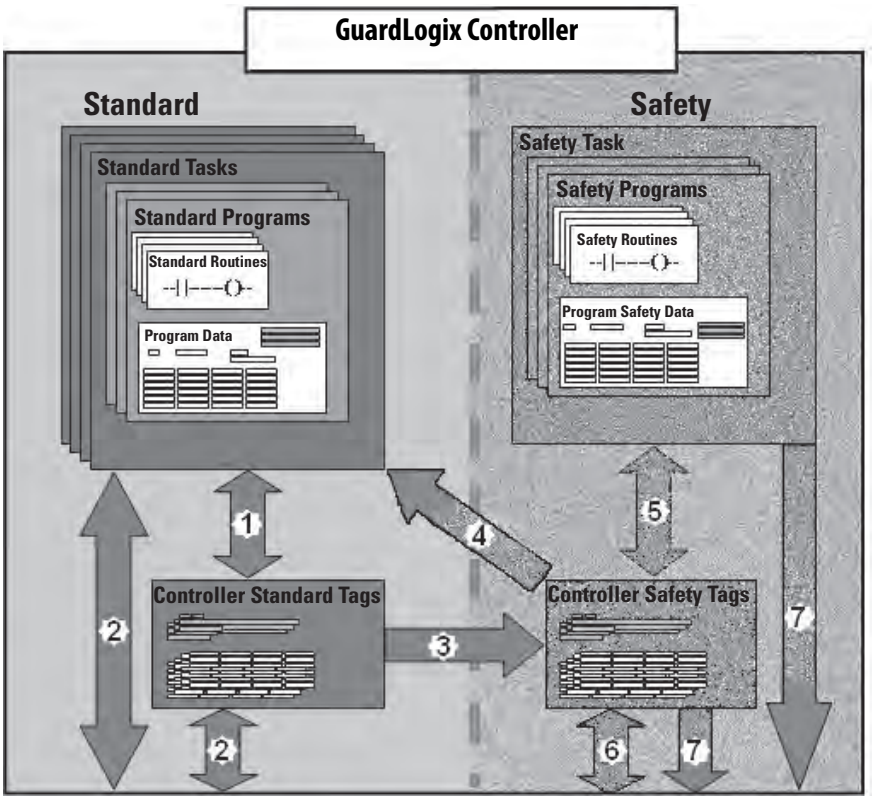
### HMI Devices

HMI devices can be used with GuardLogix controllers. HMI devices can access standard tags 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 GuardLogix controller.

**Figure 1 - Data-flow Capabilities**




| No. | Description |
|---|---|
| 1 | Standard tags and logic behave the same way that they do in the standard Logix platform. |
| 2 | Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers. |
| 3 | GuardLogix controllers are integrated controllers with the ability to move (map) standard tag data into safety tags for use within the safety task. |
| | **ATTENTION:** These data must not be used to control a SIL 3/PLe output directly. |
| 4 | Controller-scoped safety tags can be read directly by standard logic. |
| 5 | Safety tags can be read or written by safety logic. |
| 6 | Safety tags can be exchanged between safety controllers over Ethernet or ControlNet networks, including 1756 and 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. |
| | **IMPORTANT** Once this data is read, it is considered standard data, not SIL 3/PLe data. |

## Select System Hardware

The GuardLogix system supports SIL 3 and PLe safety applications. The GuardLogix controller is composed of a primary controller and a safety partner that function together in a 1oo2 architecture. Table 4 lists catalog numbers for primary controllers and safety partners.

The safety partner must be installed in the slot immediately to the right of the primary controller. The firmware major and minor revisions of the primary controller and safety partner must match exactly to establish the control partnership that is required for safety applications.

**Table 4 - Primary Controller and Corresponding Safety Partner Catalog Numbers**

| Primary Controller | Safety Partner |
|---|---|
| 1756-L71S, 1756-L72S, 1756-L73S | 1756-L7SP |
| 1756-L73SXT | 1756-L7SPXT |

### Primary Controller

The primary controller is the processor that performs standard and safety functions and communicates with the safety partner for safety-related functions in the GuardLogix control system. Standard functions include the following:

- I/O control
- Logic
- Timing
- Counting
- Report generation
- Communication
- Arithmetic computations
- Data file manipulation

The primary controller consists of a central processor, I/O interface, and memory.

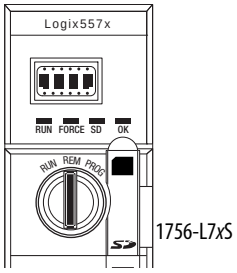
**Table 5 - Memory Capacity**

| Cat. No. | User Memory (RAM capacity) | |
|---|---|---|
| | Standard Tasks and Components | Safety Task and Components |
| 1756-L71S | 2 MB | 1 MB |
| 1756-L72S | 4 MB | 2 MB |
| 1756-L73S,1756-L73SXT | 8 MB | 4 MB |

A three-position key switch on the front of the primary controller governs the controller operational modes. The following modes are available:

- RUN
- PROGram
- REMote–this software-enabled mode can be Program, Run, or Test

**Figure 2 - Key Switch Positions**




### Safety Partner

The safety partner is a coprocessor that provides an isolated second channel (redundancy) for safety-related functions in the system.

The safety partner does not have a key switch or communication port. Its configuration and operation are controlled by the primary controller.

### Chassis

The ControlLogix chassis provides physical connections between modules and the GuardLogix controller.

### Power Supply

The ControlLogix power supplies listed on page 27 are suitable for use in SIL 3 applications. No extra configuration or wiring is required for SIL 3 operation of the power supplies.

## Select Safety I/O Device

Safety input and output devices, like sensors and actuators, can be connected to safety I/O on DeviceNet or EtherNet/IP networks. This connection controls output devices by a GuardLogix controller system via DeviceNet or EtherNet/IP communication.

For the most up-to-date information on available safety I/O catalog numbers, certified series, and firmware revisions, see the safety certificates at http://www.rockwellautomation.com/rockwellautomation/certification/safety.page.

## Select Communication Networks

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

- Distribute and control Safety I/O on DeviceNet or EtherNet/IP networks
- Distribute and control remote Safety I/O on DeviceNet, EtherNet/IP, or ControlNet networks
- Produce and consume safety tag data between 1756 and 1768 GuardLogix controllers across EtherNet/IP or ControlNet networks or within the same ControlLogix chassis
- Distribute and control standard I/O on Ethernet, ControlNet, or DeviceNet networks

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

**Table 6 - Communication Modules**

| To interface between | Use this module | See these installation instructions |
|---|---|---|
| The GuardLogix controller and DeviceNet devices | 1756-DNB | DNET-IN001 |
| The GuardLogix controller and EtherNet/IP devices | 1756-ENBT<br>1756-EN2T<br>1756-EN2F<br>1756-EN2TR<br>1756-EN3TR<br>1756-EN2TXT<br>1756-EN2TRXT | ENET-IN002 |
| Controllers on the ControlNet network | 1756-CN2<br>1756-CN2R<br>1756-CN2RXT | CNET-IN005 |

The GuardLogix controller can connect to the Logix Designer application via a USB port, an Ethernet module, or a ControlNet module.

See For More Information on page 13 for more information on network communication modules.

## Programming Requirements

Use Table 7 to identify the programming tool and the versions for use with your GuardLogix 5570 controllers.

**Table 7 - Software Versions**

| Cat. No. | Studio 5000 Environment | RSLogix 5000 Software Version(1) | RSLinx® Classic Software Version |
|---|---|---|---|
| 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT | 21 or later | 20 or later | 2.59 or later |

(1) For information on how to use a GuardLogix controller with RSLogix 5000 software, see GuardLogix Controllers User Manual, publication 1756-UM020, and GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093.

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

**Table 8 - Supported Features**

| Feature | Studio 5000 Logix Designer Application<br>Version 24 and Later | |
|---|---|---|
| | Safety Task | Standard Task |
| Add-on instructions | X | X |
| Alarms and events | | |
| Controller logging | X | |
| Data access control | | |
| Equipment phase routines | | |
| Event tasks | | |
| Firmware supervisor | X | |
| Function block diagrams (FBD) | | |
| Integrated motion | | |
| Ladder logic | X | |
| Language switching | | |
| Memory card | | |
| Network address translation (NAT) | | |
| Online import and export of program components | | |
| Safety and standard connections | X | |
| Sequential function chart (SFC) routines | | |
| Structured text | | |
| Unicast connections for produced and consumed safety tags | X | |
| Unicast connections for safety I/O devices on EtherNet/IP networks | | |

For information on how to use these features, refer to the Logix5000 Controllers Common Procedures Programming Manual, publication 1756-PM001, the publications that are listed in For More Information on page 13, and online help.

## Notes:

# Install the Controller



## 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 not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

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 help prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to help prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if 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 these publications for more information:

- 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 enclosure

## 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.

## Removal and Insertion Under Power (RIUP)

**WARNING:** When you insert or remove the module while backplane 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. Repeated electrical arcing causes excessive wear to contacts on both the module and its mating connector. Worn contacts may create electrical resistance that can affect module operation.

## 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.** |
|---|---|
| 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. | 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. |
| **WARNING:** EXPLOSION HAZARD<br>• Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.<br>• 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.<br>• Substitution of components may impair suitability for Class I, Division 2.<br>• If this product contains batteries, they must only be changed in an area known to be nonhazardous. | **AVERTISSEMENT:** RISQUE D'EXPLOSION<br>• Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement.<br>• 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.<br>• La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2.<br>• S'assurer que l'environnement est classé non dangereux avant de changer les piles. |

## 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:** Follow these guidelines to mount and use the equipment:

- Mount in an ATEX certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in IEC60529) and used in an environment of not more than Pollution Degree 2 (as defined in IEC 60664-1) when applied in Zone 2 environments. The enclosure must use a tool removable cover or door.
- Use within its specified ratings defined by Rockwell Automation.
- Use only with ATEX-certified Rockwell Automation backplanes.
- Do not disconnect unless power has been removed or the area is known to be nonhazardous.

Make provisions to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.

Secure any external connections that mate to this equipment with screws, sliding latches, threaded connectors, or other means provided with this equipment.

## Prevent Electrostatic Discharge

**ATTENTION:** This equipment is sensitive to electrostatic discharge that 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.

## Make Sure That You Have All of the Components

Before you begin, check to make sure you have all of the components you need.

**IMPORTANT** You must use a primary controller **and** a safety partner to achieve SIL 3/PLe.

These parts are included with the primary controller and safety partner.

| Cat. No. | Description | Ships with |
|---|---|---|
| 1756-L71S<br>1756-L72S<br>1756-L73S | Primary controller | • 1756-ESMCAP capacitor-based energy storage module (ESM)<br>• 1784-SD1 SD memory card, 1 GB<br>• 1747-KY key |
| 1756-L7SP | Safety partner | • 1756-SPESMNSE energy storage module (ESM) |
| 1756-L73SXT | Extreme temperature primary controller | • 1756-ESMCAPXT capacitor-based energy storage module (ESM)<br>• 1747-KY key |
| 1756-L7SPXT | Extreme temperature safety partner | • 1756-SPESMNSEXT capacitor-based energy storage module (ESM) |

The following optional equipment can be used.

| If your application requires | Then use this part |
|---|---|
| Nonvolatile memory | 1784-SD1 (1 GB) or 1784-SD2 (2 GB) |
| That the installed ESM depletes its residual stored energy to 200 µJ or less before transporting it into or out of your application(1) | 1756-ESMNSE for the primary controller<br>1756-SPESMNSE for the safety partner(2)<br>This ESM does not have WallClockTime backup power. Also, you can only use this ESM with a 1756-L73S (8 MB) or smaller memory sized controller. |
| ESM that secures the controller by preventing the USB port and SD card use(1) | 1756-ESMNRM for the primary controller<br>1756-SPESMNRM for the safety partner(3)<br>This ESM provides your application an enhanced degree of security. |

(1) For information about the hold-up time of the ESMs, see the section Estimate the ESM Support of the WallClockTime on page 121.
(2) For extreme temperature primary controller and safety partner use 1756-ESMNSEXT and 1756-SPESMNSEXT respectively.
(3) For extreme temperature primary controller and safety partner use 1756-ESMNRMXT and 1756-SPESMNRMXT respectively.

## Install a Chassis and Power Supply

Before you install a controller, you need to install a chassis and power supply.

1. Install a ControlLogix chassis according to the corresponding installation instructions.

| Cat. No. | Available Slots | Series | Refer to These Installation Instructions |
|---|---|---|---|
| 1756-A4 | 4 | B | 1756-IN005 |
| 1756-A7 | 7 | | |
| 1756-A10 | 10 | | |
| 1756-A13 | 13 | | |
| 1756-A17 | 17 | | |
| 1756-A4LXT | 4 | B | |
| 1756-A5XT | 5 | B | |
| 1756-A7XT | 7 | B | |
| 1756-A7LXT | 7 | B | |

Extreme environment (XT) controllers require an XT chassis.

2. Install a ControlLogix power supply according to the corresponding installation instructions.

| Cat. No. | Description | Series | Refer to These Installation Instructions |
|---|---|---|---|
| 1756-PA72 | Power supply, AC | C | 1756-IN005 |
| 1756-PB72 | Power supply, DC | | |
| 1756-PA75 | Power supply, AC | B | |
| 1756-PB75 | Power supply, DC | | |
| 1756-PAXT | XT power supply, AC | B | |
| 1756-PBXT | XT power supply, DC | | |

Extreme environment (XT) controllers require an XT power supply.

## Install the Controller Into the Chassis

You can install or remove a controller while chassis power is on and the system is operating.

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

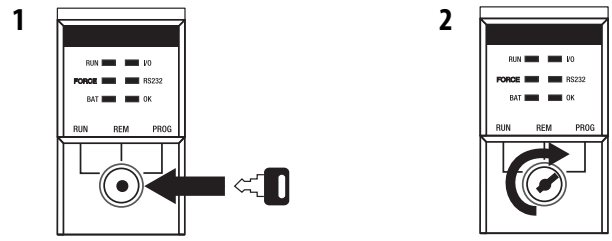
Be sure that power is removed or the area is nonhazardous before proceeding. Repeated electrical arcing causes excessive wear to contacts on both the module and its mating connector. Worn contact can create electrical resistance that can affect module operation.

**IMPORTANT** The ESM begins charging when one of these actions occurs:

- The controller and ESM are installed into a powered chassis.
- Power is applied to the chassis that contains a controller with the ESM installed.
- An ESM is installed into a powered controller.

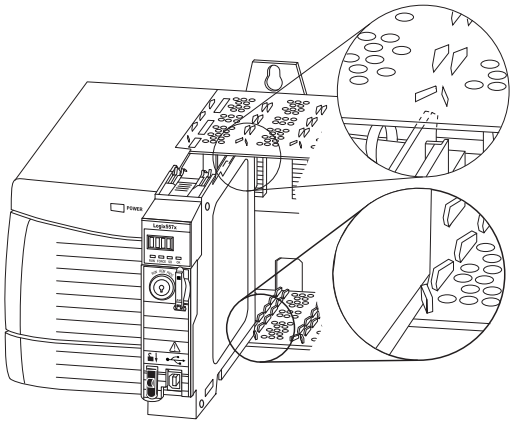
After power is applied, the ESM charges for up to two minutes as indicated by CHRG or ESM Charging on the status display.

1. Insert the key into the primary controller.
2. Turn the key to the PROG position.




The safety partner does not have a key switch.

3. Align the circuit board with the top and bottom guides in the chassis.



4. Slide the controller into the chassis.

   The controller is fully installed when it is flush with the power supply or other installed modules and the top and bottom latches are engaged.

**IMPORTANT** You must install the safety partner in the slot immediately to the right of the primary controller. Follow steps 3 and 4 above to install the safety partner.

After you have inserted the controller into the chassis, see Chapter 9 for information on interpreting the status indicators on the primary controller and safety partner.

## 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.

**ATTENTION:** If you are **not** sure of the contents of the memory card, **before** you install the card, turn the key switch of the controller to the PROG position. Depending on the contents of the card, a power cycle or fault could cause the card to load a different project or operating system into the controller.

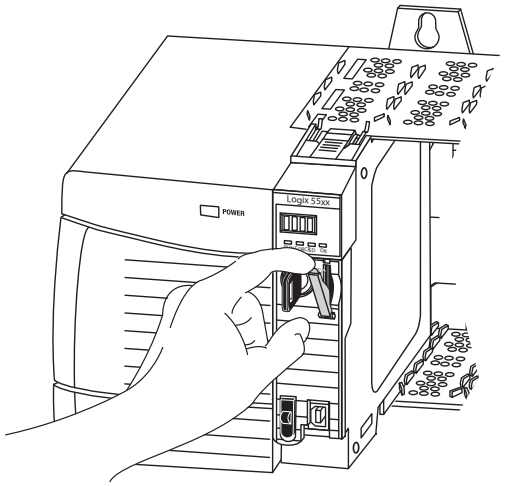
The controller ships with an SD card installed. We recommend that you leave an SD card installed.

## Remove the SD Card

Follow these steps to remove the SD card.

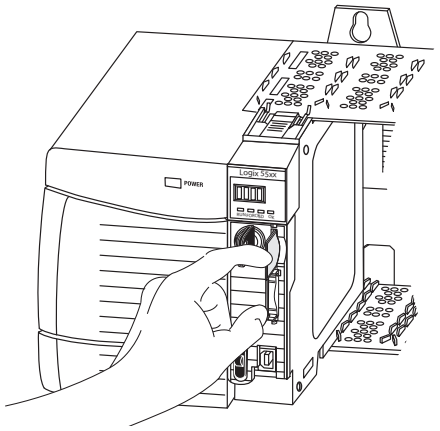
**IMPORTANT** Verify that the SD card status indicator is off and that the card is not in use before removing it.

1. Turn the key switch to the PROG position.
2. Open the door to access the SD card.




32015-M

3. Press and release the SD card to eject it.



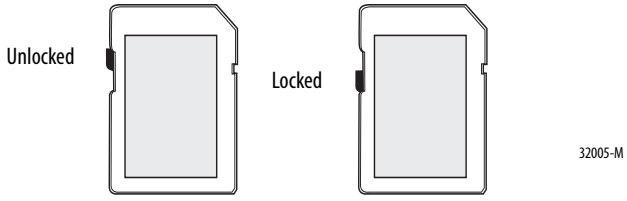

32004-M

4. Remove the SD card and close the door.

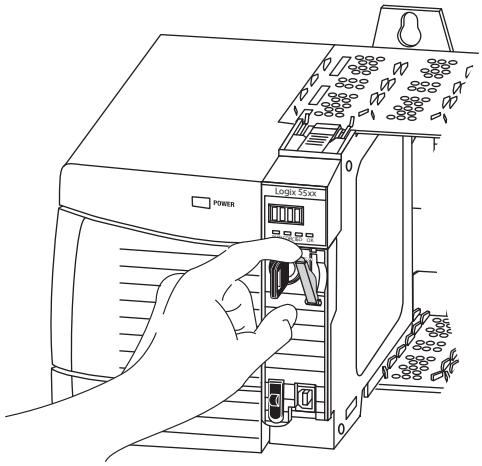
## Install the SD Card

Follow these steps to install the SD card.

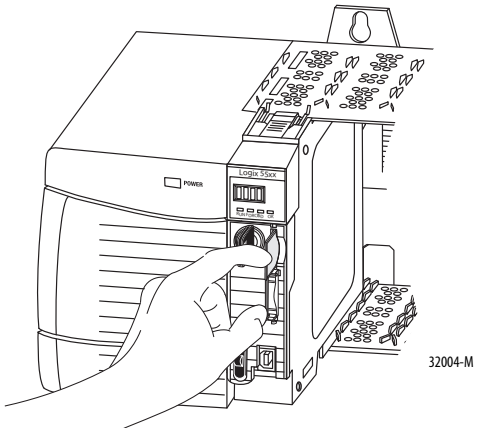
1. Verify that the SD card is locked or unlocked according to your preference.



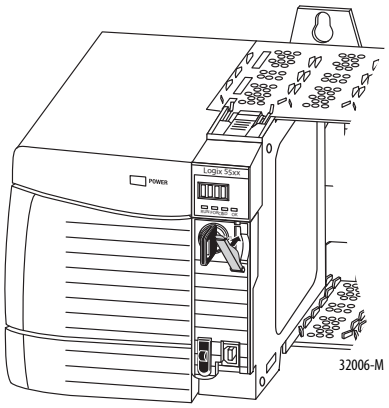

2. Open the door for the SD card.




3. Insert the SD card into the SD card slot.
4. Gently press the card until it clicks into place.



5. Close the SD card door.




## Make Communication Connections

The controller has a USB port that uses a Type B receptacle. The connection is USB 2.0-compatible and runs at 12 M.

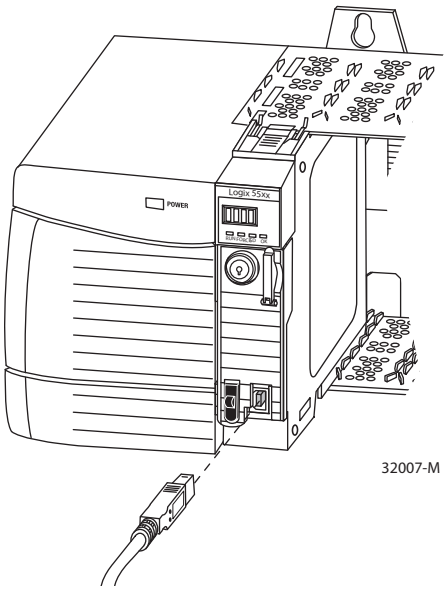
To use the USB port of the controller, you must have RSLinx software, version 2.59 or later, installed on your workstation. Use a USB cable to connect your workstation to the USB port. With this connection, you can upgrade firmware and download programs to the controller directly from your workstation.

**ATTENTION:** Use the USB port for temporary local programming purposes. Do not use the USB port as a permanent connection.

The USB cable must not exceed 3.0 m (9.84 ft) and must not contain hubs.

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

**Figure 3 - USB Port**



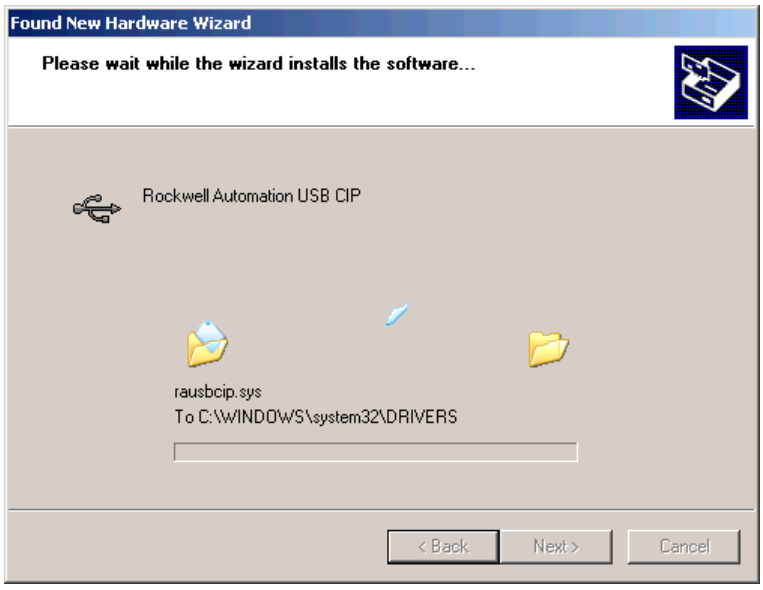
To configure RSLinx software to use a USB port, you need to first set up a USB driver. To set up a USB driver, perform this procedure.

1. Connect your controller and workstation by using a USB cable.
2. On the Found New Hardware Wizard dialog box, click any of the Windows Update connection options and click Next.


**TIP** If the software for the USB driver is not found and the installation is canceled, verify that you have installed RSLinx Classic software, version 2.59 or later.

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

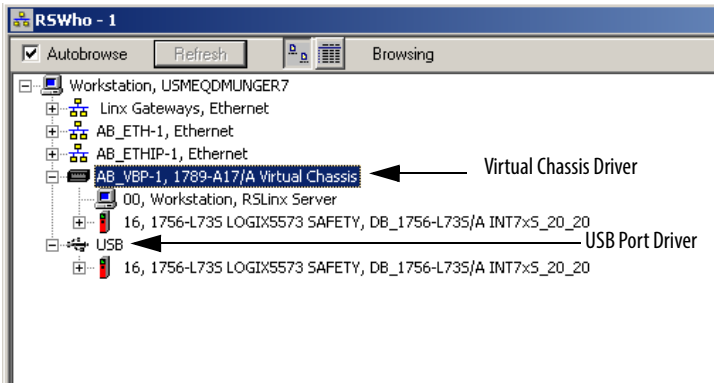
   The software is installed.




4. Click Finish to set up your USB driver.

5. To browse to your controller in RSLinx software, click RSWho  .

   In the RSLinx Workstation organizer, your controller appears under two different drivers, a virtual chassis and the USB port. You can use either driver to browse to your controller.




## Update the Controller

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

You can upgrade your firmware by using either ControlFLASH™ software or by using the AutoFlash feature of the Logix Designer application.

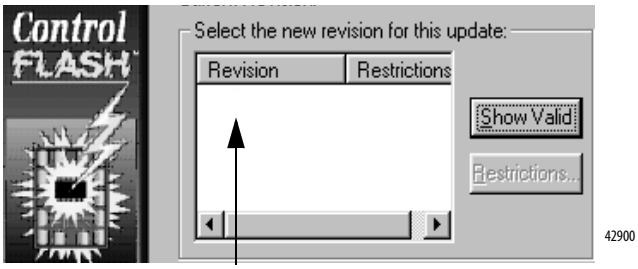
### Using ControlFLASH Software to Update Firmware

The safety partner updates automatically when the primary controller is updated.

| **IMPORTANT** | If the SD card is locked and the stored project's Load Image option is set to On Power Up, the controller firmware is not updated as a result of these steps. Any previously-stored firmware and projects are loaded instead. |
|---|---|

1. Verify that the appropriate network connection is made and the network driver has been configured in RSLinx software.
2. Start ControlFLASH software.
3. Choose Next.
4. Select the catalog number of the controller and click Next.
5. Expand the network until you see the controller.

6. Select the controller and click Next.




7. Select the revision level for the controller update and click Next.
8. To start the update of the controller, click Finish and then click Yes.

   After the controller is updated, the status dialog box displays 'Update complete'.

| **IMPORTANT** | Allow the firmware update to fully complete before cycling power or otherwise interrupting the upgrade. |
|---|---|

| **TIP** | If the ControlFLASH update of the controller is interrupted, the controller reverts to boot firmware, that is firmware revision 1.*xxx*. |
|---|---|

9. Click OK.
10. Close ControlFLASH software.

## Using AutoFlash to Update Firmware

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

1. Verify that the appropriate network connection is made and your network driver is configured in RSLinx software.
2. Use the Logix Designer application to create a controller project at the version you need.


3. Click RSWho to specify the controller path.

4. Select your controller and click Update Firmware.
5. Select the firmware revision you want.
6. Click Update.
7. Click Yes.

Allow the firmware update to complete without interruption. When the firmware upgrade is complete, the Who Active dialog box opens. You can complete other tasks in the Logix Designer application.

## Choose the Operating Mode of the Controller

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

**Table 9 - Controller Operation Modes**

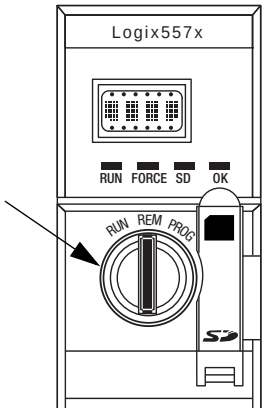
| If you want to | Select one of these modes | | | | |
|---|---|---|---|---|---|
| | Run | Remote | | | Program |
| | | Run | Test | Program | |
| Turn outputs to the state commanded by the logic of the project | X | X | | | |
| Turn outputs to their configured state for Program mode | | | X | X | X |
| Execute (scan) tasks | X | X | X | | |
| Change the mode of the controller through software | | X | X | X | |
| Download a project | | X | X | X | X |
| Schedule a ControlNet network | | | | X | X |
| While online, edit the project | | X | X | X | X |
| Send messages | X | X | X | | |
| Send and receive data in response to a message from another controller | X | X | X | X | X |
| Produce and consume tags | X | X | X | X | X |

### Use the Key Switch to Change the Operation Mode

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

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

**Figure 4 - Controller Key Switch**



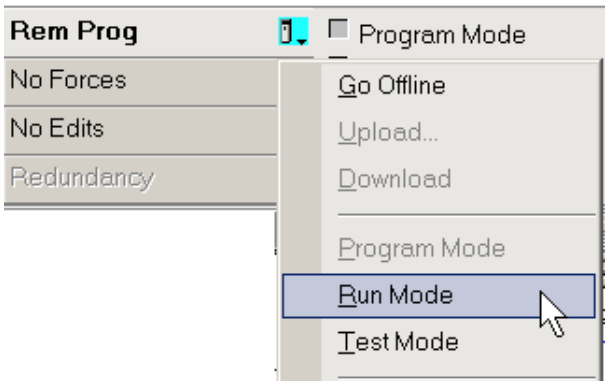

## Use the Logix Designer Application to Change the Operation Mode

Depending on the mode of the controller you specify by using the key switch, you can change the operation mode of the controller by using the Logix Designer application.

After you are online with the controller and the controller key switch is set to Remote (REM or the center position), you can use the Controller Status menu in the upper-left corner of the Logix Designer application window to specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

**Figure 5 - Operation Mode via the Logix Designer Application**




**TIP** For this example, the controller key switch is set to Remote Mode. If your controller key switch is set to Run Mode or Program Mode, the menu options change.

## Uninstall an Energy Storage Module (ESM)

The controllers ship with an ESM installed.

| Controller | Installed ESM Cat. No. |
|---|---|
| 1756-L7xS controller | 1756-ESMCAP |
| 1756-L7xSXT extreme temperature controller | 1756-ESMCAPXT |
| 1756-L7SP safety partner | 1756-SPESMNSE |
| 1756-L7SPXT extreme temperature safety partner | 1756-SPESMNSEXT |

Consider these points before removing the ESM:

- After the controller loses power, either because the chassis power is turned off or the controller has been removed from a powered chassis, do not remove the ESM immediately.

  Wait until the controller's OK status indicator transitions from Green to Solid Red to OFF before you remove the ESM.

- Use the 1756-ESMNSE module if your application requires that the installed ESM deplete its residual stored energy to 40 µJ or less before transporting it into or out of your application.

- Once it is installed, you cannot remove the 1756-ESMNRM module from the controller.

**IMPORTANT** Before you remove an ESM, make necessary adjustments to your program to account for potential changes to the WallClockTime attribute.

Follow these steps to remove a 1756-ESMCAP(XT), 1756-ESMNSE(XT), or 1756-SPESMNSE(XT) module.

**WARNING:** If your application requires the ESM to deplete its residual stored energy to 40 µJoule or less before you transport it into or out of the application, you must use the 1756-ESMNSE(XT) module for the primary controller and the 1756-SPESMNSE(XT) for the safety partner. In this case, complete these steps before you remove the ESM.

a. Turn power off to the chassis.

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

b. Wait **at least 20 minutes** for the residual stored energy to decrease to 40 µJ or less before you remove the ESM.

   There is no visual indication of when the 20 minutes has expired. **You must track that time period**.

**WARNING:** When you insert or remove the energy storage module while backplane 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. Repeated electrical arcing causes excessive wear to contacts on both the module and its mating connector.

1. Remove the key from the key switch.

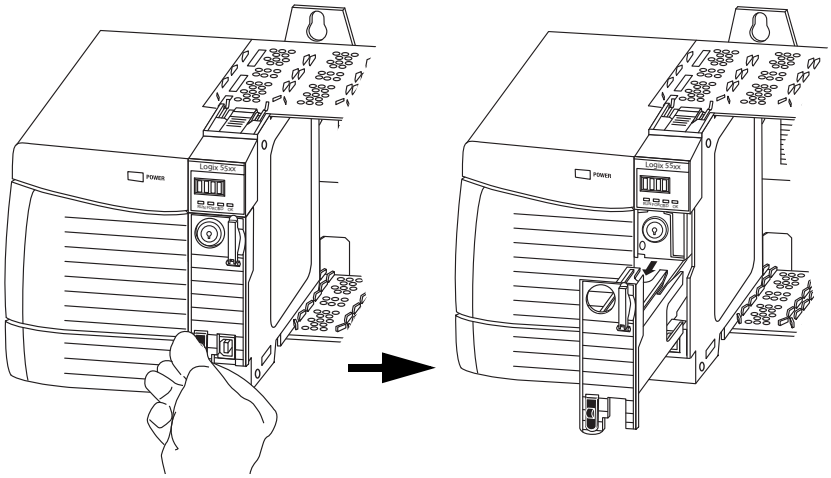
**IMPORTANT** The next step depends on the conditions that apply to your application:

- If you are removing the ESM from a powered controller, go to step 2.
- If you are removing the ESM from a controller that is not powered, either because the chassis power is turned off or the controller has been removed from a powered chassis, **do not remove** the ESM immediately.

  Wait until the controller's OK status indicator transitions from Green to Solid Red to OFF before you remove the ESM.

  After the OK status indicator transitions to OFF, go to step 2.

2. Use your thumb to press down on the black release and pull the ESM away from the controller.



## Install an Energy Storage Module (ESM)

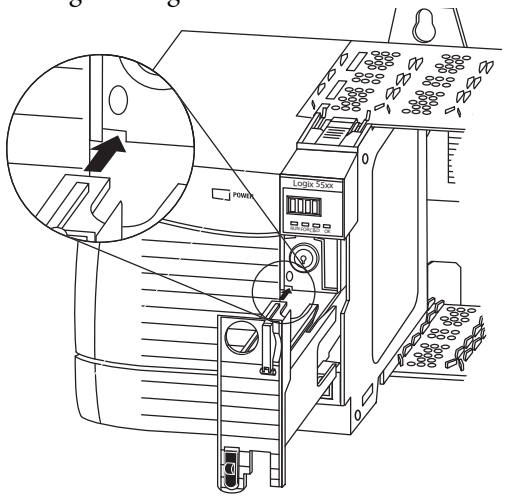
Table 10 lists the ESMs and the compatible GuardLogix controllers.

**Table 10 - Compatible Energy Storage Modules**

| Cat. No. | Compatible ESMs |
|---|---|
| 1756-L7*x*S | 1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM |
| 1756-L7*x*SXT | 1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT |
| 1756-L7SP | 1756-SPESMNSE, 1756-SPESMNRM |
| 1756-L7SPXT | 1756-SPESMNSEXT, 1756-SPESMNRMXT |

To install an ESM, complete these steps. Follow the same steps for the safety partner.

1. Align the tongue-and-groove slots of the ESM and controller.



2. Slide the ESM into the chassis until it snaps into place.

**ATTENTION:** To avoid potential damage to the product when inserting the ESM, align the ESM in the track and slide forward with minimal force until the ESM snaps into place.

The ESM begins charging after installation. Charging status is indicated by one of these status messages:

- ESM Charging
- CHRG

After you install the ESM, it can take up to 15 seconds for the charging status messages to display.

**IMPORTANT** Allow the ESM to finish charging before removing power from the controller. To verify that the ESM is fully charged, check the status display to confirm that messages 'CHRG' or 'ESM Charging' are no longer indicated.

**TIP** Check the WallClockTime object attributes after installing an ESM to verify that time of the controller is correct.

## Notes:

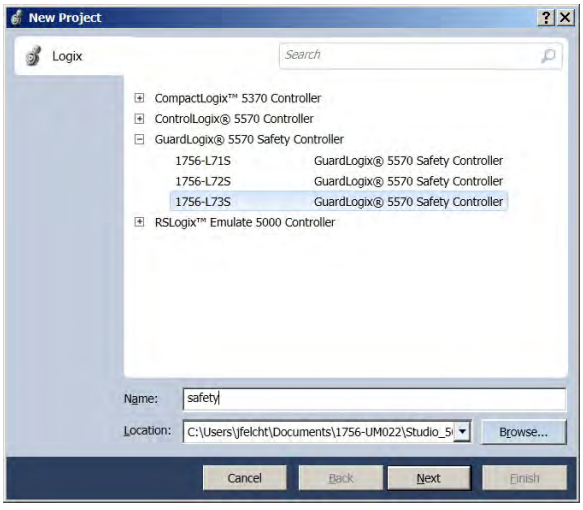
# Configure the Controller



## Create a Controller Project

To configure and program your controller, use the Logix Designer application to create and manage a project for the controller.

1. Click the New button  on the main toolbar to create a project.
2. Double-click GuardLogix 5570 Safety Controller to expand the list of controller options.
3. Choose a GuardLogix controller:
   - 1756-L71S GuardLogix 5570 Safety Controller
   - 1756-L72S GuardLogix 5570 Safety Controller
   - 1756-L73S GuardLogix 5570 Safety Controller

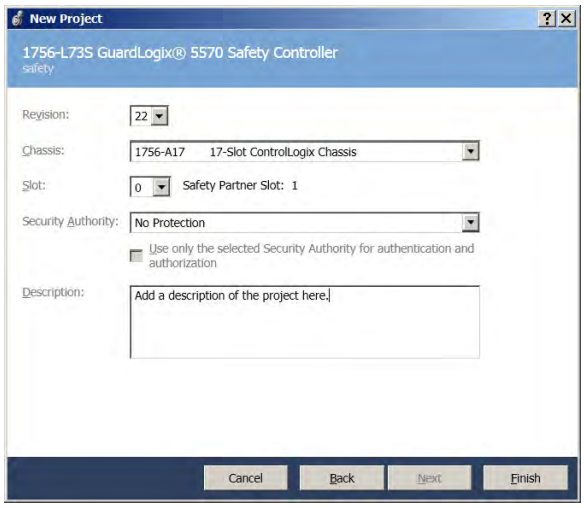



4. In the Name field, type the name of the project.
5. Click Browse to specify the folder for storing the safety controller project.
6. Click Next.

7. From the Revision pull-down menu, choose the major revision of firmware for the controller.
8. From the Chassis pull-down menu, choose the chassis size.
9. From the Slot pull-down menu, choose the slot for the safety partner.

   The New Project dialog box displays the slot location of the safety partner based on the slot number entered for the primary controller.

   If you select a slot number for the primary controller that does not accommodate placement of the safety partner immediately to the right of the primary controller, you are prompted to re-enter a valid slot number.



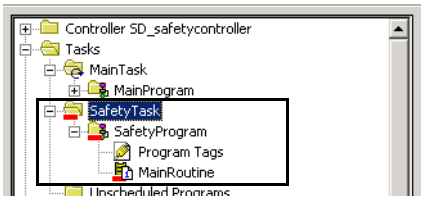

10. From the Security Authority pull-down menu, choose a security authority option.

    For detailed information on security, refer to the Logix5000 Controllers Security Programming Manual, publication 1756-PM016.

11. Check the box below Security Authority if you want to use the selected protection for authentication and authorization.
12. In the Description field, enter a description of the project.
13. Click Finish.

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

**Figure 6 - Safety Task in the Controller Organizer**



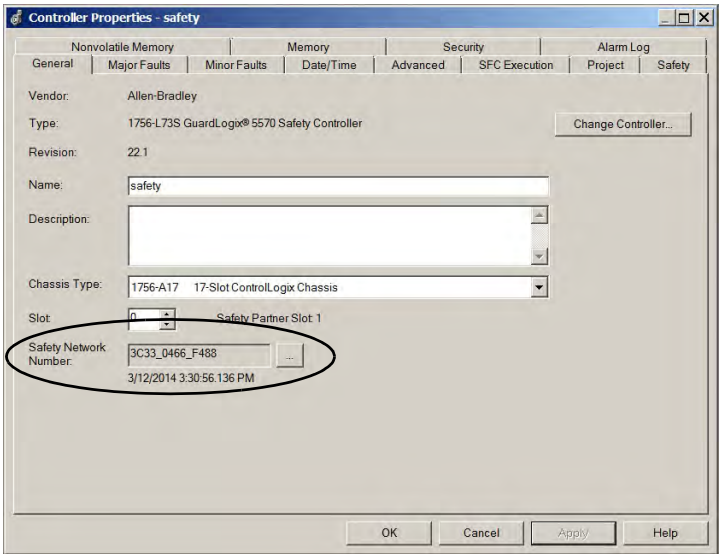

A red bar under the icon distinguishes safety programs and routines from standard project components in the Controller Organizer.

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

This SNN defines the local chassis backplane as a safety subnet. It can be viewed and modified via the General tab on the Controller Properties dialog box.

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

**Figure 7 - Safety Network Number**




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

See Appendix B, Change Controller Type, for details on the ramifications of changing controllers.

**Table 11 - Additional Resources**

| Resource | Description |
|---|---|
| Chapter 6, Develop Safety Applications | Contains more information on the safety task, safety programs, and safety routines. |
| Chapter 4, Communicate over Networks | Provides more information on managing the SSN. |

## Electronic Keying

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

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

The following Electronic Keying options are available.

| Keying Option | Description |
|---|---|
| Compatible Module | Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has the following characteristics:<br>• Same catalog number<br>• Same or higher Major Revision<br>• Minor Revision as follows:<br>– If the Major Revision is the same, the Minor Revision must be the same or higher.<br>– If the Major Revision is higher, the Minor Revision can be any number. |
| Exact Match | Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur. Exact Match is required if you are using Firmware Manager. |

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

**IMPORTANT** Changing Electronic Keying parameters online interrupts connections to the device and any devices that are connected through the device. Connections from other controllers can also be broken.

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

### More Information

For more detailed information on Electronic Keying, see Electronic Keying in Logix5000 Control Systems Application Technique, publication LOGIX-AT001.

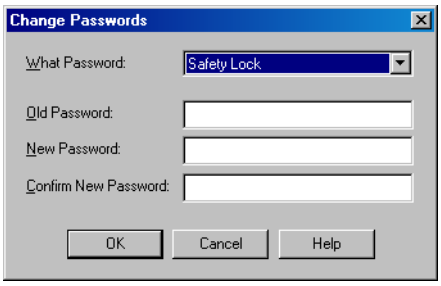
## Set Passwords for Safety-locking and -unlocking

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

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

Follow these steps to set passwords.

1. Click Tools > Safety > Change Passwords.
2. From the What Password pull-down menu, choose either Safety Lock or Safety Unlock.




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

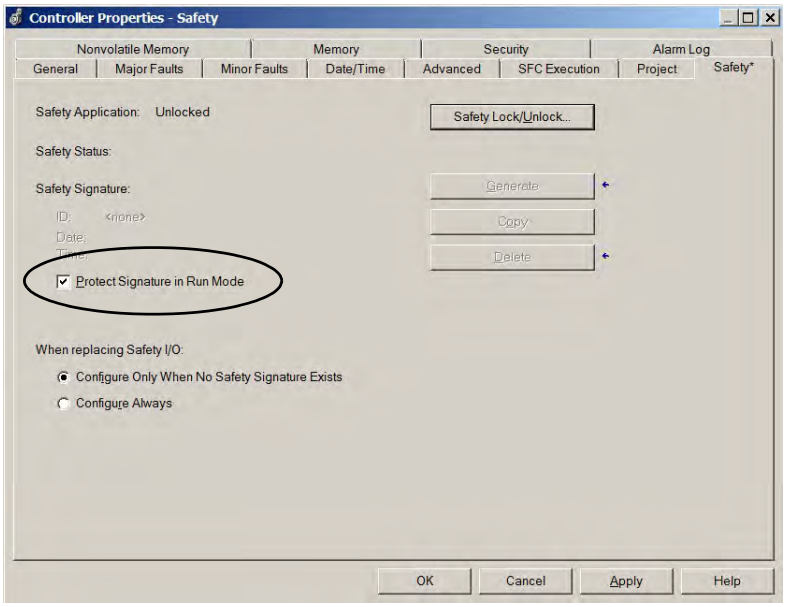
   Passwords can be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols can be used: ‘ ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .

## Protect the Safety Task Signature in Run Mode

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

Follow these steps to protect the safety task signature:

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



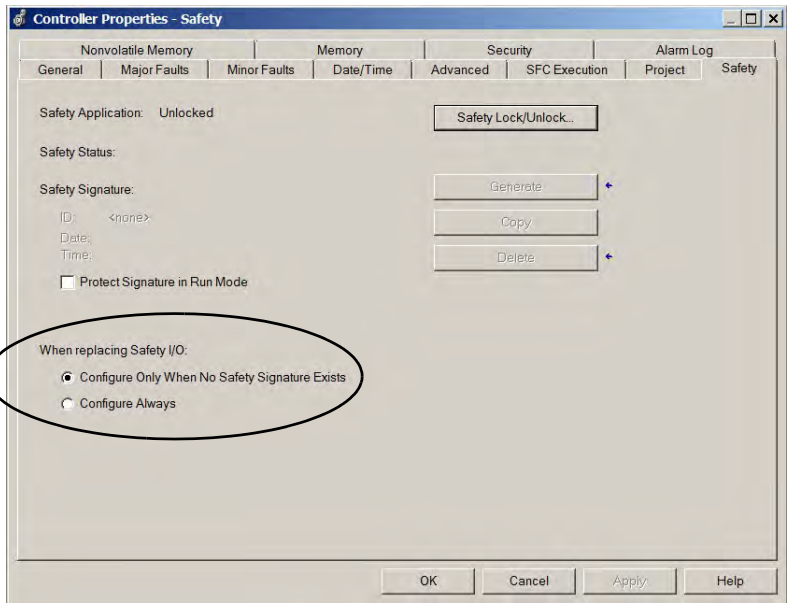
## Handling I/O Device Replacement

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

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

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

**Figure 8 - I/O Device 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 device.

See Chapter 5, Add, Configure, Monitor, and Replace CIP Safety I/O Devices for more information.

(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 16 and Generate a Safety Task Signature on page 104 for more information.

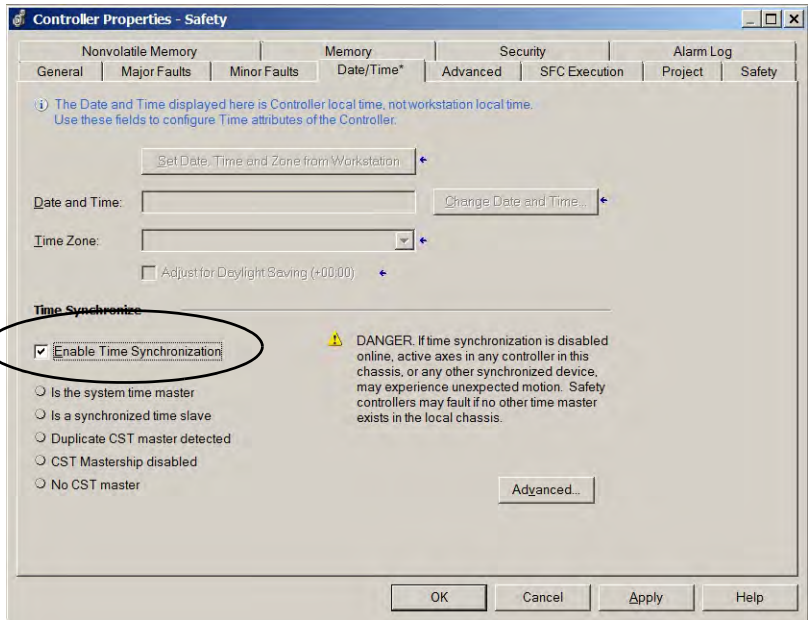
## Enable Time Synchronization

In a GuardLogix controller system, one device in the local chassis must be designated as the coordinated system time (CST) master. Time synchronization provides a standard mechanism to synchronize clocks across a network of distributed devices.

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

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

**Figure 9 - 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 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 94.

# Communicate over Networks



## The Safety Network

The CIP safety protocol is an end-node to end-node safety protocol that provides routing of CIP safety messages to and from safety I/O devices through bridges, switches, and routers.

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

### Manage the Safety Network Number (SNN)

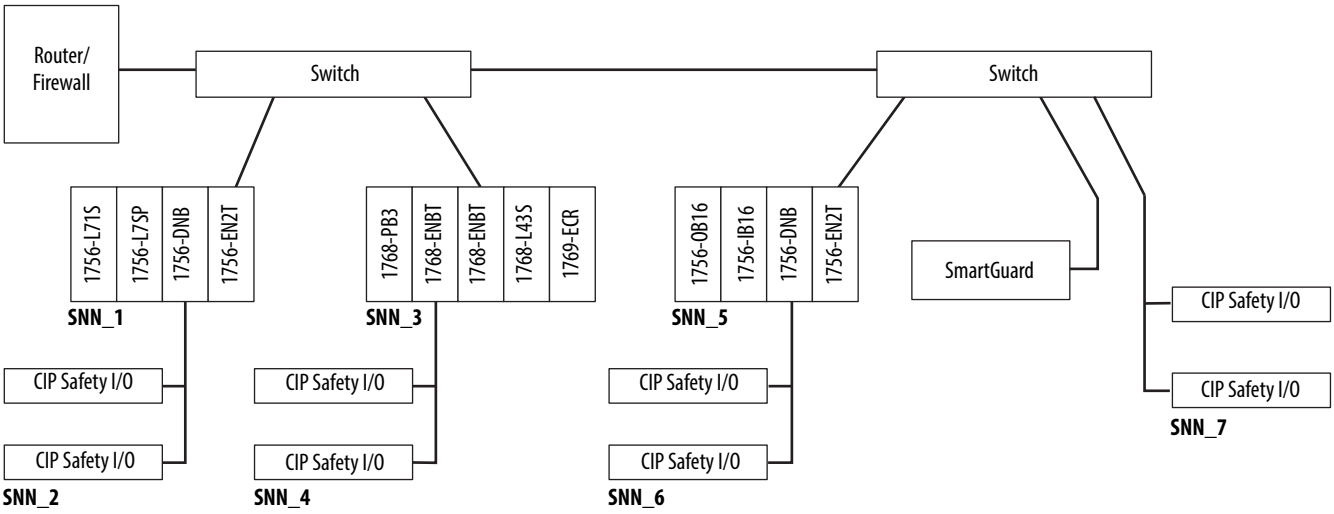
The SNN assigned to safety devices on a network segment must be unique. You must be sure that a unique SNN is assigned to the following:

- Each CIP safety network that contains safety devices
- Each chassis that contains one or more GuardLogix controllers

**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 has only one unique SNN.

Figure 10 shows a CIP safety system with seven different subnets where each subnet has one unique SNN.

**Figure 10 - CIP Safety Example with More Than One SNN**

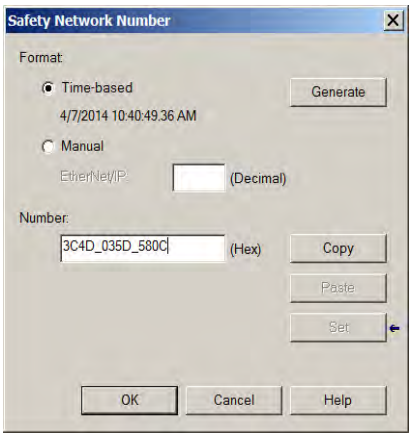



The SNN can be software-assigned (time-based) or user-assigned (manual). These two formats of the SNN are described in the following sections.

### *Time-based Safety Network Number*

If the time-based format is selected, the SNN value is the date and time when the number was generated, according to the computer running the configuration software.

**Figure 11 - Time-based Format**



*Manual Safety Network Number*

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

**Figure 12 - Manual Entry**


## Assign the Safety Network Number (SNN)

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

*Automatic Assignment*

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

*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 you can manage and assign the SNN in a logical manner for your specific application.

See Change the Safety Network Number (SNN) on page 52.

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

In Logix Designer version 24, a verification error occurs if your project contains duplicate SNN and node address combinations.

In Logix Designer version 26, a warning appears if your project contains duplicate SNN and node address combinations. You can still verify the project but Rockwell Automation recommends that you resolve the duplicate combinations.

*Automatic Versus Manual*

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.

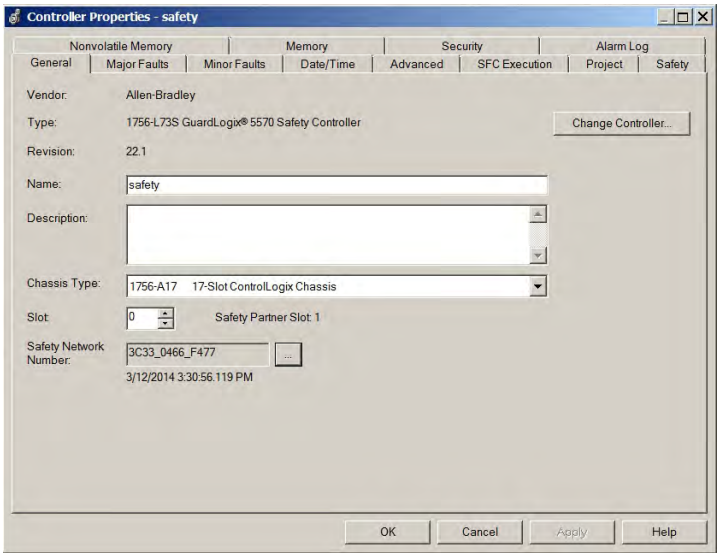
## Change the Safety Network Number (SNN)

Before changing the SNN you must do the following:

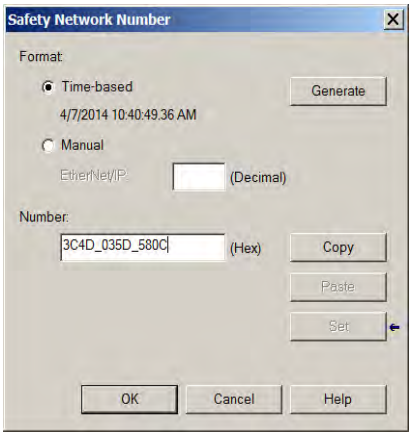
- Unlock the project, if it is safety-locked.
  See Safety-lock the Controller on page 103.
- Delete the safety task signature, if one exists.
  See Delete the Safety Task Signature on page 106.

*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.

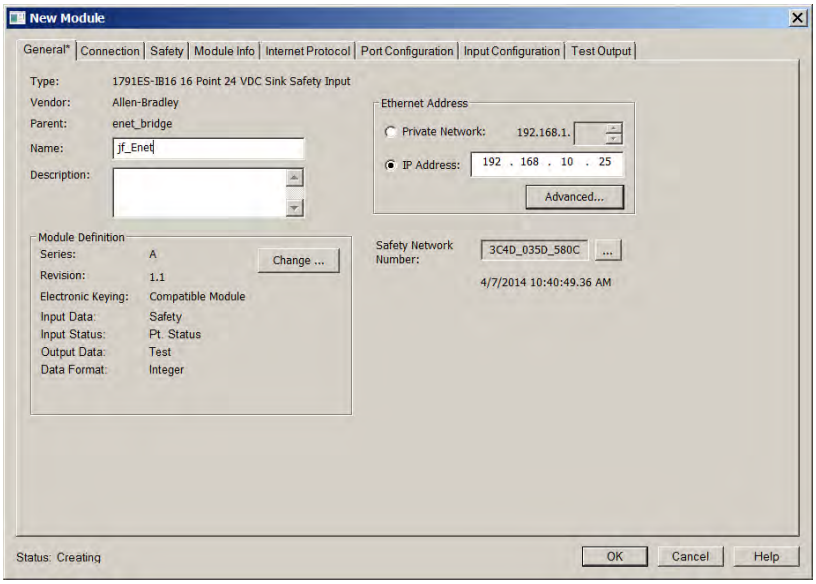



4. Click OK.

### *Change the Safety Network Number (SNN) of Safety I/O Devices 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 devices available through the EtherNet/IP communication module.
3. Double-click the first safety I/O device to view the General tab.



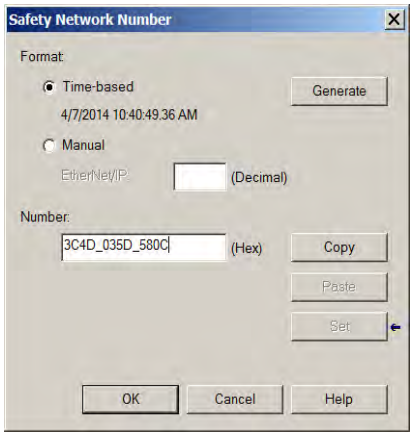

4. Click ... to the right of the safety network number to open the Safety Network Number dialog box.
5. Choose Time-based and click Generate to generate a new SNN for that EtherNet/IP network.
6. Click OK.

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 device 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 devices 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 can 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 device 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 EtherNet/IP network communication in a GuardLogix system, you have several modules to choose from. For CIP safety communication, including safety I/O device control, choose any of the modules shown in Table 12, except the 1756-EWEB module that does not support CIP safety communication.

Table 12 lists the modules and their primary features.

**Table 12 - EtherNet/IP Communication Modules and Capabilities**

| Module | Features |
|---|---|
| 1756-ENBT | • Connect controllers to I/O devices (requires an adapter for distributed I/O).<br>• Communicate with other EtherNet/IP devices (messages).<br>• Serve as a pathway for data sharing between Logix5000 controllers (produce/consume).<br>• Bridge EtherNet/IP nodes to route messages to devices on other networks. |
| 1756-EN2T | • Perform the same functions as a 1756-ENBT module, with twice the capacity for more demanding applications.<br>• Provide a temporary configuration connection via the USB port.<br>• Configure IP addresses quickly by using rotary switches. |
| 1756-EN2F | • Perform the same functions as a 1756-EN2T module.<br>• Connect fiber media by an LC fiber connector on the module. |
| 1756-EN2TXT | • Perform the same functions as a 1756-EN2T module.<br>• Operate in extreme environments with -25…70 °C (-13…158 °F) temperatures. |
| 1756-EN2TR | • Perform the same functions as a 1756-EN2T module.<br>• Support communication on a ring topology for a Device Level Ring (DLR) single-fault tolerant ring network. |
| 1756-EN2TRXT | • Perform the same functions as a 1756-EN2T module.<br>• Support communication on a ring topology for a Device Level Ring (DLR) single-fault tolerant ring network.<br>• Operate in extreme environments with -25…70 °C (-13…158 °F) temperatures. |
| 1756-EN3TR | • Perform the same functions as the 1756-EN2TR module.<br>• Two ports for DLR connection. |
| 1756-EWEB | • Provide customizable web pages for external access to controller information.<br>• Provide remote access via an Internet browser to tags in a local ControlLogix controller.<br>• Communicate with other EtherNet/IP devices (messages).<br>• Bridge EtherNet/IP nodes to route messages to devices on other networks.<br>• Support Ethernet devices that are not EtherNet/IP-based with a socket interface.<br>This module does not provide support for I/O or produced/consumed tags, and does not support CIP safety communication. |

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 products are available for EtherNet/IP networks.

**Table 13 - Product for EtherNet/IP Modules**

| Product | Is Used to | Required |
|---|---|---|
| Studio 5000 environment | • Configure the controller project<br>• Define EtherNet/IP communication | Yes |
| BOOTP/DHCP utility[1] | Assign IP addresses to devices on an EtherNet/IP network | No |
| RSNetWorx™ for EtherNet/IP software | Configure EtherNet/IP devices by IP addresses and/or host names | No |
| RSLinx software | • Configure devices<br>• Establish communication between devices<br>• Provide diagnostics | Yes |

(1) This utility comes with the Studio 5000 environment.

## 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 an MSG instruction). Unscheduled messaging lets you send and receive data when needed.

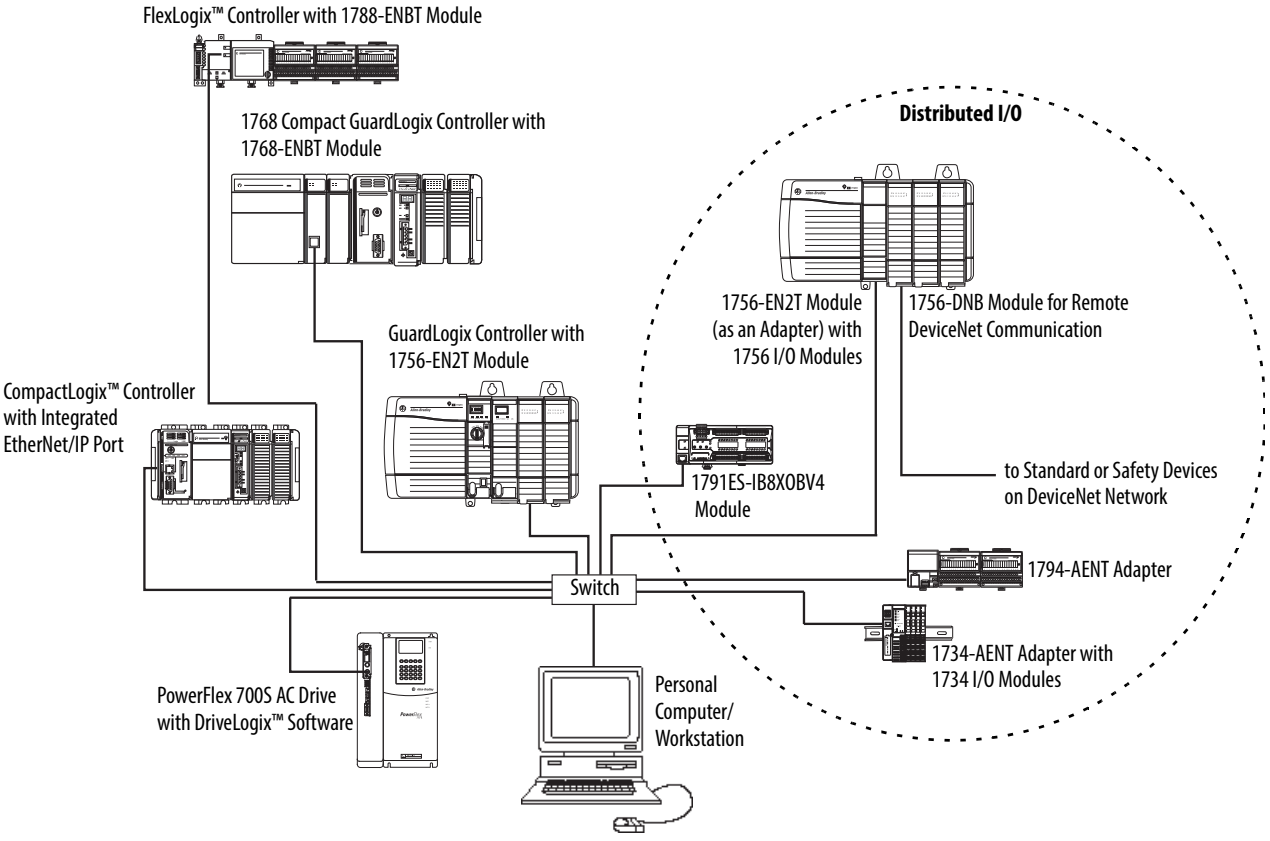
The EtherNet/IP communication modules support 128 Common Industrial Protocol (CIP) connections over an EtherNet/IP network.

## EtherNet/IP Communication Examples

Figure 13 illustrates the following communication functions:

- 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.(1)
- The EtherNet/IP communication module is used as a bridge, letting the safety controller produce and consume standard and safety data.
- The workstation can upload/download projects to the controllers.
- The workstation can configure devices on t=-09e EtherNet/IP network.

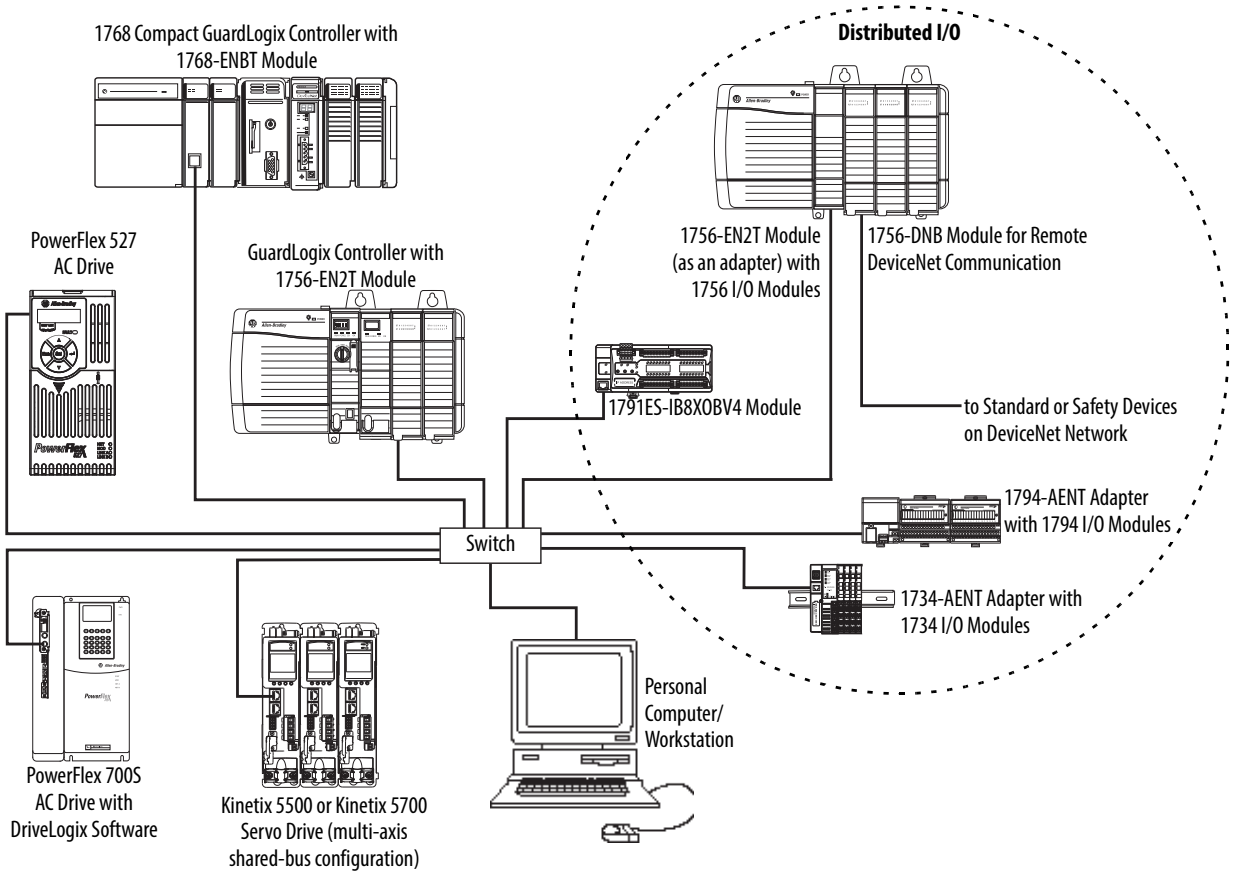
**Figure 13 - EtherNet/IP Communication Example**




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

In the Logix Designer application, version 24 and later, the controller supports both standard and safety via a single connection.

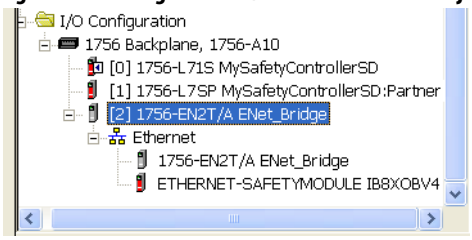
**Figure 14 - EtherNet/IP Communication with Standard and Safety Connection Example**



## EtherNet/IP Connections for Safety I/O Devices

Safety I/O devices on EtherNet/IP networks are added to the project under the EtherNet/IP communication module as described in Add Safety I/O Devices on page 65. When you add a safety I/O device, the Logix Designer application automatically creates controller-scoped safety data tags for that device.

**Figure 15 - Adding EtherNet/IP Modules to the Project**



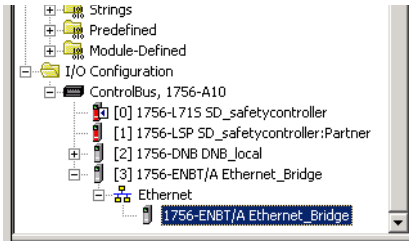

## Standard EtherNet/IP Connections

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 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 *xxx.xxx.xxx.xxx.* where each xxx is a number between 0 and 255. However, there are some values that you cannot use as the first octet in the address:<br>• 000.*xxx.xxx.xxx*<br>• 127.*xxx.xxx.xxx*<br>• 223…255.*xxx.xxx.xxx* |
| Subnet mask | Subnet addressing is an extension of the IP address scheme that lets a site 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.<br>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 GuardLogix controller project.




3. Use the Logix Designer application to download the project.

## ControlNet Communication

For ControlNet communication, choose a 1756-CNB or 1756-CNBR module for standard communication, or a 1756-CN2, 1756-CN2R, or 1756-CN2RXT module for safety communication.

**Table 14 - ControlNet Modules**

| If your application | Select |
|---|---|
| • Controls standard I/O devices<br>• Requires an adapter for distributed I/O on ControlNet links<br>• Communicates with other ControlNet devices (messages)<br>• Shares standard data with other Logix5000 controllers (produce/consume)<br>• Bridges ControlNet links to route messages to devices on other networks | 1756-CNB |
| • Performs same functions as a 1756-CNB module<br>• Also supports redundant ControlNet media | 1756-CNBR |
| • Performs the same functions supported by the 1756-CNB module with higher performance<br>• Supports CIP safety communication | 1756-CN2 |
| • Performs same functions as a 1756-CN2 module<br>• Also supports redundant ControlNet media | 1756-CN2R |
| • Perform the same functions as a 1756-CN2R module<br>• Operate in extreme environments with -25…70 °C (-13…158 °F) temperatures | 1756-CN2RXT |

These products are available for ControlNet networks.

**Table 15 - Products for ControlNet Modules**

| Product | Is Used to | Required |
|---|---|---|
| Studio 5000 environment | • Configure the GuardLogix project<br>• Define ControlNet communication | Yes |
| RSNetWorx for ControlNet software | • Configure the ControlNet network<br>• Define the network update time (NUT)<br>• Schedule the ControlNet network | Yes |
| RSLinx software | • Configure devices<br>• Establish communication between devices<br>• 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 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 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 16 - ControlNet Connections**

| Connection Type | Description |
|---|---|
| Scheduled<br>(unique to the ControlNet network) | A scheduled connection is unique to ControlNet communication. A scheduled connection lets you send and receive data repeatedly at a predetermined interval that is the requested packet interval (RPI). For example, a connection to an I/O device is a scheduled connection because you repeatedly receive data from the module at a specified interval. Other scheduled connections include connections to the following:<br>• Communication devices<br>• Produced/consumed tags<br>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. |
| Unscheduled | An unscheduled connection is a message transfer between controllers that is triggered by the requested packet interval (RPI) or the program (such as an MSG instruction). Unscheduled messaging lets you send and receive data when needed.<br>Unscheduled connections use the remainder of network bandwidth after scheduled connections are allocated.<br>Safety produced/consumed connections are unscheduled. |

The 1756-CNB and 1756-CNBR communication modules support 64 CIP connections over a ControlNet network. However, we recommend that you configure no more than 48 connections to maintain optimal performance.

The 1756-CN2 module supports 128 CIP connections over the ControlNet network.

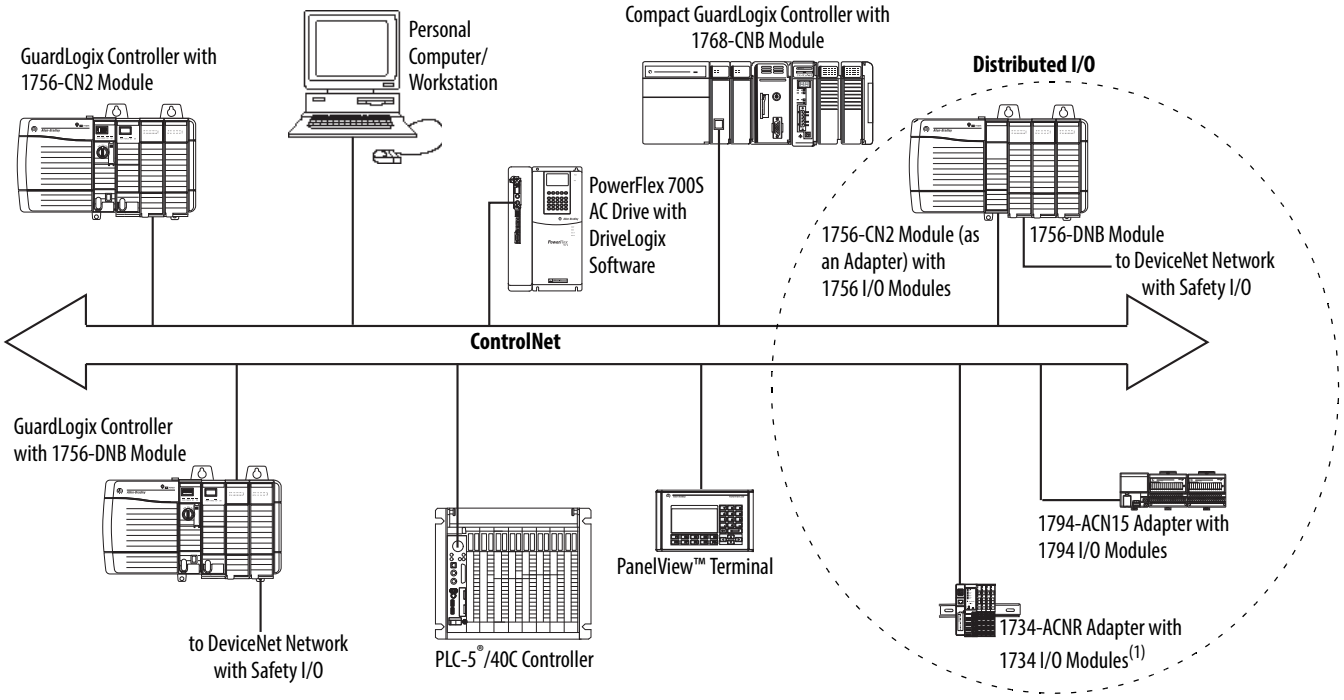
## ControlNet Communication Example

This example illustrates the following:

- GuardLogix controllers can produce and consume standard or safety tags between each other.
- GuardLogix controllers can initiate MSG instructions that send/receive standard data or configure devices.(1)
- The 1756-CN2 module can be used as a bridge, letting the GuardLogix controller produce and consume standard and safety data to and from I/O devices.
- 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) GuardLogix controllers do not support MSG instructions for safety data.

**Figure 16 - ControlNet Communication Example**




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

### ControlNet Connections for Distributed I/O

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

## DeviceNet Communication

To communicate and exchange data with safety I/O devices on DeviceNet networks, you need a 1756-DNB module in the local chassis.

For information on how to install your 1756-DNB module, refer to the ControlLogix DeviceNet Scanner Module Installation Instructions, publication 1756-IN566.

The 1756-DNB module supports communication with DeviceNet Safety devices and standard DeviceNet devices. You can use both types.

These products are used with the DeviceNet networks and 1756-DNB module.

**Table 17 - Product for Use with DeviceNet Networks**

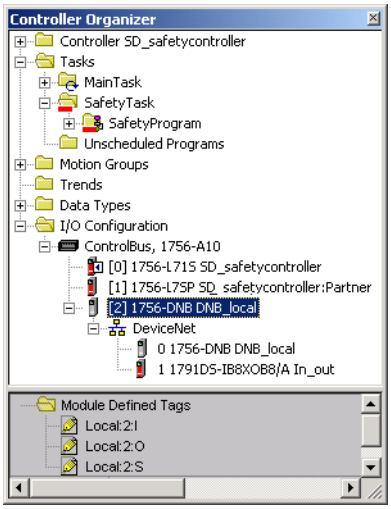
| Product | Is used to | Required |
|---|---|---|
| Studio 5000 environment | • Configure ControlLogix projects.<br>• Define DeviceNet communication. | Yes |
| RSNetWorx for DeviceNet software | • Configure DeviceNet devices.<br>• Define the scan list for those devices. | Yes |
| RSLinx Classic or<br>RSLinx Enterprise software | • Configure communication devices.<br>• Provide diagnostics.<br>• Establish communication between devices. | Yes |

## DeviceNet Connections for Safety I/O Devices

To access safety I/O devices on DeviceNet networks, add a 1756-DNB to the I/O Configuration tree of the GuardLogix controller project.

Safety I/O devices on DeviceNet networks are added to the project under the 1756-DNB module, as described in Chapter 5, Add, Configure, Monitor, and Replace CIP Safety I/O Devices. When you add a safety I/O device, the Logix Designer application automatically creates controller-scoped safety data tags for that device.

**Figure 17 - DeviceNet Module in Controller in the I/O Configuration Tree**




## Standard DeviceNet Connections

If you use standard DeviceNet I/O with your GuardLogix controller, you need to allocate two connections for each 1756-DNB module. One connection is for module status and configuration. The other connection is a rack-optimized connection for the DeviceNet I/O data.

To use the 1756-DNB module to access standard data via the DeviceNet network, you must use RSNetWorx for DeviceNet software to do the following:

- Create a configuration file for the network.
- Configure each standard device on the network.
- Configure the 1756-DNB.
- Add the standard I/O devices to the 1756-DNB scan list.

When you add the 1756-DNB module to the I/O Configuration of the controller, the Logix Designer application automatically creates a set of standard tags for the input, output, and status data of the network.

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



For more information on installation, configuration, and operation of safety I/O devices, refer to For More Information on page 13.

## Add Safety I/O Devices

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

- Node address for DeviceNet networks

  You cannot set the node address of a safety I/O device on DeviceNet networks via the Logix Designer application. Node addresses are set via rotary switches on the devices.

- IP address for EtherNet/IP networks

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

- Safety network number (SNN)

  See page 69 for information on setting the SNN.

- Configuration signature

  See page 73 for information on when the configuration signature is set automatically and when you need to set it.
- Reaction time limit

  See page 69 for information on setting the reaction time limit.
- Safety input, output, and test parameters complete the module configuration

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

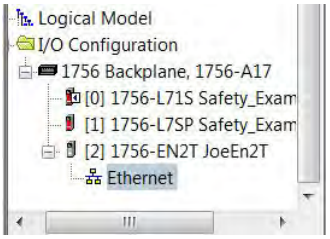
**TIP** Safety I/O devices support standard and safety data. Device configuration defines what data is available.

## Configure Safety I/O Devices

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

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

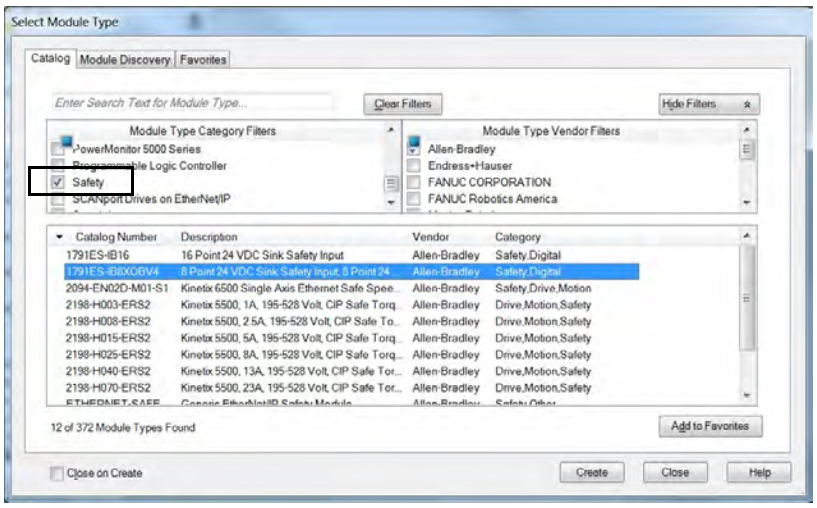
1. Right-click the DeviceNet or Ethernet network and choose New Module.




This example uses an Ethernet network.

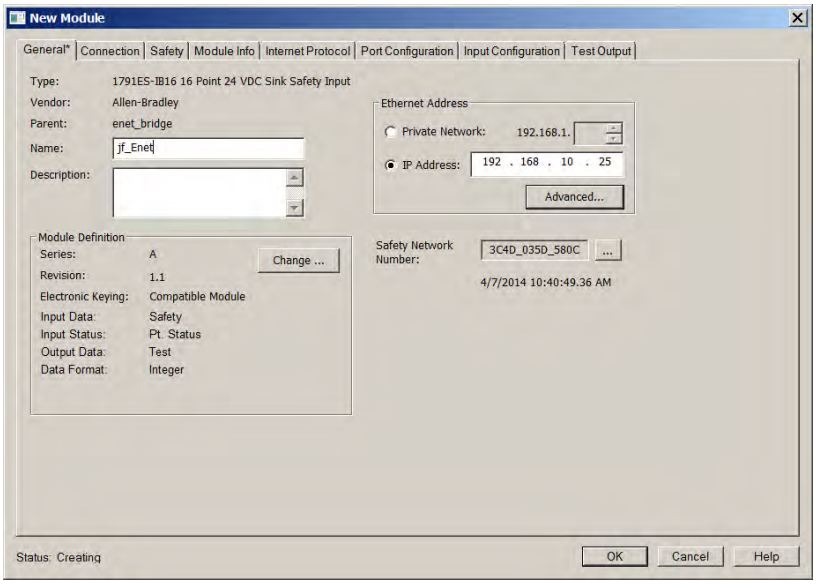
2. From the Catalog tab, select the safety I/O device.

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




3. Click Create.

4. Type a name for the new device.




5. To modify the Module Definition settings, click Change (if required).
6. Enter the node address for DeviceNet networks, or the IP address for EtherNet/IP networks.

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

   If your network uses network address translation (NAT), see Set the IP Address by Using Network Address Translation (NAT) on page 67.
7. To modify the Safety Network Number, click the ... button (if required).

   See page 69 for details.
8. Set the Connection Reaction Time Limit by using the Safety tab.

   See page 69 for details.
9. To complete configuration of the safety I/O device, refer to its user documentation and the Logix Designer application's online help.

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

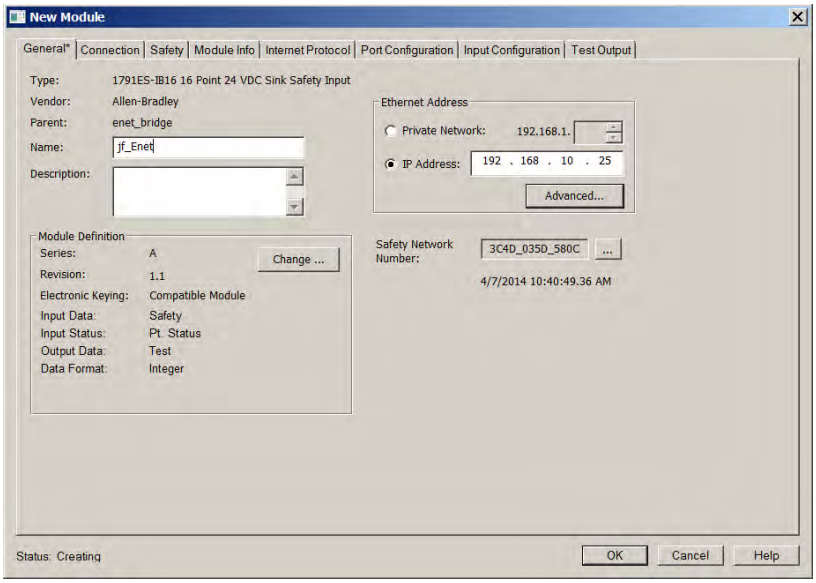
NAT translates one IP address to another IP address via a NAT-configured router or switch. The router or switch translates the source and destination addresses within data packets as traffic passes between subnets.

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

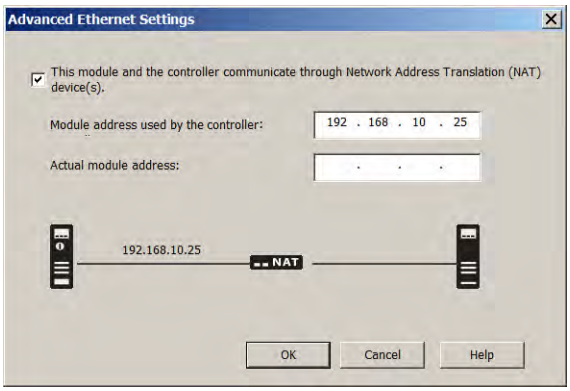
If you are using NAT, follow these steps to set the IP address.

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

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




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




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

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

5. Click OK.

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

## Set the Safety Network Number (SNN)

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

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

See Assign the Safety Network Number (SNN) on page 51.

## Use Unicast Connections on EtherNet/IP Networks

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

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

## Set the Connection Reaction Time Limit

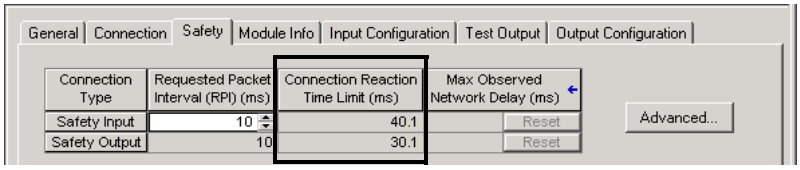
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. The Connection Reaction Time Limit is determined by the following equations:

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

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

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

**Figure 18 - Connection Reaction Time Limit**



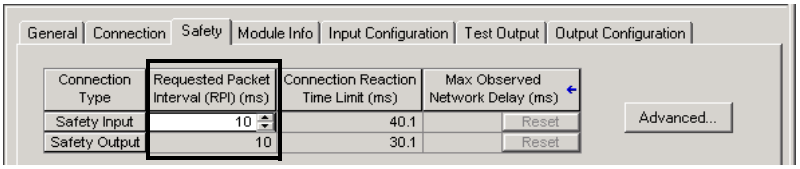

## Specify the Requested Packet Interval (RPI)

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

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

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

**Figure 19 - 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.

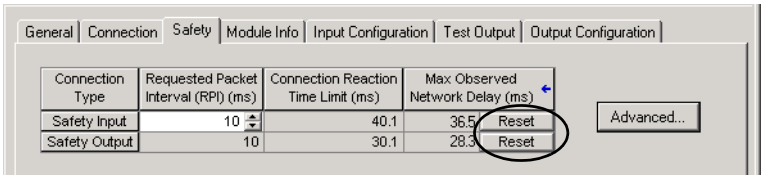
See Safety Task Period Specification on page 88 for more information on the safety task period.

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 71.

## View the Maximum Observed Network Delay

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

**Figure 20 - Reset the Max Observed Network Delay**

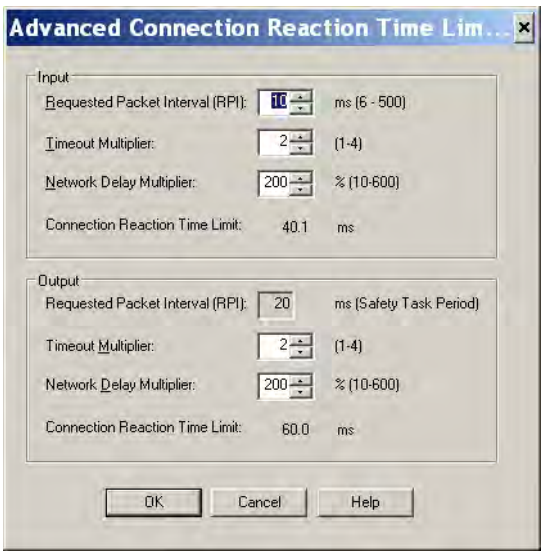



**IMPORTANT** The actual Maximum Network Delay time from the producer to the consumer is less than the value displayed in the Maximum Network Delay field on the Safety tab. In general, the actual maximum message delay is approximately one-half the Maximum Network Delay value that is displayed.

## Set the Advanced Connection Reaction Time Limit Parameters

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

**Figure 21 - 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 can be lost before a connection error is declared.

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

### *Network Delay Multiplier*

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 can 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 when all of the following conditions apply:

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

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

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

**EXAMPLE** **Calculate the Approximate Output Network Delay Multiplier**

If:

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

Then, the Output Network Delay Multiplier equals:

200% x [10 ÷ 20] = 100%

**Method 2:** Use the Maximum Observed Network Delay. If the system is run for an extended 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:

[Maximum Observed Network Delay + Margin_Factor] ÷ RPI

**EXAMPLE** **Calculate the Network Delay Multiplier from Maximum Observed Network Delay**

If:

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

Then, the Network Delay Multiplier equals:

[20 + 10] ÷ 50 = 60%

**Table 18 - More Information**

| Resource | Description |
|---|---|
| GuardLogix 5570 Controllers Systems Safety Reference Manual, publication 1756-RM099 | Provides information on calculating reaction times. |
| Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001 | |
| Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001 | |

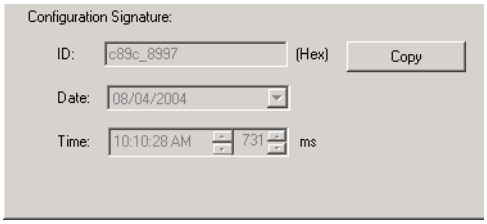
# Understanding the Configuration Signature

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

## Configuration via the Logix Designer Application

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

**Figure 22 - View and Copy the Configuration Signature**




## Different Configuration Owner (listen-only connection)

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

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

## Reset Safety I/O Device Ownership

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

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


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

## Address Safety I/O Data

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

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

### Safety I/O Modules Address Format

A Safety I/O module address follows this example.

**EXAMPLE** Modulename:Type.Member

**Table 19 - Safety I/O Device Address Format**

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

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

A Kinetix 5500, Kinetix 5700, and PowerFlex 527 drive address follows this example.

**EXAMPLE** Drivename:Type.Member

**Table 20 - Drive Safety I/O Device Address Format**

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

**Table 21 - More Resources**

| Resource | Description |
|---|---|
| Chapter 9, Monitor Status and Handle Faults | Contains information on monitoring safety tag data |
| Logix5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004 | Provides information on addressing standard I/O devices |

## Monitor Safety I/O Device Status

You can monitor safety I/O device status via Explicit Messaging or via the status indicators on the I/O modules. Refer to the Guard I/O manuals listed in For More Information on page 13 for information on I/O module troubleshooting.

**Table 22 - Status Indicator Operation for Guard I/O Modules**

| Indicator | Status | Description | | |
|---|---|---|---|---|
| | | Guard I/O DeviceNet Modules | Guard I/O EtherNet/IP Modules | POINT Guard I/O Modules |
| Module Status (MS) | Off | No power. | | |
| | Green, on | Operating under normal conditions. | | |
| | Green, flashing | Device is idle. | | |
| | Red, flashing | A recoverable fault exists. | A recoverable fault exists or a firmware update is in progress. | |
| | Red, on | An unrecoverable fault exists. | | |
| | Red/Green, flashing | Self-tests in progress. | Self-tests are in progress or the module is not configured properly. See the network status indicator for more information. | |

**Table 22 - Status Indicator Operation for Guard I/O Modules (Continued)**

| Indicator | Status | Description | | |
|---|---|---|---|---|
| | | **Guard I/O DeviceNet Modules** | **Guard I/O EtherNet/IP Modules** | **POINT Guard I/O Modules** |
| Network Status (NS) | Off | Device is not online or does not have power. | | |
| | Green, on | Device is online; connections are established. | | |
| | Green, flashing | Device is online; no connections established. | | |
| | Red, flashing | Communication timeout. | 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 | Device is in Communication Faulted state or safety network number (SNN) is being set. | Self-test in progress. | Not applicable. |
| Input Points (IN*x*) | 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 (O*x*) | 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. | | |
| Test Output Points (T*x*) | Off | Not applicable. | The output is OFF. | Not applicable. |
| | Yellow, on | | The output is ON. | |
| | Red, on | | An error has occurred in the output circuit. | |
| LOCK | Yellow, on | Device configuration is locked. | The Logix Designer application does not support this function. | |
| | Yellow, flashing | Device configuration is valid, but device is not locked. | | |
| | Yellow, off | Invalid, no configuration data, or device has been configured. | | |
| IN PWR | Green, off | No input power. | | Not applicable. |
| | 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. | | |
| PWR | Green, off | Not applicable. | | No power. |
| | Green, on | | | Power voltage is within specification. |
| | Yellow, on | | | Power voltage is out of specification. |

See page 13 for more information on the Kinetix 5500, Kinetix 5700, and PowerFlex 527 drive status indicators.

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

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

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

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

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


## Replace a Device by Using the Logix Designer Application

You can use the Logix Designer application to replace a safety I/O device on an Ethernet network. To replace a Guard I/O module on a DeviceNet network, your choice depends on the type of module.

**Table 23 - Software**

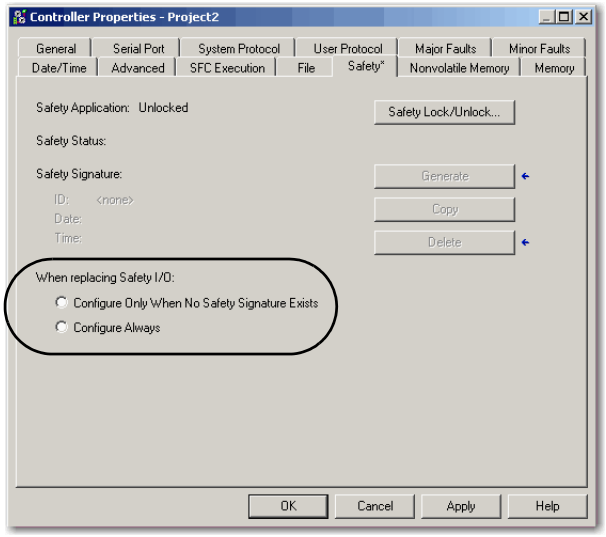
| If you are using a | Use | See |
|---|---|---|
| 1791DS Guard I/O module with 1756-DNB adapter | The Logix Designer application | Below |
| 1734 POINT Guard I/O module with a 1734-PDN adapter | RSNetWorx for DeviceNet software | Replace a POINT Guard I/O Module by Using RSNetWorx for DeviceNet Software on page 83 |

If you are relying on a portion of the CIP safety system to maintain SIL 3 behavior during device replacement and functional testing, the Configure Always feature cannot be used. Go to Replacement with 'Configure Only When No Safety Signature Exists' Enabled on page 78.

If the entire routable CIP safety control system is not being relied on to maintain SIL 3/PLe during the replacement and functional testing of a device, the Configure Always feature can be used. Go to Replacement with 'Configure Always' Enabled on page 82.

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

**Figure 23 - Safety I/O Device Replacement**




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

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

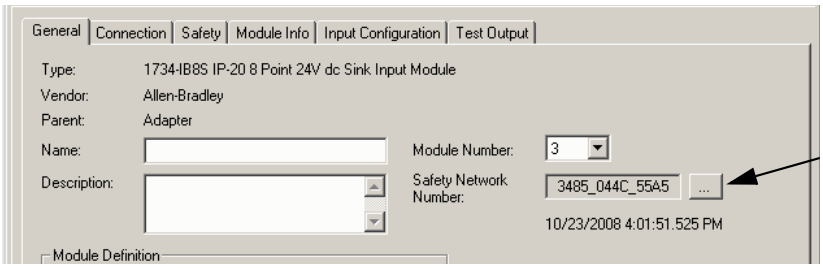
If the project is configured as 'Configure Only When No Safety Signature Exists', follow the appropriate steps in Table 24 to replace a safety I/O device based on your scenario. Once you have completed the steps correctly, the DeviceID matches the original, enabling the safety controller to download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

**Table 24 - Replacing a Module**

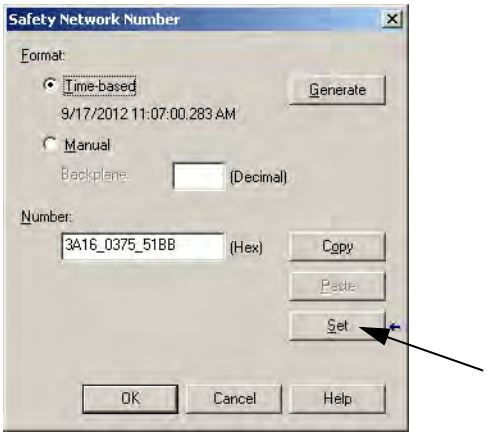
| GuardLogix Safety Signature Exists | Replacement Module Condition | Action Required |
|---|---|---|
| No | No SNN (Out-of-box) | None. The device is ready for use. |
| Yes or No | Same SNN as original safety task configuration | None. The device is ready for use. |
| Yes | No SNN (Out-of-box) | See Scenario 1 - Replacement Device is Out-of-box and Safety Signature Exists on page 79. |
| Yes | Different SNN from original safety task configuration | See Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists on page 79. |
| No | | See Scenario 3 - Replacement Device SNN is Different from Original and No Safety Signature Exists on page 81. |

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

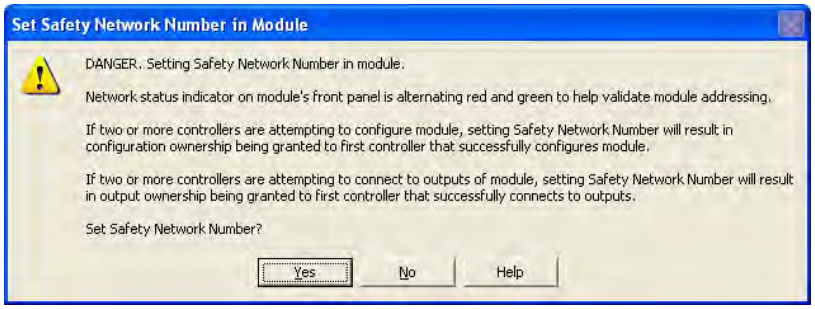
1. Remove the old I/O device and install the new device.
2. Right-click the replacement safety I/O device and choose Properties.
3. Click ... to the right of the safety network number to open the Safety Network Number dialog box.




4. Click Set.




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

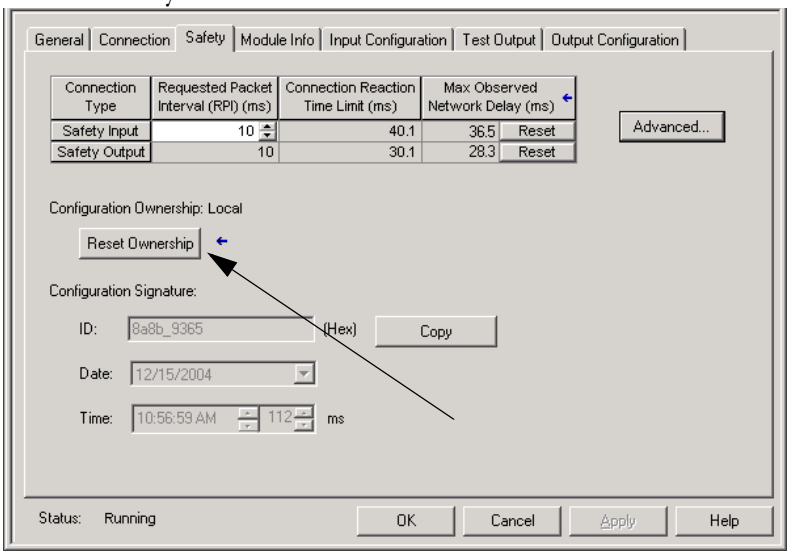



6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

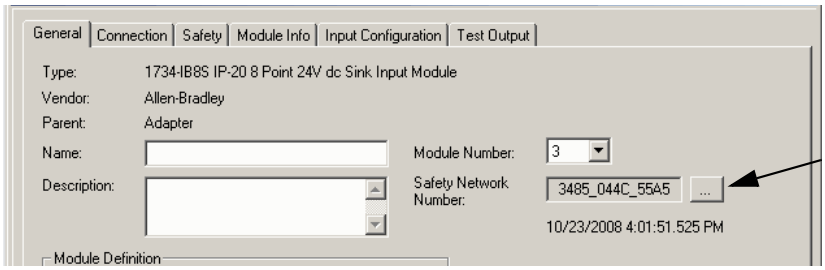
*Scenario 2 - Replacement Device SNN is Different from Original and Safety Signature Exists*

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

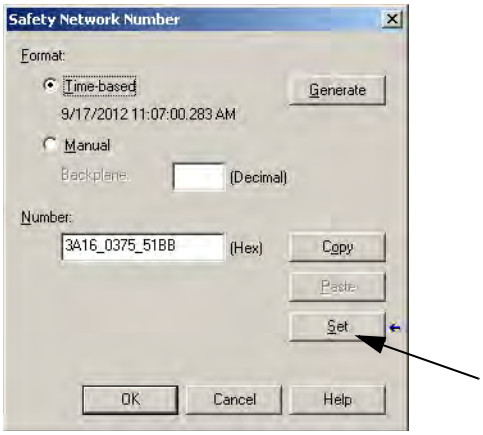
3. Click the Safety tab.



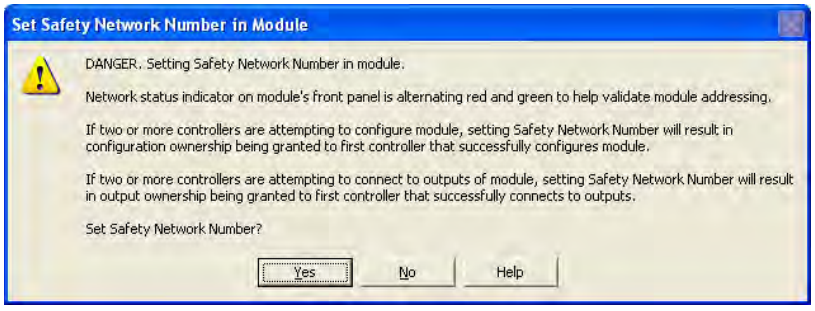

4. Click Reset Ownership.
5. Click OK.
6. Right-click the device and choose Properties.
7. Click ... to the right of the safety network number to open the Safety Network Number dialog box.




8. Click Set.



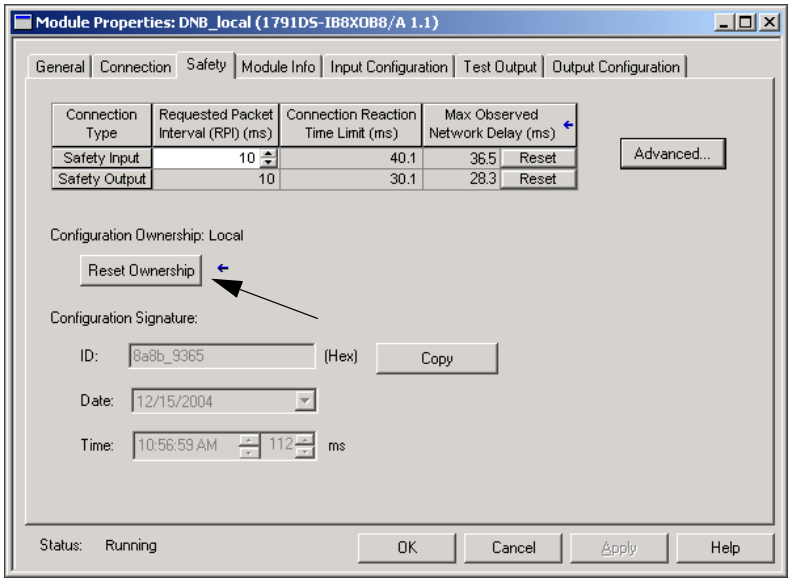
9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct device before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement device.




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

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

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




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

## Replacement with 'Configure Always' Enabled

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

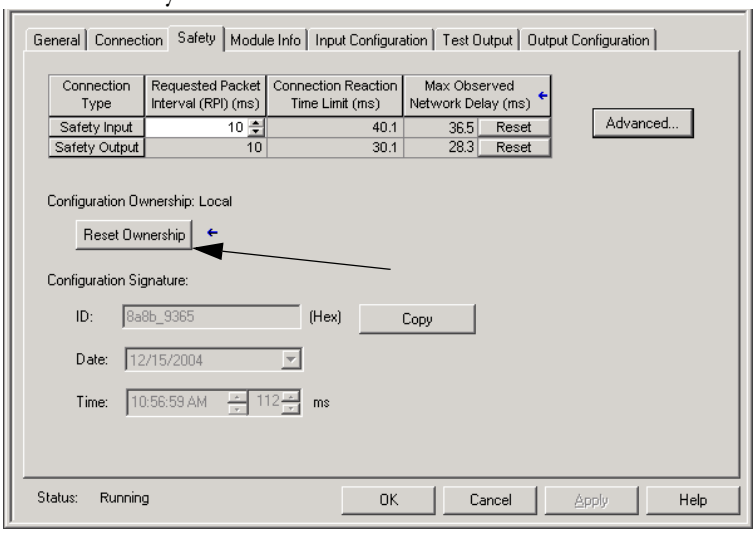
Do not place devices that are in the out-of-box condition on a CIP safety network when the Configure Always feature is enabled, except while following this replacement procedure.

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

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

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

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



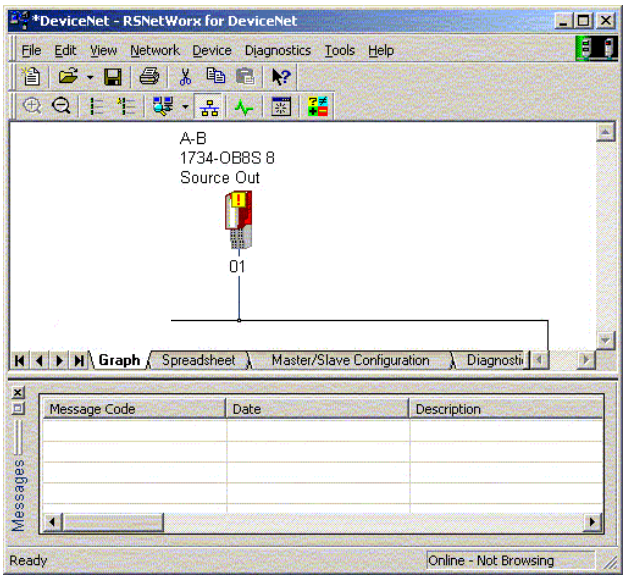

4. Click Reset Ownership.
5. Click OK.
6. Follow your company-prescribed procedures to functionally test the replaced I/O device and system and to authorize the system for use.

## Replace a POINT Guard I/O Module by Using RSNetWorx for DeviceNet Software

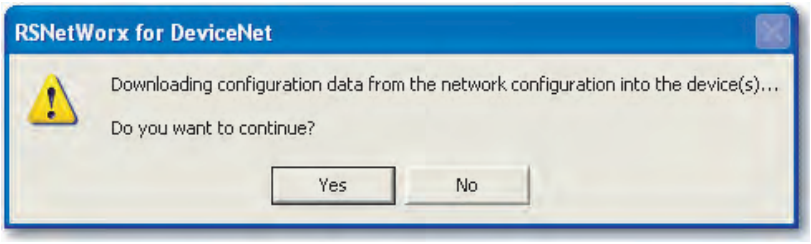
Follow these steps to replace a POINT Guard I/O module when the module and the controller are on a DeviceNet network.

1. Replace the module and match the node number of the original module.
2. In RSNetWorx for DeviceNet software, open your project.

   If the replacement module is out-of-box or has an SNN that does not match the original module, the module appears with an exclamation mark.

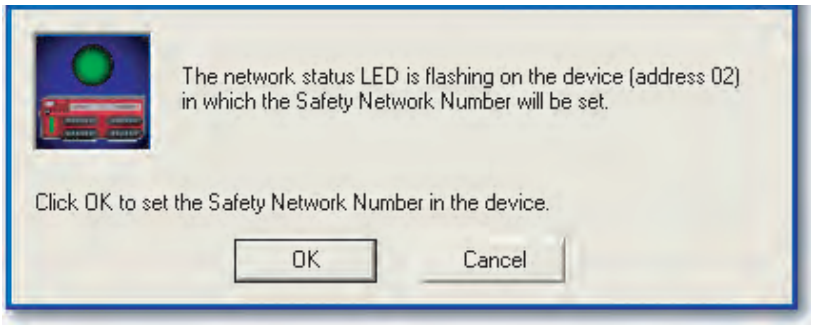



3. Right-click the module and choose Download to Device.



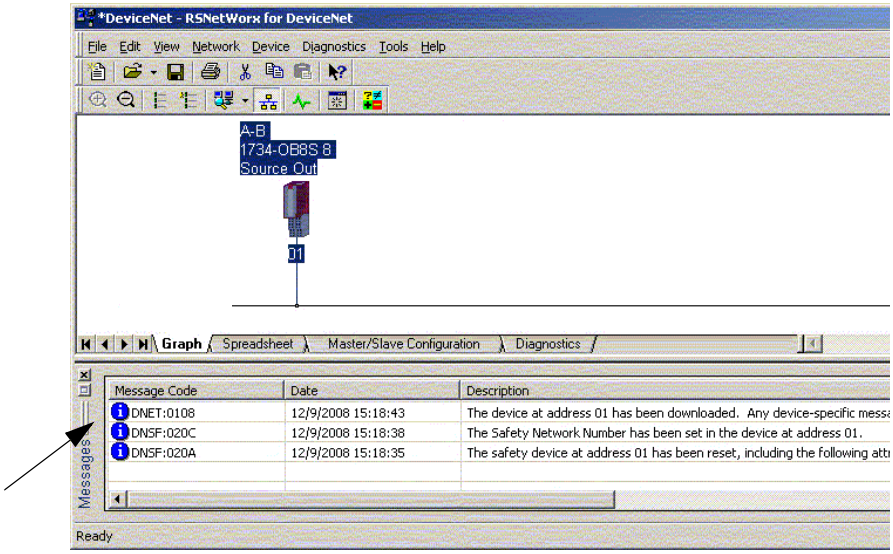

4. Click Yes to confirm.
5. Click Download on the Safety Network Number Mismatch dialog box to set the SNN on the replacement module.

6. Verify that the (NS) network status indicator is flashing on the correct module and click OK to set the SNN on that device.




RSNetWorx for DeviceNet software confirms that the SNN has ben set.

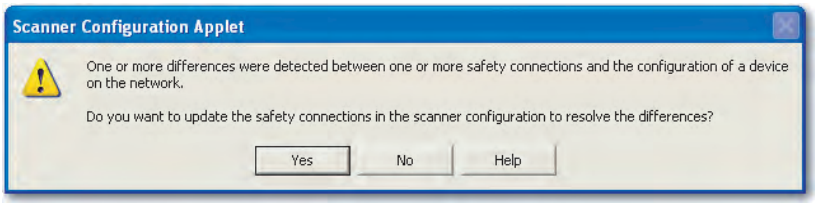

Once the download is completes successfully, the main project view displays this message: 'The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.'




Assuming this is the proper configuration from the original DNT file, the SNN and configuration signature now match that of the original. If you are already connected to the controller, a connection is made. The controller does not need to be taken out of Run mode to download to the replacement module.

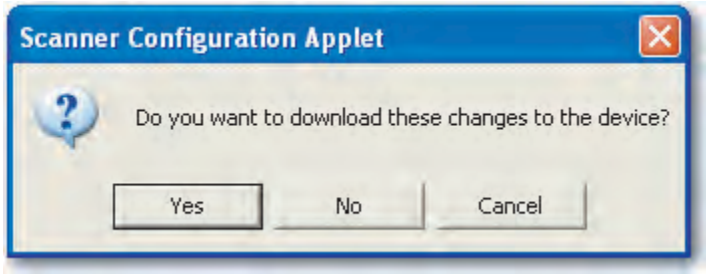
If you download this configuration to a temporary setup, place the module on the network and it automatically connects to the controller.

If the configuration downloaded to the module is not from the original DNT file, the configuration signature does not match the original. Even if you recreate the same parameters in a new DNT file, the time and date portions of the signature are different so the connection to the controller is not made. If this occurs, click the Safety Connection tab for the controller that prompted you that the configuration signature is different and provides you with the option to match the new configuration signature. However, first re-validate the safety system, because it is not using the original DNT file.




7. Click Yes.

   This takes the controller out of Run mode and prompts you to download the changes.




8. Click Yes to download the new connection configuration to the controller.

   After the download is complete, place the controller back in Run mode and the connection to the replacement module is established.

9. 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



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 5570 Controller Systems Safety Reference Manual, publication 1756-RM099.

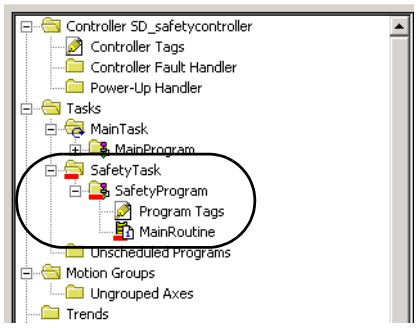
The Safety Reference Manual addresses the following topics:

- 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, the Logix Designer application automatically creates a safety task with a safety program and a main (safety) routine.

**Figure 24 - Safety Task in the Controller Organizer**



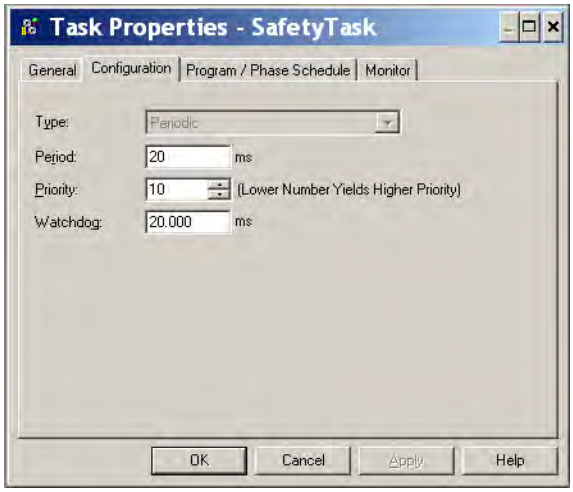

Within the safety task, you can use multiple safety programs, composed of multiple safety routines. The GuardLogix controller supports one safety task. The safety task cannot be deleted.

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 set the task priority and watchdog time via the Task Properties - Safety Task dialog box. To open the dialog box, right-click the Safety Task and choose Properties.

**Figure 25 - Configure the Safety Task Period**



The safety task is a high priority. You specify the safety task period (in ms) and the safety task watchdog (in ms). The safety task period is the period that the safety task executes. The safety task watchdog is the maximum time 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 5570 Controller Systems Safety Reference Manual, publication 1756-RM099, 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 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 100 for information on safety tag mapping.
- Safety output tag (output and produced) values are updated at the conclusion of safety task execution.

## Safety Programs

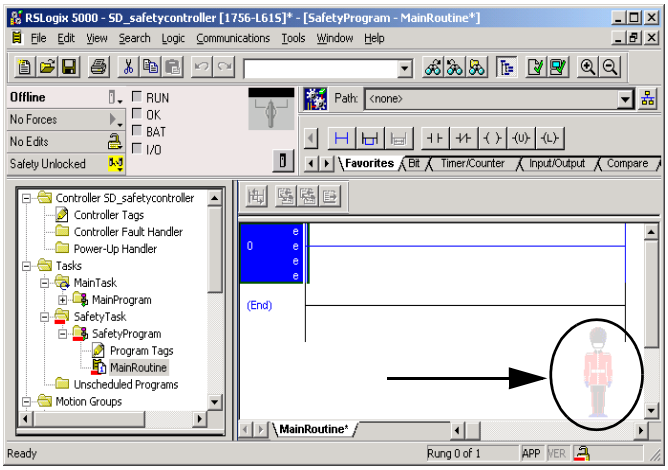
Safety programs have all the attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines. One safety routine must be designated as the main routine, and another safety routine can be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

Safety programs cannot contain standard routines or standard tags.

## Safety Routines

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

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




## Safety Tags

A tag is an area of a controller's memory where data is stored. Tags are the basic mechanism 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.

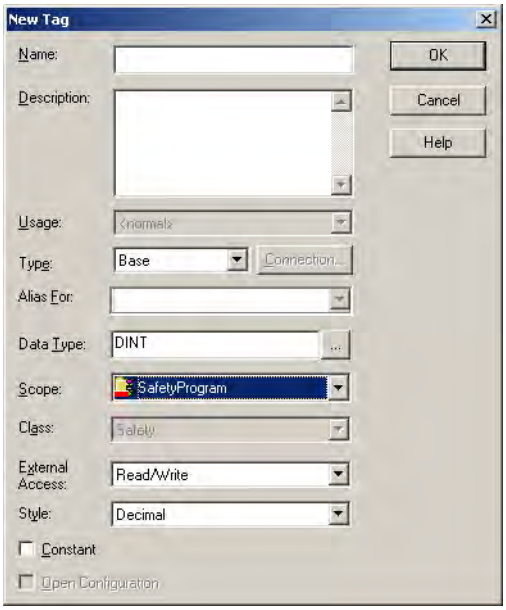
When you create a tag, you assign the following properties:

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

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

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

**Figure 26 - Creating a New Tag**




## Tag Type

Table 25 defines the four types of tags.

**Table 25 - Four Tag Types**

| Tag Type | Description |
|---|---|
| Base tag | These tags store values for use by logic within the project. |
| Alias tag | A tag that references another tag. An alias tag can refer to another alias tag or a base tag. An alias tag can also refer to a component of another tag by referencing a member of a structure, an array element, or a bit within a tag or member.<br>**IMPORTANT:** Do not use alias tags between standard and safety tags in safety applications. Instead, standard tags can be mapped to safety tags using safety tag mapping. See Safety Tag Mapping on page 100. |
| Produced tag | A tag that a controller makes available for use by other controllers. A maximum of 15 controllers can simultaneously consume (receive) the data. A produced tag sends its data to one or more consuming tags without using logic. Produced tag data is sent at the RPI of the consuming tag. |
| Consumed tag | A tag that receives the data of a produced tag. The data type of the consumed tag must match the data type of the produced tag. The requested packet interval (RPI) of the consumed tag determines the period when the data updates. |

## Data Type

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

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

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

These data types are permitted for safety tags.

**Table 26 - Valid Data Types for Safety Tags**

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

## Scope

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

### *Controller-scoped Tags*

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

- More than one program in the project
- To produce or consume data
- To communicate with a PanelView™ terminal
- In safety tag mapping

  See Safety Tag Mapping on page 100 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 27 - Additional Resources**

| Resource | Description |
|---|---|
| Safety Connections on page 125 | Provides more information on the CONNECTION_STATUS member |
| Logix5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004 | 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.

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

### External Access

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

**Table 28 - External Access Levels**

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

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

## Produced/Consumed Safety Tags

To transfer safety data between 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.

**Table 29 - Produced and Consumed Connections**

| Tag | Connection Description |
|---|---|
| Produced | A GuardLogix controller can produce (send) safety tags to other 1756 or 1768 GuardLogix controllers.<br>The producing controller uses a single connection for each consumer. |
| Consumed | GuardLogix controllers can consume (receive) safety tags from other 1756 or 1768 GuardLogix controllers.<br>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). The SNN of the peer safety controller depends on its placement in the system.

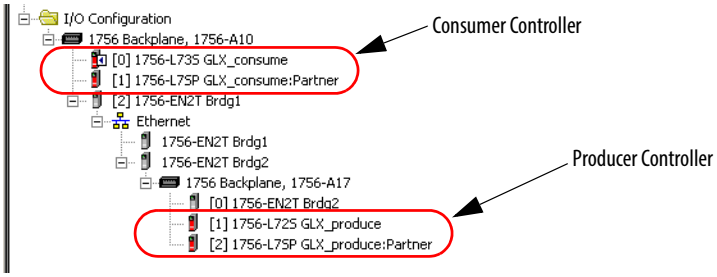
**Table 30 - SNN and Controller Placement**

| Peer Safety Controller Location | SNN |
|---|---|
| Placed in the local chassis | GuardLogix controllers in a common chassis have the same SNN. |
| Placed in another chassis | The controller must have a unique SNN. |

Follow these steps to copy and paste the SNN.

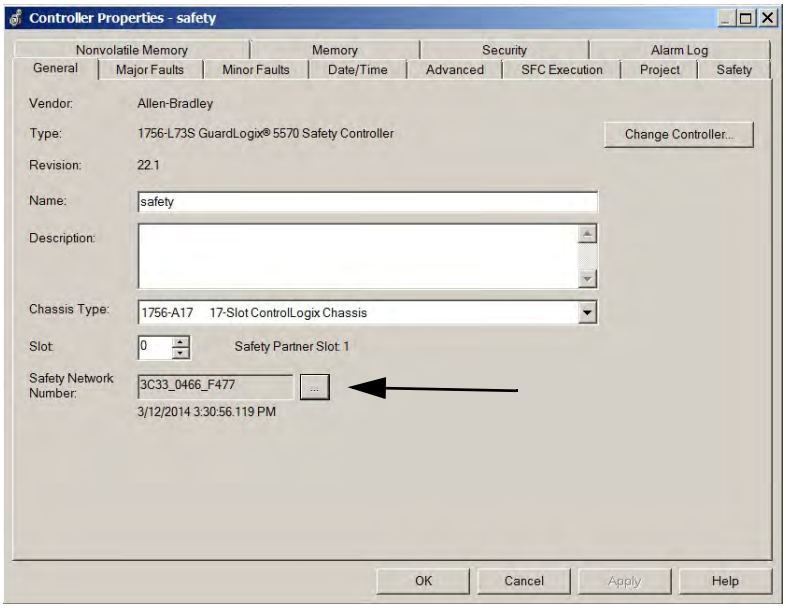
1. Add the producer controller to the consumer controller's I/O tree.

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

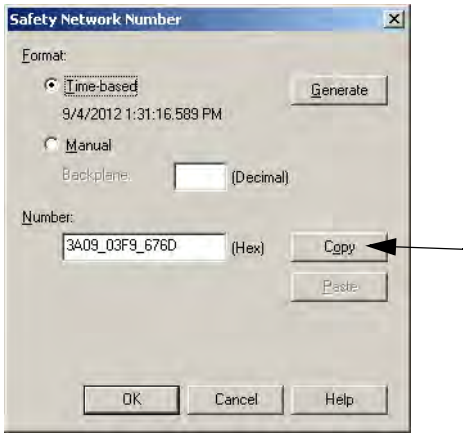



2. In the producer controller's project, right-click the producer controller and choose Controller Properties.

3. Click ... to open the Safety Network Number dialog box.




4. Copy the producer controller's SNN.



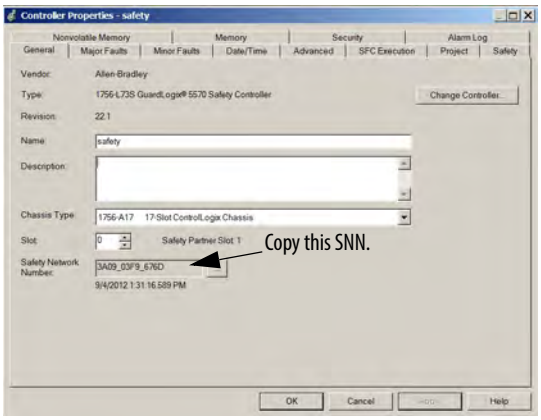

5. In the consumer controller's project, right-click the producer controller and choose Module Properties.

6. Click ... to open the Safety Network Number dialog box.

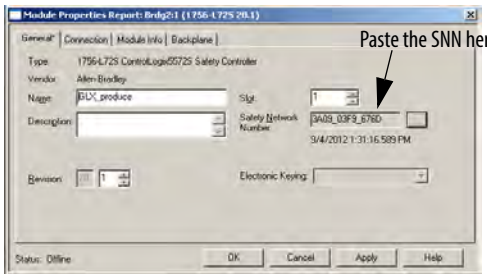
7. Paste the producer controller's SNN into the SNN field and click OK.

   The safety network numbers match.

**Producer Controller Properties Dialog Box in Producer Project**




**Module Properties Dialog Box in Consumer Project**



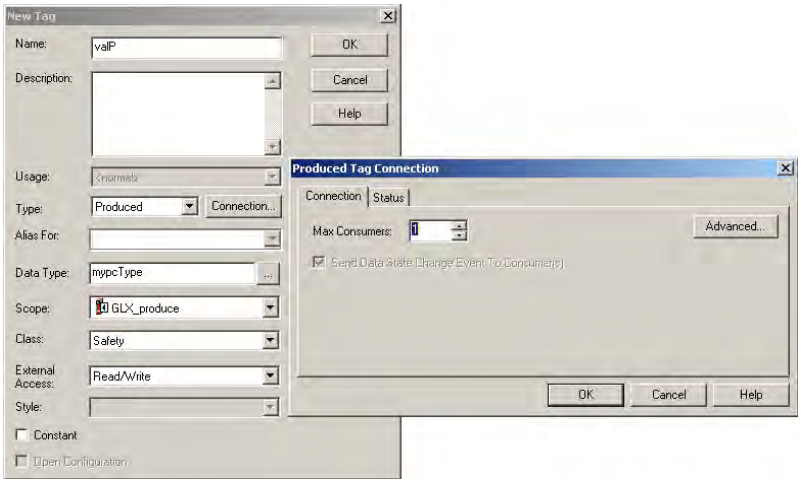

## Produce a Safety Tag

Follow this procedure to produce a safety tag.

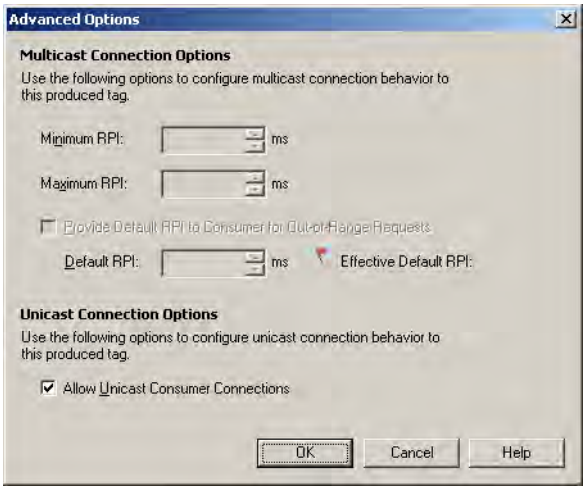
1. In the producing controllers project, create a user-defined data type defining the structure of the data to be produced.

   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.

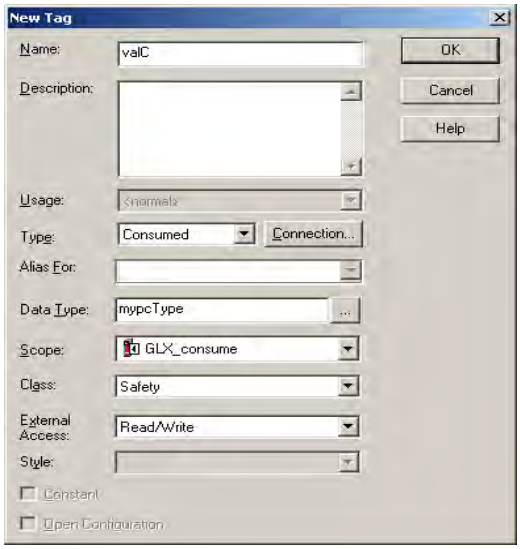
## Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

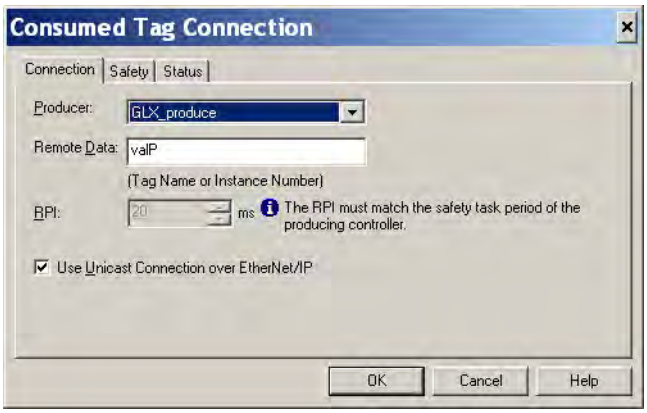
1. In the consumer controller's project, create a user-defined data type identical to the one created in the producer project.

   **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.

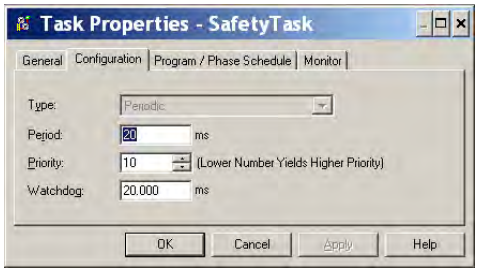



5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.
7. Click the Safety tab.
8. In the Requested Packet Interval (RPI) field, enter the RPI for the connection in 1 ms increments.

   The default is 20 ms.

**Consumer's Project**


**Producer's Project**

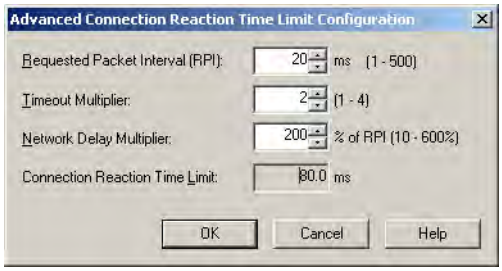



The RPI specifies the period when data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.

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, click Reset Max to reset the Max Network Delay.

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 31 - More Resources**

| Resource | Description |
|---|---|
| Pages 69…71 | 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 |
| Chapter 9 | Contains information on the CONNECTION_STATUS predefined data type |
| Logix5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011 | 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 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:

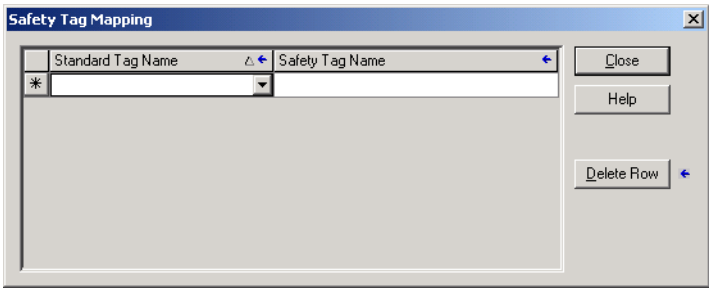
- The safety tag and standard tag pair must be controller-scoped.
- The data types of the safety and standard tag pair must match.
- Alias tags are not allowed.
- Mapping must take place at the whole tag level. For example, myTimer.pre is not allowed if myTimer is a TIMER tag.
- A mapping pair is one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

**ATTENTION:** When using standard data in a safety routine, you must verify that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 3/PLe safety output with standard tag data.

Refer to the GuardLogix 5570 Controller Systems Safety Reference Manual, publication 1756-RM099, for more information.

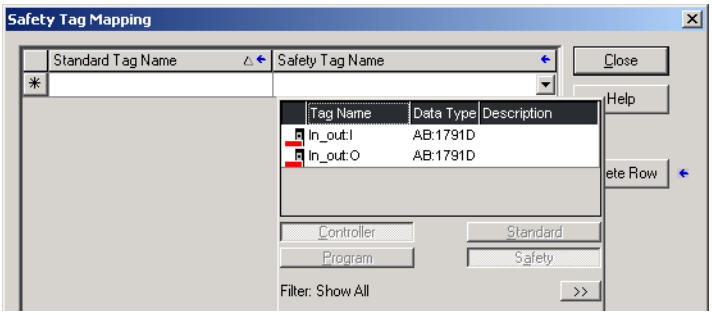
## Create Tag Mapping Pairs

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



2. 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 only controller-scoped safety tags.




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

## Monitor Tag Mapping Status

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

**Table 32 - Tag Mapping Status Icons**

| Cell Contents | Description |
|---|---|
| Empty | Tag mapping is valid. |
|  | When offline, the X icon indicates that tag mapping is invalid. You can move to another row or close the Safety Tag Mapping dialog box.(1)<br>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 101.

# 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 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 can be present.

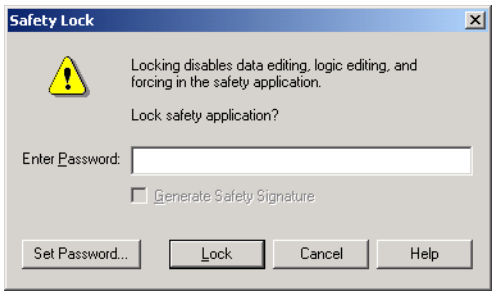
Safety-locked or -unlocked status cannot be changed when the key switch is in the RUN position.

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

For more information on accessing the controller log, refer to Logix5000 Controllers Controller Information and Status Programming Manual, publication 1756-PM015.

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

**Figure 27 - 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 45.

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

Refer to the Logix5000 Controllers Security Programming Manual, publication 1756-PM016, for information on Logix Designer security features.

## Generate a Safety Task Signature

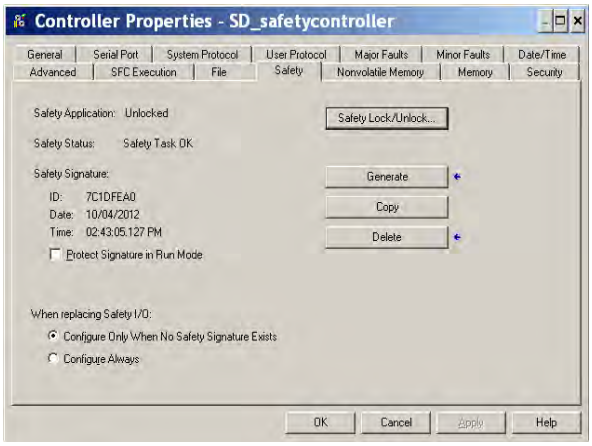
Before verification testing, you must generate the safety task signature. You can generate the safety task signature only when online with the safety-unlocked GuardLogix controller in Program mode, and with no safety forces, pending online safety edits, or safety faults. The safety status must be Safety 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 124) or on the Safety tab of the Controller Properties dialog box, as shown on page 105.

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

**Figure 28 - Safety Tab**




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

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

For more information on accessing the controller log, refer to Logix5000 Controllers Controller Information and Status Programming Manual, publication 1756-PM015.

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

- 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 key switch 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 5570 Controller Systems Safety Reference Manual, publication 1756-RM099, for more information on SIL 3/PLe requirements.

## Programming Restrictions

Restrictions limiting the availability of some menu items and features (that is, cut, paste, delete, search and replace) are imposed by the Logix Designer application 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.
- Safety status is as follows:
  - Partner missing
  - Partner unavailable
  - Hardware incompatible
  - Firmware incompatible

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

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

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

- Apply forces to safety tags.
- Create new safety tag mappings.
- Modify or delete tag mappings.
- Modify or delete user-defined data types that are used by safety tags.
- Modify the controller name, description, chassis type, slot, and safety network number.
- Modify or delete the safety task signature, when safety-locked.

# Go Online with the Controller



## Connect the Controller to the Network

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

**Table 33 - Communication Connections**

| For this type of connection | Use | See |
|---|---|---|
| USB | USB 2.0 cable | Make Communication Connections on page 31 |
| EtherNet/IP | EtherNet/IP device in an open slot in the same chassis as the controller | Connect Your EtherNet/IP Device and Computer on page 108 |
| DeviceNet | 1756-DNB module in an open slot in the same chassis as the controller | Connect Your ControlNet Communication Module or DeviceNet Scanner and Your Computer on page 108 |
| ControlNet | 1756-CN2 module in an open slot in the same chassis as the controller | |

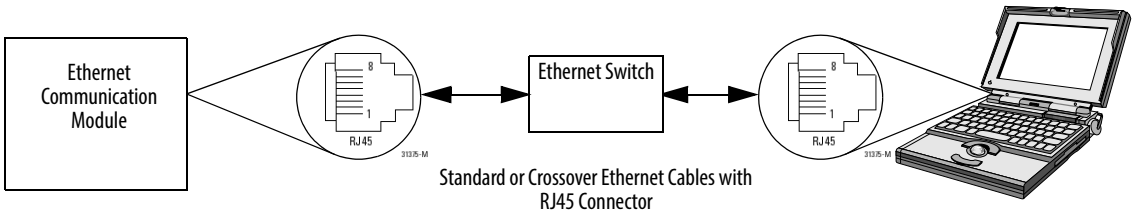
## Connect Your EtherNet/IP Device and Computer

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

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

**Figure 29 - Ethernet Connections**




## Connect Your ControlNet Communication Module or DeviceNet Scanner and Your Computer

To access the ControlNet or DeviceNet 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.

## Configure an EtherNet/IP, ControlNet, or DeviceNet 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
- DeviceNet Modules in Logix5000 Control Systems, publication DNET-UM004

## Understanding the Factors that Affect Going Online

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

A number of factors affect these processes, including Project to Controller Match feature, the safety status and faults, the existence of a safety 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, the Logix Designer application compares the serial number of the controller in the offline project to that of the connected controller. If they do not match, you must cancel the download/upload, connect to the correct controller, or confirm that you are connected to the correct controller that updates the serial number in the project to match the target controller.

### Firmware Revision Matching

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

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

| | |
|---|---|
| **TIP** | You can also upgrade the firmware by choosing ControlFLASH from the Tools menu in the Logix Designer application. |

### Safety Status/Faults

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

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

## Safety 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 34 - 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.<br>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. |

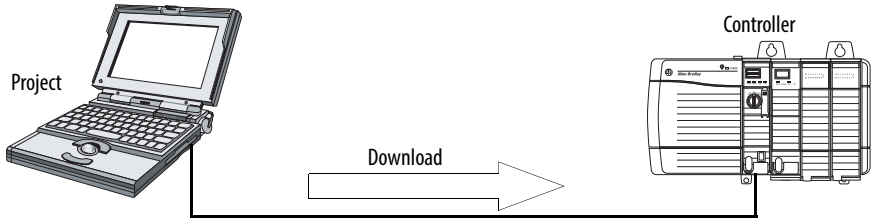
**IMPORTANT** During a download to a controller that is safety-unlocked, if firmware in the controller is different than in the offline project, do one of the following:

- 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 key switch of the controller to REM.
2. Open the controller project that you want to download.
3. Define the path to the controller.
   a. Click Who Active  .
   b. Select the controller.
      To open a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
4. Click Download.

   The Logix Designer application compares the following information in the offline project and the controller:
   - Controller serial number (if project to controller match is selected)
   - Firmware major and minor revisions
   - Safety status
   - Safety task signature (if one exists)
   - Safety-lock status

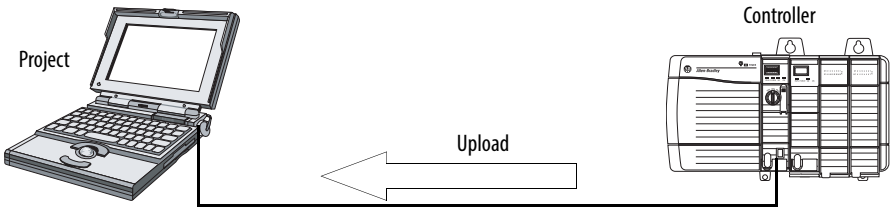
5. Follow the directions in this table to complete the download based on the Logix Designer application's response.

| If the software indicates | Then |
|---|---|
| Download to the controller. | Choose Download. The project downloads to the controller and 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, check the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number. |
| Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible. | Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection. |
| Unable to download to controller. The safety partner is missing or unavailable. | Cancel the download process. Install a compatible safety partner before attempting to download. |
| Unable to download to controller. The firmware revision of the safety partner is not compatible with the primary controller. | Update the firmware revision of the safety partner. Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection. |
| Unable to download to controller. Safety partnership has not been established. | Cancel this download process and attempt a new download. |
| Unable to download to controller. Incompatible safety 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.<br>**IMPORTANT:** The safety system requires revalidation. |
| Cannot download in a manner that preserves the safety task signature. Controller's firmware minor revision is not compatible with safety task signature in offline project. | • If the firmware minor revision is incompatible, to preserve the safety task signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project.<br>• To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted.<br>**IMPORTANT:** The safety system requires revalidation. |
| Unable to download to controller. Controller is locked. Controller and offline project safety task signatures do not match. | Choose Unlock. The Safety Unlock for Download dialog box appears. If the Delete Signature checkbox is selected and you choose Unlock, click Yes to confirm the deletion. |
| 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, the Logix Designer application 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.

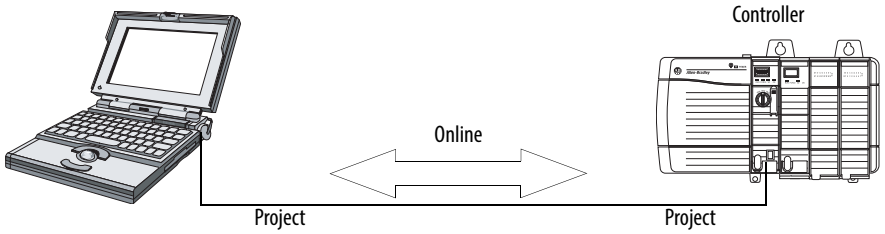
5. The Logix Designer application checks whether the open project matches the controller project.
   a. If the projects do not match, you must select a matching file or cancel the upload process.
   b. If the projects match, the software checks for changes in the offline (open) project.
6. The Logix Designer application 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 Logix Designer application checks for the following:
   - Do the offline project and controller serial numbers match (if Project to Controller Match is selected)?
   - Does the offline project contain changes that are not in the controller project?
   - Do the revisions of the offline project and controller firmware match?
   - Are either the offline project or the controller safety-locked?
   - Do the offline project and the controller have compatible safety task signatures?

3. Follow the directions in the table below to connect to the controller.

**Table 35 - 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:<br>• Choose Update Firmware. Choose the required revision and click Update. Click Yes to confirm your selection.<br>**IMPORTANT:** The online project is deleted.<br>• To preserve the online project, cancel the online process and install a version of the Studio 5000 environment that is compatible with the firmware revision of your controller. |
| You need to upload or download to go online by using the open project. | Choose one of the following options:<br>• Upload to update the offline project.<br>• Download to update the controller project.<br>• Choose File to select another offline project. |
| Unable to connect in a manner that preserves safety task signature. Controller's firmware minor revision is not compatible with safety task signature in offline project. | • To preserve the safety task signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller.<br>• To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted.<br>**IMPORTANT:** The safety system requires revalidation. |
| Unable to connect to controller. Incompatible safety task signature cannot be deleted while project is safety-locked. | Cancel the online process. You must safety-unlock the offline project before attempting to go online. |

When the controller and the Logix Designer application 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.

## Notes:

# Store and Load Projects Using Nonvolatile Memory



## Use Memory Cards for Nonvolatile Memory

GuardLogix 5570 controllers support a memory 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.

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 the Logix Designer application

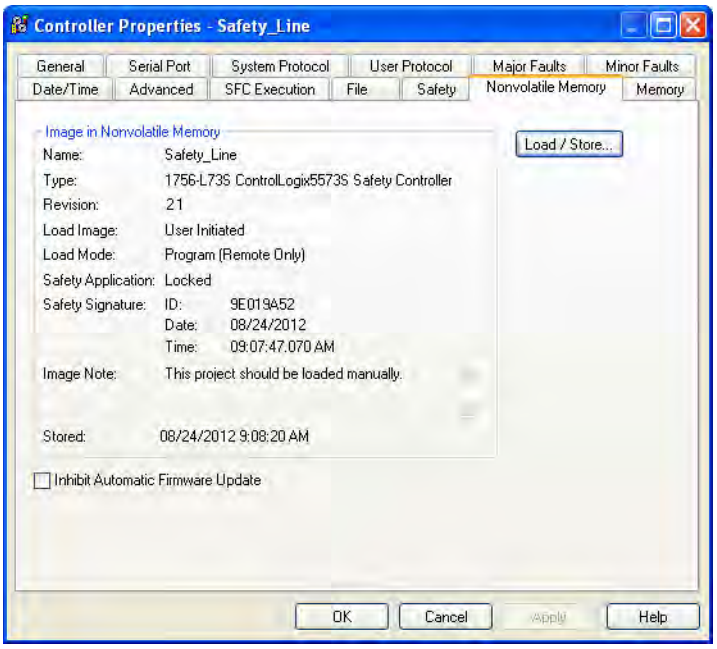
**IMPORTANT** Nonvolatile memory stores the contents of the user memory at the time that you store the project:

- 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 OK 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 OK status indicator turns solid green.

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 30 - Nonvolatile Memory Tab**




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

## Store a Safety Project

You cannot store a safety project if the safety task status is Safety Task Inoperable. When you store a safety project, the firmware of both the primary controller and the safety partner are saved to the memory card.

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

If a safety 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 that the controller enters following the load.

## Load a Safety Project

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

- The controller type specified by the project stored in nonvolatile memory matches the controller type.
- The major and minor revision of the project in nonvolatile memory matches the major and minor revision 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 36 - 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 | • During a power cycle, you lose any online changes, tag values, and network schedule that you have not stored in the nonvolatile memory.<br>• The controller loads the stored project and firmware at every powerup regardless of the firmware or application project on the controller. The load occurs whether or not the controller is safety-locked or has a safety task signature.<br>• You can always use the Logix Designer application to load the project. |
| Whenever there is no project in the controller and you turn on or cycle chassis power | On Corrupt Memory | • For example, if the battery becomes discharged and the controller loses power, the project is cleared from memory. When power is restored, this load option loads the project back into the controller.<br>• The controller updates the firmware on the primary controller or the safety partner, if required. The application project stored in nonvolatile memory is also loaded and the controller enters the selected mode, either Program or Run.<br>• You can always use the Logix Designer application to load the project. |
| Only through the Logix Designer application | User Initiated | • 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.<br>• You can load a project to a safety-locked controller only when the safety task signature of the project stored in nonvolatile memory matches the project on the controller.<br>• 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.<br>**IMPORTANT:** When you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety task signature are set to the values contained in nonvolatile memory once the load is complete.<br>• If the firmware on the primary controller matches the revision in nonvolatile memory, the safety partner firmware is updated, if required, the application stored in nonvolatile memory is loaded so that the Safety Task status becomes Safety Task Operable and the controller enters the selected mode, either Program or Run. |

**IMPORTANT** Before using ControlFLASH software, make sure the SD card is unlocked if set to load On Power Up. Otherwise the updated data can be overwritten by firmware on the memory card.

## Use Energy Storage Modules

You can use the GuardLogix ESMs to execute either of the following tasks:

- Provide power to the controller to save the program to the controller's on-board non-volatile storage (NVS) memory after power is removed from the chassis or the controller is removed from a powered chassis.

**IMPORTANT** When you are using an ESM to save the program to on-board NVS memory, you are **not** saving the program to the SD card installed in the controller.

- Clear the program from the controller's on-board NVS memory. For more information, see Clear the Program from On-board NVS Memory

The following table describes the ESMs.

**Table 37 - Energy Storage Modules**

| Cat. No. | Description |
|---|---|
| 1756-ESMCAP(XT) | Capacitor-based ESM<br>The controllers come with this ESM installed. |
| 1756-ESMNSE(XT) | Capacitor-based ESM without WallClockTime backup power<br>Use this ESM if your application requires that the installed ESM depletes its residual stored energy to 40 µJ or less before transporting it into or out of your application. Also, you can only use this ESM with a 1756-L73S (8MB) or smaller memory-sized controller. |
| 1756-ESMNRM(XT) | Secure capacitor-based ESM (non-removable)<br>This ESM provides your application an enhanced degree of security by preventing physical access to the USB connector and the SD card. |
| 1756-SPESMNSE(XT) | Capacitor-based ESM without WallClockTime backup power for the safety partner<br>Use this ESM if your application requires that the installed ESM deplete its residual stored energy to 40 µJ or less before transporting it into or out of your application.<br>The 1756-L7SPXT extreme temperature safety partner ships with the 1756-SPESMNSEXT installed. |
| 1756-SPESMNRM(XT) | Secure capacitor-based ESM (non-removable) for the safety partner |

## Save the Program to On-board NVS Memory

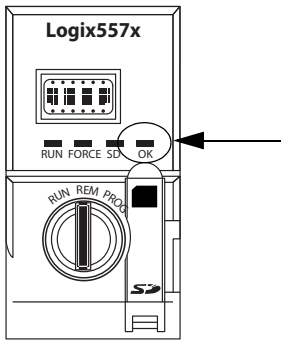
Follow these steps to save the program to NVS memory when the controller loses power.

1. Remove power from the controller.

   You can remove power in either of two ways:
   - Turn power off to the chassis while the controller is installed in the chassis.
   - Remove the controller from a powered chassis.

   Immediately after the controller is no longer powered, the OK status indicator transitions to solid red and remains that way long enough to save the program.

**Figure 31 - OK Status Indicator.**



2. Leave the ESM on the controller until the OK status indicator is off.
3. If necessary, remove the ESM from the controller after the OK status indicator transitions from solid red to off.

### Clear the Program from On-board NVS Memory

If your application lets you clear programs, follow these steps to clear the program from the controller's on-board NVS memory.

1. Remove the ESM from the controller.
2. Remove power from the controller by turning off power to the chassis while the controller is installed in the chassis, or by removing the controller from a powered chassis.
3. Reinstall the ESM into the controller.
4. Restore power to the controller.
   a. If the controller is already installed in the chassis, turn power to the chassis back on.
   b. If the controller is not installed into the chassis, reinstall the controller into the chassis and turn chassis power back on.

## Estimate the ESM Support of the WallClockTime

The ESM provides support for the maintenance of the WallClockTime attribute of the controller when power is not applied. Use this table to estimate the hold-up time of the ESM, based on the temperature of the controller and installed ESM.

**Table 38 - Temperature vs. Hold-up Time**

| Temperature | Hold-up Time (in days) | | |
|---|---|---|---|
| | 1756-ESMCAP(XT) | 1756-ESMNRM(XT)<br>1756-SPESMNRM(XT) | 1756-ESMNSE(XT)<br>1756-SPESMNSE(XT) |
| 20 °C (68 °F) | 12 | 12 | 0 |
| 40 °C (104 °F) | 10 | 10 | 0 |
| 60 °C (140 °F) | 7 | 7 | 0 |

## Manage Firmware with Firmware Supervisor

You can use the Firmware Supervisor feature to manage firmware on 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 ControlFLASH software.

Firmware Supervisor supports non-modular distributed I/O products that sit directly on the network without an adapter, including safety I/O devices on EtherNet/IP networks. Safety I/O devices 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.

The Logix Designer application 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 the firmware supervisor updates. This does not include the controller firmware updates that occur when the controller image is reloaded from the memory card.

# Monitor Status and Handle Faults

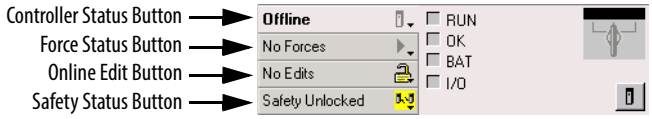


See Appendix A, Status Indicators for information on interpreting the controller's status indicators and display messages.

## View Status via the Online Bar

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

**Figure 32 - 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 BAT indicator combines the status of the primary controller and the safety partner. If either or both have a battery fault, the status indicator illuminates. 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 33 - 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 39 - Safety Status Icon**

| If the safety status is | This icon is displayed |
|---|---|
| Safety Task OK |  |
| Safety Task Inoperable |  |
| Partner Missing<br>Partner Unavailable<br>Hardware Incompatible<br>Firmware Incompatible |  |
| 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. 

## Monitor the 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 device fault is produced that you can access through the Connections tab of the Module Properties dialog box for the device 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/PLe integrity.

See Safety Connections on page 125.

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

## Monitor the Status Flags

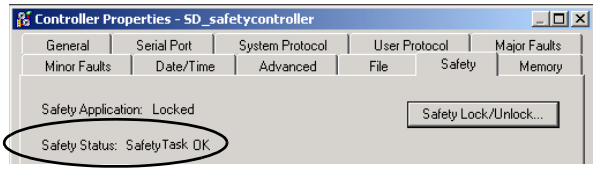
Logix controllers, including GuardLogix controllers, support status keywords that you can use in your logic to monitor certain events.

For more information on how to use these keywords, refer to the Logix5000 Controllers Controller Information and Status Programming Manual, publication 1756-PM015.

## Monitor the 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 34 - Safety Task Status**




These are the possible values for safety status:

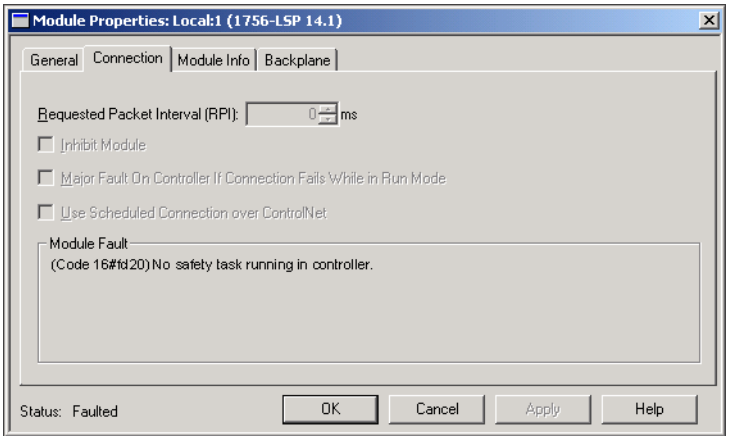
- Safety partner is missing or unavailable.
- Safety partner hardware is incompatible with primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety task OK.

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

See Major Safety Faults (Type 14) on page 128 for fault codes and corrective actions.

The status of the safety partner can be viewed on the Connections tab of its Module Properties dialog box.

**Figure 35 - Safety Partner Status**




## Controller Faults

Faults in the 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 safety I/O devices 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 and control partnership 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 a safety fault does not clear the fault. If you override a safety fault it is your responsibility to prove that operation of your system is still safe.

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

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

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

When a recoverable fault in the safety application is not cleared programmatically, a Type 14, Code 2 recoverable safety fault occurs. The safety program execution is stopped, and safety protocol connections are closed and reopened to 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.

## View Faults

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

The status display on the controller also shows fault codes with a brief status message, as described beginning on page 131.

## Fault Codes

Table 41 shows the fault codes specific to GuardLogix controllers. The type and code correspond to the type and code displayed on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

**Table 41 - Major Safety Faults (Type 14)**

| Code | Cause | Status | Corrective Action |
|---|---|---|---|
| 01 | Task watchdog expired. User task has not completed in a specified period of time. A program error caused an infinite loop, the program is too complex to execute as quickly as specified, a higher priority task is keeping this task from finishing, or the safety partner has been removed. | Nonrecoverable | Clear the fault.<br>If a safety task signature exists, safety memory is re-initialized and the safety task begins executing.<br>If a safety task signature does not exist, you must re-download the program so the safety task can run.<br>Reinsert the safety partner, if it was removed. |
| 02 | An error exists in a routine of the safety task. | Recoverable | Correct the error in the user-program logic. |
| 03 | Safety partner is missing. | Nonrecoverable | Install a compatible safety partner. |
| 04 | Safety partner is unavailable. | Nonrecoverable | Install a compatible safety partner. |
| 05 | Safety partner hardware is incompatible. | Nonrecoverable | Install a compatible safety partner. |
| 06 | Safety partner firmware is incompatible. | Nonrecoverable | Update the safety partner so that the firmware major and minor revision matches the primary controller. |
| 07 | Safety task is inoperable.<br>This fault occurs when the safety logic is invalid, for example a mismatch in logic exists between the primary controller and safety partner, a watchdog timeout occurred, or memory is corrupt. | Nonrecoverable | Clear the fault.<br>If a safety task signature exists, safety memory is re-initialized via the safety task signature and the safety task begins executing.<br>If a safety task signature does not exist, you must download the program again so the safety task can run. |
| 08 | Coordinated system time (CST) not found. | Nonrecoverable | Clear the fault. Configure a device to be the CST master. |
| 09 | Safety partner nonrecoverable controller fault. | Nonrecoverable | Clear the fault and download the program. If the problem persists, replace the safety partner. |

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.

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

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

The 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 130.

### 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 cannot clear the fault or does not exist.

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

The 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 the attributes that you can set.

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

For safety objects, the Table 42 shows the attributes that you can get values for by using the GSV instruction, and the attributes that you can 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 42 - GSV/SSV Accessibility**

| Safety Object | Attribute Name | Data Type | Attribute Description | Accessible from the Safety Task | | Accessible from Standard Tasks | |
|---|---|---|---|---|---|---|---|
| | | | | GSV | SSV | GSV[4] | SSV |
| Safety Task | Instance | DINT | Provides instance number of this task object. Valid values are 0…31. | X | | X | |
| | MaximumInterval | DINT[2] | The max time interval between successive executions of this task. | | | X | X |
| | MaximumScanTime | DINT | Max recorded execution time (ms) for this task. | | | X | X |
| | MinimumInterval | DINT[2] | The min time interval between successive executions of this task. | | | X | X |
| | Priority | INT | Relative priority of this task as compared to other tasks. Valid values are 0…15. | X | | X | |
| | Rate | DINT | Period for the task (in ms), or timeout value for the task (in ms). | X | | X | |
| | Watchdog | DINT | Time limit (in ms) for execution of all programs associated with this task. | X | | X | |
| Safety Program | Instance | DINT | Provides the instance number of the program object. | X | | X | |
| | MajorFaultRecord[1] | DINT[11] | Records major faults for this program. | X | X | X | |
| | MaximumScanTime | DINT | Max recorded execution time (ms) for this program. | | | X | X |
| Safety Routine | Instance | DINT | Provides the instance number for this routine object. Valid values are 0…65,535. | X | | | |

**Table 42 - GSV/SSV Accessibility (Continued)**

| Safety Object | Attribute Name | Data Type | Attribute Description | Accessible from the Safety Task | | Accessible from Standard Tasks | |
|---|---|---|---|---|---|---|---|
| | | | | GSV | SSV | GSV[4] | SSV |
| Safety Controller | SafetyLocked | SINT | Indicates whether the controller is safety-locked or -unlocked. | X | | X | |
| | SafetyStatus[2] | INT | Specifies the safety status as the following:<br>• Safety task OK. (1000000000000000)<br>• Safety task inoperable. (1000000000000001)<br>• Partner missing. (0000000000000000)<br>• Partner unavailable. (0000000000000001)<br>• Hardware incompatible. (0000000000000010)<br>• Firmware incompatible. (0000000000000011) | | | X | |
| | SafetySignatureExists | SINT | Indicates whether the safety task signature is present. | X | | X | |
| | SafetySignatureID | DINT | 32-bit identification number. | | | X | |
| | SafetySignature | String[3] | 32-bit identification number. | | | X | |
| | SafetyTaskFaultRecord[1][2] | DINT[11] | Records safety task faults. | | | X | |
| AOI (Safety) | LastEditDate | LINT | Date and time stamp of the last edit to an Add-On Instruction definition. | | | X | |
| | SignatureID | DINT | ID number. | | | X | |
| | SafetySignatureID | DINT | 32-bit identification number. | | | X | |

(1) See Access FaultRecord Attributes on page 131 for information on how to access this attribute.
(2) See Capture Fault Information on page 132 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 43 - 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.

# Status Indicators



## Controllers Status Indicators

The status of the primary controller is displayed via four status indicators.

**Table 44 - Primary Controller Status Indicator Descriptions**

| Indicator | Status | Description |
|---|---|---|
| RUN | Off | No user tasks running. Controller is in PROGram mode. |
| | Green | Controller is in RUN mode. |
| FORCE | Off | No forces, standard or safety, are enabled on the controller. |
| | Amber | Standard and/or safety forces have been enabled.<br>**Use caution if you install (add) a force. If you install a force, it takes immediate effect.** |
| | Amber, Flashing | One or more I/O addresses, standard and/or safety, have been forced to an on or off state, but forces are not enabled.<br>**Use caution if you enable I/O forces. If you enable I/O forces, all existing I/O forces also take effect.** |
| SD | Off | No activity is occurring with the memory card. |
| | Green, Flashing | The controller is reading from or writing to the memory card. Do not remove the memory card while the controller is reading or writing. |
| | Green | |
| | Red, Flashing | The memory card does not have a valid file system. |
| | Red | The memory card is not recognized by the controller. |
| OK | Off | No power is applied. |
| | Green | The controller is operating with no faults. |
| | Red, Flashing | • Nonrecoverable fault or recoverable fault not handled in the fault handler. All user tasks, both standard and safety, are stopped.<br>• If the controller is new, out-of-the-box, it requires a firmware upgrade. The status display indicates Firmware Installation Required. |
| | Red | • The controller is completing power-up diagnostics<br>• A nonrecoverable major fault occurred and the program was cleared from memory.<br>• The charge of the capacitor in the Energy Storage Module (ESM) is being discharged upon powerdown.<br>• The controller is powered but inoperable.<br>• The controller is loading a project to nonvolatile memory. |

The safety partner has an OK status indicator.

**Table 45 - 1756-L7SP Status Indicator**

| Indicator | Status | Description |
|---|---|---|
| OK | Off | No power is applied. |
| | Green | The safety partner is operating with no faults. |
| | Red | Powering up or nonrecoverable controller fault. |

## Controller Status Display

The controller status display scrolls messages that provide information about the controller's firmware revision, energy storage module (ESM) status, project status, and major faults.

### Safety Status Messages

The primary controller display can show the following messages. The safety partner displays 'L7SP'.

**Table 46 - Safety Status Display**

| Message | Interpretation |
|---|---|
| No Safety Signature | Safety Task is in Run mode without a safety task signature. |
| Safety Partner Missing | The safety partner is missing or unavailable. |
| Hardware Incompatible | The safety partner and primary controller hardware is incompatible. |
| Firmware Incompatible | The safety partner and primary controller firmware revision levels are incompatible. |
| No CST Master | A coordinated system time (CST) master has not been found |
| Safety Task Inoperable | The safety logic is invalid. For example, a mismatch occurred between the primary controller and the safety partner, a watchdog timeout occurred, or memory is corrupt. |
| Safety Unlocked | The controller is in Run mode with a safety signature, but is not safety-locked. |

## General Status Messages

The messages described in Table 47 are typically indicated upon powerup, powerdown, and while the controller is running. These messages indicate the status of the controller and the ESM.

**Table 47 - General Status Display**

| Message | Interpretation |
|---|---|
| No message is indicated | The controller is off, or a major nonrecoverable fault (MNRF) has occurred.<br>Check the OK indicator to determine if the controller is powered and determine the state of the controller. |
| TEST | Power-up tests are being conducted by the controller. |
| PASS | Power-up tests have been successfully completed. |
| SAVE | A project is being saved to the SD card at powerdown. You can also view the SD Indicator (see page 133) for additional status information.<br>Let the save complete before removing the SD card or disconnecting power. |
| LOAD | A project is being loaded from the SD card at controller powerup. You can also view the SD Indicator (see page 133) for additional status information.<br>Let the load complete before removing the SD card, removing the ESM module, or disconnecting power. |
| UPDT | A firmware upgrade is being conducted from the SD card upon powerup. You can also view the SD Indicator (see page 133) for additional status information.<br>If you do not want the firmware to update upon powerup, change the controller's Load Image property. |
| CHRG | The capacitor-based ESM is being charged. |
| 1756-L7*x*/*X* | The controller catalog number and series. |
| Rev *XX.xxx* | The major and minor revision of the controller's firmware. |
| No Project | No project is loaded on the controller.<br>To load a project, use the Logix Designer application to download the project to the controller, or use an SD card to load a project to the controller. |
| *Project Name* | The name of the project that is currently loaded on the controller. The name indicated is based on the project name specified in the Logix Designer application. |
| BUSY | The I/O devices associated with the controller are not yet fully-powered.<br>Allow time for powerup and I/O device self-testing. |
| Corrupt Certificate Received | The security certificate associated with the firmware is corrupted.<br>Go to http://www.rockwellautomation.com/support/ and download the firmware revision you are trying to upgrade to. Replace the firmware revision you have previously installed with that posted on the Technical Support website. |
| Corrupt Image Received | The firmware file is corrupted.<br>Go to http://www.rockwellautomation.com/support/ and download the firmware revision you are trying to upgrade to. Replace the firmware revision you have previously installed with that posted on the Technical Support website. |
| ESM Not Present | An ESM is not present and the controller cannot save the application at powerdown.<br>Insert a compatible ESM, and, if a capacitor-based ESM is used, do not remove power until the ESM is charged. |
| ESM Incompatible | The ESM is incompatible with the memory size of the controller.<br>Replace the incompatible ESM with a compatible ESM. |
| ESM Hardware Failure | A failure with the ESM has occurred and the controller is incapable of saving of the program in the event of a powerdown.<br>Replace the ESM before removing power to the controller so the controller program is saved. |
| ESM Energy Low | The capacitor-based ESM does not have sufficient energy to enable the controller to save the program in the event of a powerdown.<br>Replace the ESM. |
| ESM Charging | The capacitor-based ESM is charging.<br>Do not remove power until charging is complete. |
| Flash in Progress | A firmware upgrade initiated via ControlFLASH or AutoFlash software is in progress.<br>Allow the firmware upgrade to complete without interruption. |
| Firmware Installation Required | The controller is using boot firmware (that is revision 1.*xxx*) and requires a firmware upgrade.<br>Upgrade controller firmware. |
| SD Card Locked | An SD card that is locked is installed. |

## Fault Messages

If the controller is faulted, these messages can be indicated on the status display.

**Table 48 - Fault Messages(1)**

| Message | Interpretation |
|---|---|
| Major Fault T*XX*:C*XX message* | A major fault of Type *XX* and Code *XX* has been detected.<br>For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, then a JMP instruction is programmed to jump to an invalid LBL instruction. |
| I/O Fault Local:*X #XXXX message* | An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description.<br>For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open.<br>Take corrective action specific to the type of fault indicated. |
| I/O Fault *ModuleName #XXXX message* | An I/O fault has occurred on a module in a remote chassis. The name of the faulted module, as configured in the I/O Configuration tree of the Logix Designer application, is indicated with the fault code and brief description of the fault.<br>For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named 'My_Module' is not open.<br>Take corrective action specific to the type of fault indicated. |
| I/O Fault *ModuleParent:X #XXXX message* | An I/O fault has occurred on a module in a remote chassis. The module's parent name is indicated because no module name is configured in the I/O Configuration tree of the Logix Designer application. In addition, the fault code is indicated with a brief description of the fault.<br>For example, I/O Fault My_CNet:3 #0107 Connection Not Found indicates that a connection to a module in slot 3 of the chassis with the communication module named 'My_CNet' is not open.<br>Take corrective action specific to the type of fault indicated. |
| *X* I/O Faults | I/O faults are present and *X* = the number of I/O faults present.<br>In the event of multiple I/O faults, the controller indicates the first fault reported. As each I/O fault is resolved, the number of faults indicated decreases and the next fault reported is indicated by the I/O Fault message.<br>Take corrective action specific to the type of fault indicated. |

(1) For details about fault codes, see the Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

## Major Recoverable Fault Messages

Major recoverable faults are indicated by Major Fault T*XX*:C*XX message* on the controller status display. Table 49 on page 137 lists specific fault types, codes, and the associated messages as they are shown on the status display.

For detailed descriptions and suggested recovery methods for major recoverable faults, see the Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

**Table 49 - Major Recoverable Fault Status Messages**

| Type | Code | Message |
|---|---|---|
| 1 | 1 | Run Mode Powerup |
| 1 | 60 | Non-recoverable |
| 1 | 61 | Non-recoverable – Diagnostics Saved |
| 1 | 62 | Non-recoverable – Program Saved |
| 3 | 16 | I/O Connection Failure |
| 3 | 20 | Chassis Failure |
| 3 | 21 | |
| 3 | 23 | Connection Failure |
| 4 | 16 | Unknown Instruction |
| 4 | 20 | Invalid Array Subscript |
| 4 | 21 | Control Structure LEN or POS < 0 |
| 4 | 31 | Invalid JSR Parameter |
| 4 | 34 | Timer Failure |
| 4 | 42 | Invalid JMP Target |
| 4 | 82 | SFC Jump Back Failure |
| 4 | 83 | Value Out of Range |
| 4 | 84 | Stack Overflow |
| 4 | 89 | Invalid Target Step |
| 4 | 90 | Invalid Instruction |
| 4 | 91 | Invalid Context |
| 4 | 92 | Invalid Action |
| 4 | 990 | User-defined |
| 4 | 991 | |
| 4 | 992 | |
| 4 | 993 | |
| 4 | 994 | |
| 4 | 995 | |
| 4 | 996 | |
| 4 | 997 | |
| 4 | 998 | |
| 4 | 999 | |
| 6 | 1 | Task Watchdog Expired |
| 7 | 40 | Save Failure |
| 7 | 41 | Bad Restore Type |
| 7 | 42 | Bad Restore Revision |
| 7 | 43 | Bad Restore Checksum |
| 8 | 1 | key switch Change Ignored |
| 11 | 1 | Positive Overtravel Limit Exceeded |
| 11 | 2 | Negative Overtravel Limit Exceeded |
| 11 | 3 | Position Error Tolerance Exceeded |
| 11 | 4 | Encoder Channel Connection Fault |
| 11 | 5 | Encoder Noise Event Detected |
| 11 | 6 | SERCOS Drive Fault |
| 11 | 7 | Synchronous Connection Fault |
| 11 | 8 | Servo Module Fault |
| 11 | 9 | Asynchronous Connection Fault |
| 11 | 10 | Motor Fault |
| 11 | 11 | Motor Thermal Fault |
| 11 | 12 | Drive Thermal Fault |
| 11 | 13 | SERCOS Communications Fault |
| 11 | 14 | Inactive Drive Enable Input Detected |
| 11 | 15 | Drive Phase Loss Detected |
| 11 | 16 | Drive Guard Fault |
| 11 | 32 | Motion Task Overlap Fault |
| 11 | 33 | CST Reference Loss Detected |
| 18 | 1 | CIP Motion Initialization Fault |
| 18 | 2 | CIP Motion Initialization Fault Mfg |
| 18 | 3 | CIP Motion Axis Fault |
| 18 | 4 | CIP Motion Axis Fault Mfg |
| 18 | 5 | CIP Motion Fault |
| 18 | 6 | CIP Module Fault |
| 18 | 7 | Motion Group Fault |
| 18 | 8 | CIP Motion Configuration Fault |
| 18 | 9 | CIP Motion APR Fault |
| 18 | 10 | CIP Motion APR Fault Mfg |
| 18 | 128 | CIP Motion Guard Fault |

## I/O Fault Codes

I/O faults indicated by the controller are indicated on the status display in one of these formats:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent*:*X #XXXX message*

The first part of the format is used to indicate the location of the faulted module. How the location is indicated depends on your I/O configuration and the module's properties specified in the Logix Designer application.

The latter part of the format, #XXXX message, can be used to diagnose the type of I/O fault and potential corrective actions. For details about each I/O fault code, see the Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

**Table 50 - I/O Fault Messages**

| Code | Message | Code | Message |
|---|---|---|---|
| #0001 | Connection Failure | #0115 | Wrong Device Type |
| #0002 | Insufficient Resource | #0116 | Wrong Revision |
| #0003 | Invalid Value | #0117 | Invalid Connection Point |
| #0004 | IOI Syntax | #0118 | Invalid Configuration Format |
| #0005 | Destination Unknown | #0119 | Module Not Owned |
| #0006 | Partial Data Transferred | #011A | Out of Connection Resources |
| #0007 | Connection Lost | #0203 | Connection Timeout |
| #0008 | Service Unsupported | #0204 | Unconnected Message Timeout |
| #0009 | Invalid Attribute Value | #0205 | Invalid Parameter |
| #000A | Attribute List Error | #0206 | Message Too Large |
| #000B | State Already Exists | #0301 | No Buffer Memory |
| #000C | Object Mode Conflict | #0302 | Bandwidth Not Available |
| #000D | Object Already Exists | #0303 | No Bridge Available |
| #000E | Attribute Not Setable | #0304 | ControlNet Schedule Error |
| #000F | Permission Denied | #0305 | Signature Mismatch |
| #0010 | Device State Conflict | #0306 | CCM Not Available |
| #0011 | Reply Too Large | #0311 | Invalid Port |
| #0012 | Fragment Primitive | #0312 | Invalid Link Address |
| #0013 | Insufficient Command Data | #0315 | Invalid Segment Type |
| #0014 | Attribute Not Supported | #0317 | Connection Not Scheduled |
| #0015 | Data Too Large | #0318 | Invalid Link Address |
| #0100 | Connection In Use | #0319 | No Secondary Resources Available |
| #0103 | Transport Not Supported | #031E | No Available Resources |
| #0106 | Ownership Conflict | #031F | No Available Resources |
| #0107 | Connection Not Found | #0800 | Network Link Offline |
| #0108 | Invalid Connection Type | #0801 | Incompatible Multicast RPI |
| #0109 | Invalid Connection Size | #0802 | Invld Safety Conn Size |
| #0110 | Module Not Configured | #0803 | Invld Safety Conn Format |
| #0111 | RPI Out of Range | #0804 | Invld Time Correct Conn Format |
| #0113 | Out of Connections | #0805 | Invld Ping Intrvl EPI Multiplier |
| #0114 | Wrong Module | #0806 | Time Coord Msg Min Multiplier |

**I/O Fault Messages (continued)**

| Code | Message |
|---|---|
| #0807 | Time Expectation Multiplier |
| #0808 | Timeout Multiplier |
| #0809 | Invld Max Consumer Number |
| #080A | Invld CPCRC |
| #080B | Time Correction Conn ID Invld |
| #080C | Safety Cfg Signature Mismatch |
| #080D | Safety Netwk Num Not Set OutOfBx |
| #080E | Safety Netwk Number Mismatch |
| #080F | Cfg Operation Not Allowed |
| #0814 | Data Type Mismatch |
| #FD01 | Bad Backplane EEPROM |
| #FD02 | No Error Code |
| #FD03 | Missing Required Connection |
| #FD04 | No CST Master |
| #FD05 | Axis or GRP Not Assigned |
| #FD06 | SERCOS Transition Fault |
| #FD07 | SERCOS Init Ring Fault |
| #FD08 | SERCOS Comm Fault |
| #FD09 | SERCOS Init Node Fault |
| #FD0A | Axis Attribute Reject |
| #FD1F | Safety Data Fault |
| #FD20 | No Safety Task Running |
| #FD21 | Invld Safety Conn Parameter |
| #FE01 | Invalid Connection Type |
| #FE02 | Invalid Update Rate |
| #FE03 | Invalid Input Connection |
| #FE04 | Invalid Input Data Pointer |
| #FE05 | Invalid Input Data Size |
| #FE06 | Invalid Input Force Pointer |
| #FE07 | Invalid Output Connection |

| Code | Message |
|---|---|
| #FE08 | Invalid Output Data Pointer |
| #FE09 | Invalid Output Data Size |
| #FE0A | Invalid Output Force Pointer |
| #FE0B | Invalid Symbol String |
| #FE0C | Invalid Scheduled P/C Instance |
| #FE0D | Invalid Symbol Instance |
| #FE0E | Module Firmware Updating |
| #FE0F | Invalid Firmware File Revision |
| #FE10 | Firmware File Not Found |
| #FE11 | Firmware File Invalid |
| #FE12 | Automatic Firmware Update Failed |
| #FE13 | Update Failed - Active Connection |
| #FE14 | Searching Firmware File |
| #FE22 | Invalid Connection Type |
| #FE23 | Invalid Unicast Allowed |
| #FF00 | No Connection Instance |
| #FF01 | Path Too Long |
| #FF04 | Invalid State |
| #FF08 | Invalid Path |
| #FF0B | Invalid Config |
| #FF0E | No Connection Allowed |
| #FE22 | Invalid Connection Type |
| #FE23 | Invalid Unicast Allowed |
| #FF00 | No Connection Instance |
| #FF01 | Path Too Long |
| #FF04 | Invalid State |
| #FF08 | Invalid Path |
| #FF0B | Invalid Config |
| #FF0E | No Connection Allowed |
| — | |

## Notes:

# Change Controller Type



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

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

**IMPORTANT** GuardLogix 5560 controllers and 1768 Compact GuardLogix® controllers are not supported in Studio 5000 version 21 or later.

## Change from a Standard to a Safety Controller

To successfully change the controller type from a standard controller to a safety controller, the chassis slot immediately to the right of the safety primary controller must be available for the safety partner.

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 (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).

## Change from a Safety to a Standard Controller

Upon confirmation of a change from a safety controller project to a standard controller, some components are changed and others are deleted, as described below:

- The safety partner is deleted from the I/O chassis.
- Safety I/O devices and their tags are deleted.
- The safety task, programs, and routines are changed to a standard task, programs, and routines.
- All safety tags, except safety consume tags, are changed to standard tags. Safety consume tags are deleted.
- Safety tag mappings are deleted.
- The safety network 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 can still reference modules that have been deleted and can produce verification errors.
- Consumed tags are deleted when the producing module is deleted.
- As a result of the above changes to the system, safety-specific instructions and safety I/O tags do not verify.

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

## Change Safety Controller Types

**IMPORTANT** 1768 Compact GuardLogix controllers and GuardLogix 5560 controllers are not supported in the Logix Designer application, version 21.

When you change from one safety controller type to another, the class of tags, routines, and programs remain unaltered. Any I/O devices that are no longer compatible with the target controller are deleted.

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 from a 1768 Compact GuardLogix to a GuardLogix 5570 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 GuardLogix 5570 controller supports 100 safety programs in the safety task while a 1768 Compact GuardLogix controller supports 32.

Floating-point instructions, such as FAL, FLL, FSC, SIZE, CMP, SWPB, and CPT are supported in GuardLogix 5570 controllers, but not in GuardLogix 5560 and 1768 Compact GuardLogix controllers. If your safety program contains these instructions, verification errors can occur when changing from a GuardLogix 5570 controller to a GuardLogix 5560 or 1768 Compact GuardLogix controller.

## More Resources

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

## Notes:

## Numerics



## A



## B



## C

## D



## E



## F

## G



## H



## I



## K



## L



## M



## N

## O



## P



## R

## S

## T



## U



## V



## W



## X

## Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

## Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

| | |
|---|---|
| United States or Canada | 1.440.646.3434 |
| Outside United States or Canada | Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page, or contact your local Rockwell Automation representative. |

## New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

| | |
|---|---|
| United States | Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process. |
| Outside United States | Please contact your local Rockwell Automation representative for the return procedure. |

## Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.