

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

User Manual

Allen-Bradley

GuardLogix Controllers

Catalog Numbers 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT









Important User Information

Solid-state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication SGI-1.1 available from your local Rockwell Automation sales office or online at http://www.rockwellautomation.com/literature/) describes some important differences between solid-state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid-state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

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

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

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

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

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

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

Rockwell Automation, Allen-Bradley, TechConnect, Integrated Architecture, ControlLogix, ControlLogix-XT, GuardLogix, Logix-XT, Guard I/O, CompactBlock Guard I/O, POINT Guard I/O, PowerFlex, PanelView, PLC-5, DriveLogix, FlexLogix, PhaseManager, ControlFLASH, Logix5000, RSLogix 5000, FactoryTalk, RSNetWorx for EtherNet/IP, RSNetWorx for DeviceNet, RSNetWorx for ControlNet, and RSLinx are trademarks of Rockwell Automation, Inc.

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

The information below summarizes the changes to this manual since the last publication.

To help you find new and updated information in this release of the manual, we included change bars as shown to the right of this paragraph.

Topic	Pages
Information on 1756-L71S controllers	11, 18, 21, 26, 47
Guidance on installing the Energy Storage module	46

Notes:

Preface

About 1756 GuardLogix Controllers 11
Understanding Terminology 12
Additional Resources 13

Chapter 1

System Overview

Safety Application Requirements 15
- Safety Network Number 15
- Safety Task Signature 16

Distinguishing Between Standard and Safety Components 16
- HMI Devices 16

Controller Data Flow Capabilities 17
Selecting System Hardware 18
- Primary Controller 18
- Safety Partner 19
- Chassis 19
- Power Supply 19

Selecting Safety I/O Modules 20
Selecting Communication Networks 20
Programming Requirements 21

Chapter 2

Install the Controller

Precautions 23
- Environment and Enclosure Information 23
- Programmable Electronic Systems (PES) 24
- Removal and Insertion Under Power (RIUP) 24
- North American Hazardous Location Approval 24
- European Hazardous Location Approval 25
- Prevent Electrostatic Discharge 25

Make Sure That You Have All of the Components 25
- 1756-L6*x*S Controllers 26
- 1756-L7*x*S Controllers 26

Install a Chassis and Power Supply 27
Connect the Battery
(1756-L6*x*S controllers only) 27
Install the Controller into the Chassis 28
Insert or Remove a Memory Card 29
- Secure Digital Card (1756-L7*x*S controllers) 30
- CompactFlash Card (1756-L6*x*S controllers) 32

Make Communication Connections 34
- Connect to the 1756-L7*x*S Controller's USB Port 34
- Connect to the 1756-L6*x*S Controller's Serial Port 36

Update the Controller 39
- Using ControlFLASH Software to Update Firmware 39
- Using AutoFlash to Update Firmware 41

Choose the Operating Mode of the Controller 42
Use the Keyswitch to Change the Operation Mode 42
Use RSLogix 5000 Software to Change the Operation Mode 43
Uninstall an Energy Storage Module (ESM) 44
Install an Energy Storage Module (ESM) 46

Chapter 3

Configure the Controller

Create a Controller Project 47
Set Passwords for Safety-locking and -unlocking 49
Protecting the Safety Task Signature in Run Mode 50
Handling I/O Module Replacement 51
Enable Time Synchronization 51
Configure a Peer Safety Controller 52

Chapter 4

Communicate over Networks

The Safety Network 53
Managing the Safety Network Number (SNN) 53
Assigning the Safety Network Number (SNN) 55
Changing the Safety Network Number (SNN) 55
EtherNet/IP Communication 59
Producing and Consuming Data via an EtherNet/IP Network . . . 60
Connections over the EtherNet/IP Network 60
EtherNet/IP Communication Example 61
EtherNet/IP Connections for CIP Safety I/O Modules 61
Standard EtherNet/IP Connections 62
ControlNet Communication 63
Producing and Consuming Data via a ControlNet Network 63
Connections over the ControlNet Network 64
ControlNet Communication Example 64
ControlNet Connections for Distributed I/O 65
DeviceNet Communication 65
DeviceNet Connections for CIP Safety I/O Modules 66
Standard DeviceNet Connections 66
Serial Communication 67
Additional Resources 68

Chapter 5

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

Adding CIP Safety I/O Modules 69
Configure CIP Safety I/O Modules via RSLogix 5000 Software 70
Setting the Safety Network Number (SNN) 71
Using Unicast Connections on EtherNet/IP Networks 71
Setting the Connection Reaction Time Limit 71
Specify the Requested Packet Interval (RPI) 72
View the Maximum Observed Network Delay 72
Setting the Advanced Connection Reaction Time Limit Parameters 73

Understanding the Configuration Signature 75
Configuration via RSLogix 5000 Software 75
Different Configuration Owner (listen only connection) 76
Reset Safety I/O Module Ownership 76
Addressing Safety I/O Data 76
Monitor Safety I/O Module Status 77
Resetting a Module to Out-of-box Condition 79
Replacing a Module by Using RSLogix 5000 Software 79
Replacement with 'Configure Only When No Safety Signature Exists' Enabled 80
Replacement with 'Configure Always' Enabled 84
Replacing a POINT Guard I/O Module By Using RSNetWorx for DeviceNet Software 86

Chapter 6

Develop Safety Applications

The Safety Task 90
Safety Task Period Specification 90
Safety Task Execution 91
Safety Programs 92
Safety Routines 92
Safety Tags 92
Tag Type 93
Data Type 94
Scope 95
Class 96
Constant Value 96
External Access 96
Produced/Consumed Safety Tags 97
Configure the Peer Safety Controllers' Safety Network Numbers . 97
Produce a Safety Tag 99
Consume Safety Tag Data 100
Safety Tag Mapping 102
Restrictions 103
Create Tag Mapping Pairs 103
Monitor Tag Mapping Status 104
Safety Application Protection 105
Safety-lock the Controller 105
Generate a Safety Task Signature 106
Software Restrictions 108

Chapter 7

Go Online with the Controller

Connecting the Controller to the Network 109
Connect Your EtherNet/IP Device and Computer 110
Connect Your ControlNet Communication Module or DeviceNet Scanner and Your Computer 110
Configuring an EtherNet/IP, ControlNet, or DeviceNet Driver 110
Understanding the Factors that Affect Going Online 111
Project to Controller Matching 111
Firmware Revision Matching 111
Safety Status/Faults 111
Safety Task Signature and Safety-locked and -unlocked Status . . . 112
Download 113
Upload 115
Go Online 116

Chapter 8

Store and Load Projects Using Nonvolatile Memory

Using Memory Cards for Nonvolatile Memory 119
Storing a Safety Project 120
Loading a Safety Project 121
Use Energy Storage Modules (1756-L7*x*S controllers only) 122
Save the Program to On-board NVS Memory 122
Clear the Program from On-board NVS Memory 123
Estimate the ESM Support of the WallClockTime 124
Manage Firmware with Firmware Supervisor 124

Chapter 9

Monitor Status and Handle Faults

Viewing Status via the Online Bar 125
Monitoring Connections 126
All Connections 126
Safety Connections 127
Monitoring Status Flags 127
Monitoring Safety Status 128
Controller Faults 128
Nonrecoverable Controller Faults 129
Nonrecoverable Safety Faults in the Safety Application 129
Recoverable Faults in the Safety Application 129
Viewing Faults 130
Fault Codes 130
Developing a Fault Routine 131
Program Fault Routine 131
Controller Fault Handler 131
Use GSV/SSV Instructions 132

Appendix A

Status Indicators

1756-L6*x*S Controller Status Indicators 135
1756-L7*x*S Controllers Status Indicators 136
1756-L7*x*S Controller Status Display 137
Safety Status Messages 137
General Status Messages 138
Fault Messages 139
Major Recoverable Fault Messages 139
I/O Fault Codes 140

Appendix B

Maintain the Battery

Estimate Battery Life 143
Before BAT Indicator Turns On 143
After BAT Indicator Turns On 144
When to Replace the Battery 145
Replace the Battery 145
Store Replacement Batteries 147
Additional Resources 147

Appendix C

Change Controller Type in RSLogix 5000 Projects

Changing from a Standard to a Safety Controller 149
Changing from a Safety to a Standard Controller 150
Changing from a 1756 GuardLogix Controller to a 1768 Compact GuardLogix Controller or Vice Versa 151
Changing from a 1756-L7*x*S Controller to a 1756-L6*x*S or 1768-L4*x*S Controller 151
Additional Resources 151

Appendix D

History of Changes

1756-UM020H-EN-P April 2012 153
1756-UM020G-EN-P, February 2012 153
1756-UM020F-EN-P, August 2010 154
1756-UM020E-EN-P, January 2010 154
1756-UM020D-EN-P, July 2008 154
1756-UM020C-EN-P, December 2006 155
1756-UM020B-EN-P, October 2005 155
1756-UM020A-EN-P, January 2005 155

Index

Topic	Page
About 1756 GuardLogix Controllers	11
Understanding Terminology	12
Additional Resources	13

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

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

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

For detailed information on related topics like programming your GuardLogix controller, SIL 3/PLe requirements, or information on standard Logix components, see the list of Additional Resources on page 13.

About 1756 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 1756-L7*x*S and 1756-L6*x*S Controllers

Feature	**1756-L7*x*S** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**1756-L6*x*S** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Clock support and backup 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 card
Status indicators	Scrolling status display and LED status indicators	LED status indicators

The extreme environment GuardLogix controller, catalog numbers 1756-L73SXT and 1756-L7SPXT, provides 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.

Understanding Terminology

This table defines terms 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 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 1756-L7*x*S and 1756-L73SXT 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.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
RPI	Requested Packet Interval	The expected rate in time for production of data when communicating over a network.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	An instruction that sets controller system data.
—	Standard	An object, task, tag, program, or component in your project that is not a safety-related item.
—	Unicast	The transmission of information from one sender to one receiver.

Additional Resources

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

Table 3 - Publications Related to GuardLogix Controllers and Systems

For more information about	See This Resource	Description
(Safety) Application requirements	GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093	Contains detailed requirements for achieving and maintaining SIL 3/PLe with the GuardLogix controller system.
Batteries	Guidelines for Handling Lithium Batteries, publication AG-5.4	Provides information regarding storage, handling, transportation, and disposal of lithium batteries.
	Programmable Controllers Battery Reference, http://www.ab.com/programmablecontrol/batteries.html	Provides Material Safety Data Sheets (MSDS) for individual replacement batteries.
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.
Design and selection	Logix5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides advanced users with guidelines for system optimization and with system information to guide system design choices.
	ControlLogix Selection Guide, publication 1756-SG001	Provides a high-level selection process for ControlLogix® system components, critical specifications information for making initial decisions, and links to complete specifications information.
Guard I/O	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.
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 grounding and wiring 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.
	CIP Motion Configuration and Startup User Manual, publication MOTION-UM003	Details how to configure a Integrated Motion on EtherNet/IP networks application system.
	CIP Motion 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 for setting up and programming a Logix5000 controller to use equipment phases.

Table 3 - Publications Related to GuardLogix Controllers and Systems

For more information about	See This Resource	Description
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 managing project files, organizing tags, ladder logic programming, testing routines, creating Add-On Instructions, controller status data, handling faults, importing and exporting project components and more.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087	Assists in estimating the memory use and execution time of programmed logic and in selecting among different programming options.
Redundancy	ControlLogix Redundancy System User Manual, publication 1756-UM523	Guides the design, development, and implementation of a standard ControlLogix redundancy system.
	ControlLogix Enhanced Redundancy System User Manual, publication 1756-UM535	Guides the design, development, and implementation of an enhanced ControlLogix redundancy system.

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

System Overview

Topic	Page
Safety Application Requirements	15
Distinguishing Between Standard and Safety Components	16
Controller Data Flow Capabilities	17
Selecting System Hardware	18
Selecting Safety I/O Modules	20
Selecting Communication Networks	20
Programming Requirements	21

Safety Application Requirements

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

For SIL 3 and PLe safety system requirements, including functional validation test intervals, system reaction time, and PFD/PFH calculations, refer to the GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093. You must read, understand, and fulfill these requirements prior to operating a GuardLogix SIL 3, PLe safety system.

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

Refer to the GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093, for details.

Safety Network Number

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

For information on assigning the SNN, see Managing the Safety Network Number (SNN) on page 53.

Safety Task Signature

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

See Generate a Safety Task Signature on page 106 for more information.

Distinguishing Between Standard and Safety Components

Slots of a GuardLogix system chassis not used by the safety function may be populated with other ControlLogix modules that are certified to the Low Voltage and EMC Directives. Refer to http://ab.com/certification/ce to find the CE certificate for the Programmable Control – ControlLogix Product Family and determine which modules are certified.

You must create and document a clear, logical, and visible distinction between the safety and standard portions of the application. To aid in creating this distinction, RSLogix 5000 programming software features safety identification icons to identify the safety task, safety programs, safety routines, and safety components. In addition, the RSLogix 5000 software uses a safety class attribute that is visible whenever safety task, safety programs, safety routine, safety tag, or safety Add-On Instruction properties are displayed.

The controller does not allow writes to safety tag data from external HMI devices or via message instructions from peer controllers. RSLogix 5000 software can write safety tags when the 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.

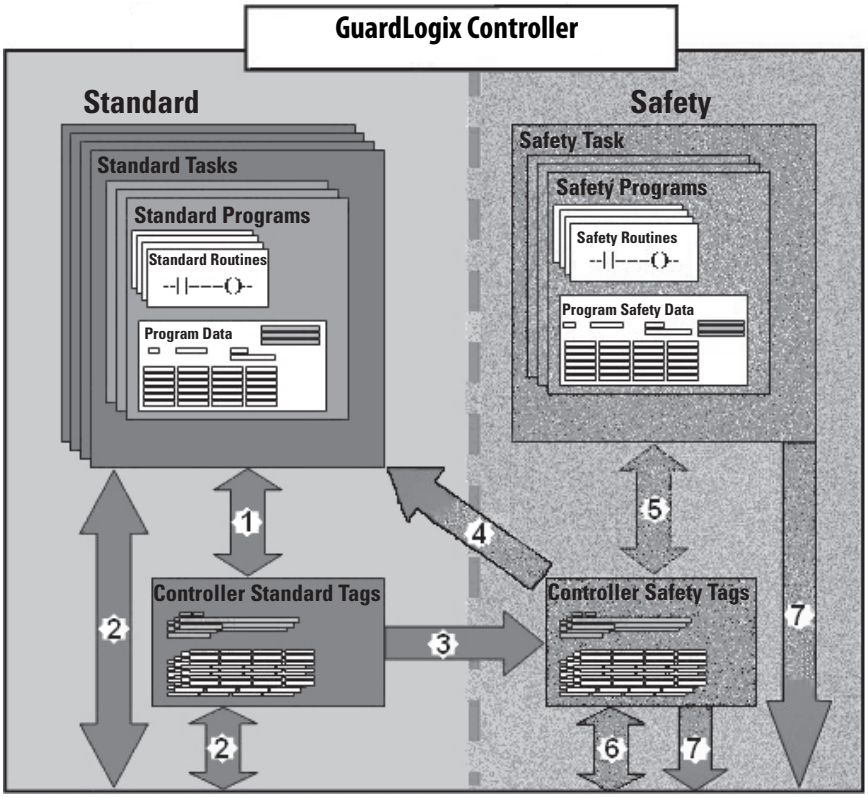
HMI Devices

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

Controller Data Flow Capabilities

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

Figure 1 - Data Flow Capabilities



No.	Description	
1	Standard tags and logic behave the same way they do in the standard Logix platform.	
2	Standard tag data, program- or controller-scoped, can be exchanged with external HMI devices, personal computers, and other controllers.	
3	GuardLogix controllers are integrated controllers with the ability to move (map) standard tag data into safety tags for use within the safety task.	
		**ATTENTION:** This data must not be used to directly control a SIL 3/PLe output.
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.

Selecting System Hardware

The GuardLogix system supports SIL 3 and PLe safety applications. The GuardLogix controller is made up 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 required for safety applications.

Table 4 - Primary Controller and Corresponding Safety Partner Catalog Numbers

Primary Controller	Safety Partner
1756-L61S, 1756-L62S, 1756-L63S	1756-LSP
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-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB
1756-L63S	8 MB	3.75 MB
1756-L71S	2MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

In RSLogix 5000 software, version 18 or later, the GuardLogix controller supports OS upgrades or user program storage and retrieval by using a memory card. However, in version 16 and 17 of RSLogix 5000 software, you could only

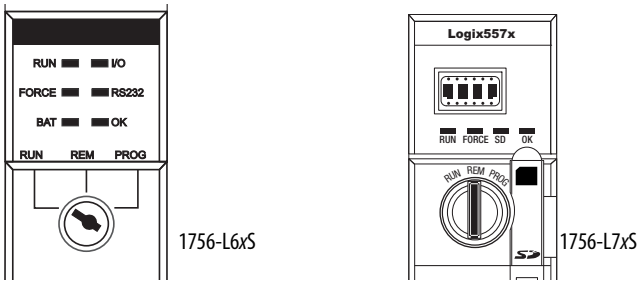
view the contents of a memory card if one was installed in the primary controller. Prior to version 16, memory cards were not supported.

See Chapter 8, Store and Load Projects Using Nonvolatile Memory, for more information.

A three-position keyswitch 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 - Keyswitch 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 keyswitch 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.

Selecting Safety I/O Modules

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

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

Selecting Communication Networks

The 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	Refer to these Installation Instructions
The GuardLogix controller and DeviceNet devices	1756-DNB	DNET-IN001
The GuardLogix controller and EtherNet/IP devices	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR, 1756-EN3TR 1756-EN2TXT	ENET-IN002
Controllers on the ControlNet network	1756-CN2, 1756-CN2R 1756-CN2RXT	CNET-IN005

The GuardLogix controller can connect to RSLogix 5000 programming software via a serial or USB connection, an EtherNet module, or a ControlNet module.

1756-L6*x*S controllers have a serial port. 1756-L7*x*S controllers have a USB port.

See the Additional Resources on page 13 for more information on using network communication modules.

Programming Requirements

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

Use Table 7 to identify the minimum software versions for use with your GuardLogix controllers. RSLogix 5000 software, version 15, does not support Safety Integrity Level (SIL) 3.

Table 7 - Software Versions

Cat. No.	RSLogix 5000 Software Version(1)	RSLinx® Classic Software Version(1)
1756-L61S, 1756-L62S	14	Any version
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) This version or later.

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

Table 8 - Supported Features by RSLogix 5000 Software Version

Feature	Version 14		Version 16		Version 17		Version 18		Version 19		Version 20	
	Safety Task	Standard Task	Safety Task	Standard Task	Safety Task	Standard Task	Safety Task	Standard Task	Safety Task	Standard Task	Safety Task	Standard Task
Add-On Instructions				X		X	X	X	X	X	X	X
Alarms and events				X		X		X		X		X
Controller logging					X	X	X	X	X	X	X	X
Data Access Control							X	X	X	X	X	X
Equipment phase routines				X		X		X		X		X
Event tasks				X		X		X		X		X
Firmware Supervisor				X		X	X	X	X	X	X	X
Function block diagrams (FBD)				X		X		X		X		X
Integrated motion				X		X		X		X		X
Ladder logic	X	X	X	X	X	X	X	X	X	X	X	X
Language switching					X	X	X	X	X	X	X	X
Memory card							X	X	X	X	X	X
Online import and export of program components						X		X		X		X
Sequential function chart (SFC) routines				X		X		X		X		X
Structured text				X		X		X		X		X
Unicast connections for produced and consumed safety tags									X	X	X	X
Unicast connections for safety I/O modules on EtherNet/IP networks											X	X

For information on using these features, refer to the Logix5000 Controllers Common Procedures Programming Manual, publication 1756-PM001, the publications listed in the Additional Resources on page 13, and RSLogix 5000 software online help.

Notes:

Install the Controller

Topic	Page
Precautions	23
Make Sure That You Have All of the Components	25
Install a Chassis and Power Supply	27
Connect the Battery (1756-L6xS controllers only)	27
Install the Controller into the Chassis	28
Insert or Remove a Memory Card	29
Make Communication Connections	34
Update the Controller	39
Choose the Operating Mode of the Controller	42
Uninstall an Energy Storage Module (ESM)	44
Install an Energy Storage Module (ESM)	46

Precautions

Read and follow these precautions for use.

Environment and Enclosure Information



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

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

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

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by 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 • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • 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. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	 **AVERTISSEMENT:** RISQUE D'EXPLOSION • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • 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. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • 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:

- This equipment must be installed in an enclosure providing at least IP54 protection when applied in Zone 2 environments.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- This equipment must be used only with ATEX certified Rockwell Automation backplanes.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.

Prevent Electrostatic Discharge



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

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

Make Sure That You Have All of the Components

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

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

1756-L6*x*S Controllers

A 1747-KY key and a 1756-BA2 battery ship with the 1756-L6*x*S controller, while the 1756-LSP safety partner ships with a 1756-BA2 battery.

If you want to connect a device to the serial port of the controller (for example, connect a computer to the controller), use a 1756-CP3 serial cable.

For nonvolatile memory, you can use a 1784-CF128 CompactFlash card with 1756-L6*x*S GuardLogix controllers, firmware revision 18 and later.

1756-L7*x*S Controllers

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

Cat. No.	Description	Ships with
1756-L71S 1756-L72S 1756-L73S	Primary controller	• 1756-ESMCAP capacitor-based energy storage module (ESM) • 1784-SD1 Secure Digital (SD) memory card, 1 GB • 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) • 1747-KY key
1756-L7SPXT	Extreme temperature safety partner	• 1756-SPESMNSEXT capacitor-based energy storage module (ESM)

The following optional equipment may 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 deplete 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 1756-SPESMNSE for the safety partner(2) This ESM does not have WallClockTime backup power. Additionally, you can use this ESM with a 1756-L73S (8 MB) or smaller memory sized controller only.
ESM that secures the controller by preventing the USB connection and SD card use(1)	1756-ESMNRM for the primary controller 1756-SPESMNRM for the safety partner(3) 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 124.

(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.

Connect the Battery (1756-L6*x*S controllers only)

1756-L6*x*S controllers and the 1756-LSP safety partner contain a lithium battery, which is intended to be replaced during the life of the product.



WARNING: When you connect or disconnect the battery, 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.

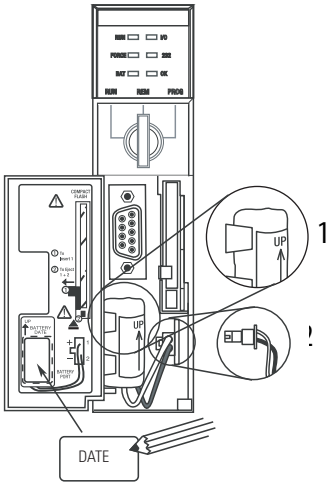
For safety information on the handling of lithium batteries, including handling and disposal of leaking batteries, see Guidelines for Handling Lithium Batteries, publication AG 5-4.

To maintain the memory of the controller while the controller is without power, connect a battery. Follow the procedure for both the 1756-L6*x*S controller and 1756-LSP safety partner.

IMPORTANT Connect only a 1756-BA2 battery to the controller. If you connect a different battery, you may damage the controller.

Follow these steps to install a new 1756-BA2 battery.

1. Insert the battery as shown.
2. Connect the battery:
   + Red
   - Black
3. Write the date you installed the battery on the battery label and attach the label to the inside of the controller door.



See Appendix B for more information on maintaining the battery.

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.

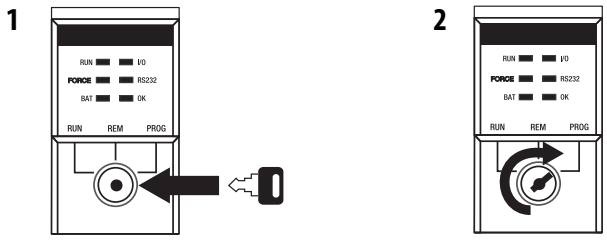
Be sure that power is removed or the area is nonhazardous before proceeding. Repeated electrical arcing causes excessive wear to contacts on both the module and its mating connector. Worn contact may create electrical resistance that can affect module operation.

IMPORTANT For 1756-L7*x*S controllers and 1756-L7SP safety partners, 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.

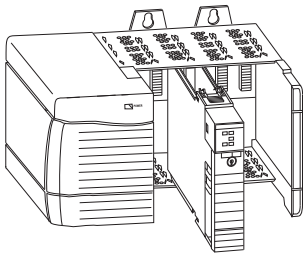
After power is applied, the ESM charges for up to two minutes as indicated by CHRG or ESM Charging on the status display.

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



The safety partner does not have a keyswitch.

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 keyswitch 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.

1756-L7*x*S controllers use Secure Digital (SD) cards. See page 30.

1756-L6*x*S controller use CompactFlash (CF) cards. See page 32.

Secure Digital Card (1756-L7*x*S controllers)

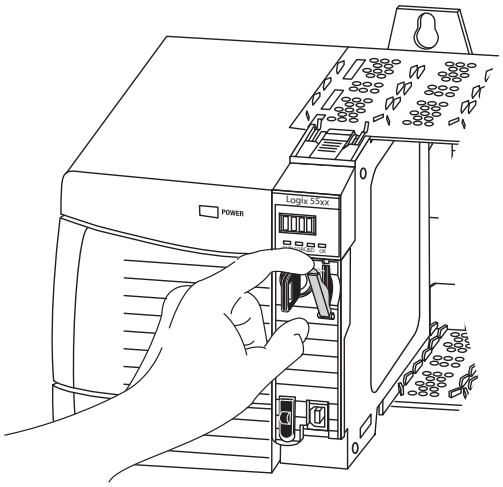
The 1756-L7*x*S controller ships with an SD card installed. We recommend that you leave an SD card installed.

Remove the SD Card

If you want to remove the SD card from the 1756-L7*x*S controller, follow these steps.

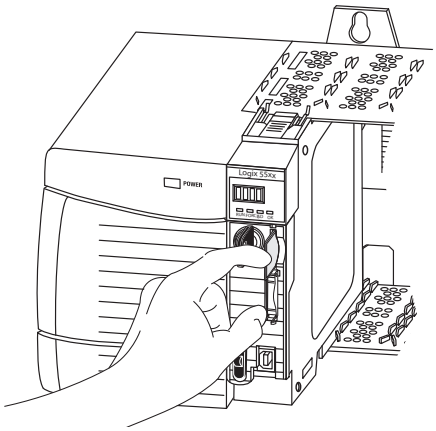
IMPORTANT	Verify that the SD card status indicator is off and that the card is not in use before removing it.

1. Turn the keyswitch 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.



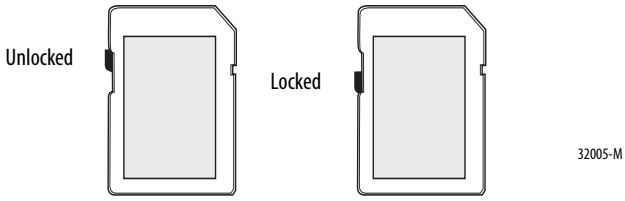
32004-M

4. Remove the SD card and close the door.

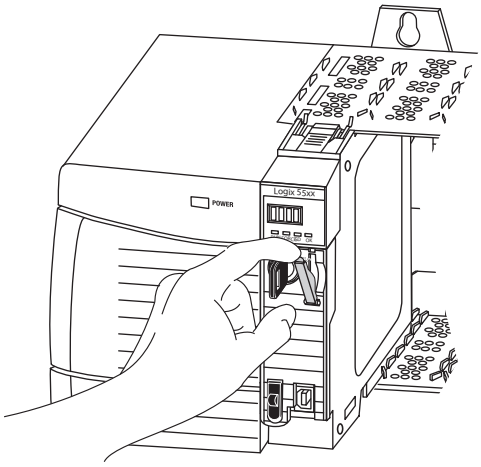
Install the SD Card

Follow these steps to install the SD card on the 1756-L7*x*S controllers.

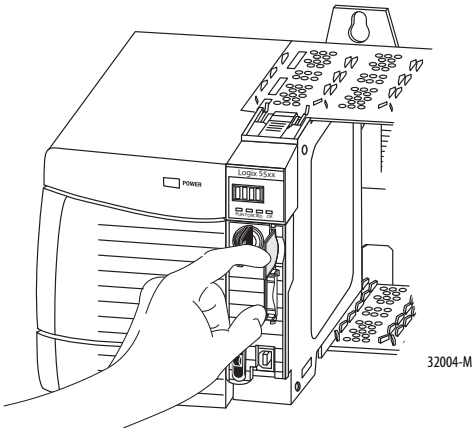
1. Verify that the SD card is locked or unlocked according to your preference.



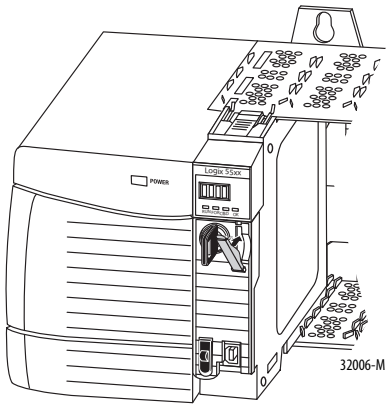
2. Open the door for the SD card.



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.



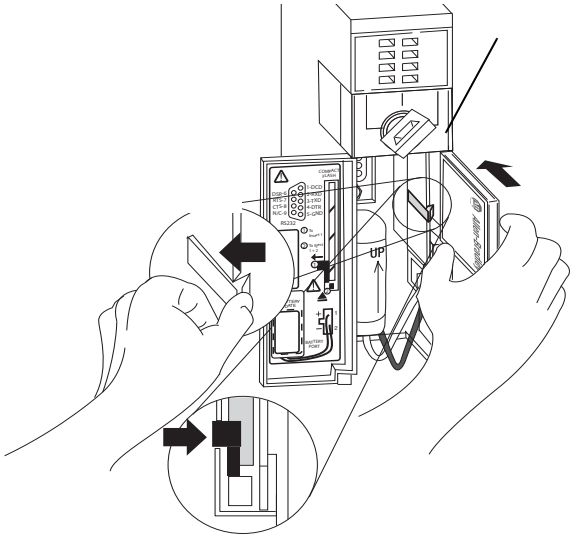
CompactFlash Card (1756-L6*x*S controllers)

The 1756-L6xS controllers do not ship with CompactFlash cards installed.

Install a CF Card

Follow these steps to insert the memory card.

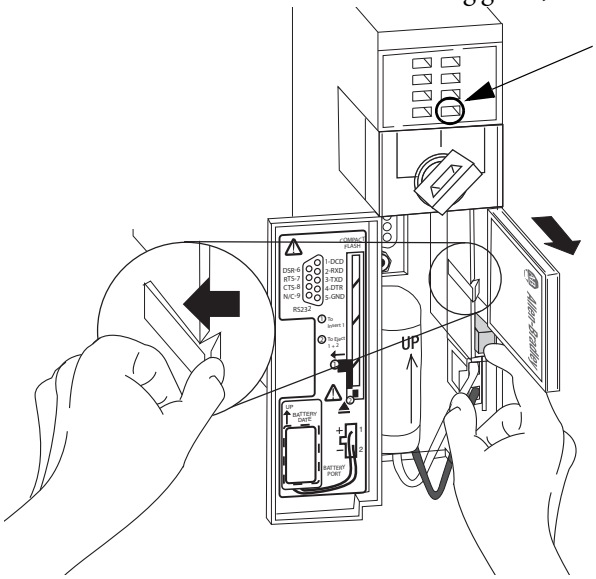
1. Turn the keyswitch to the PROG position.
2. Open the door of the controller.
3. Push the latch to the left.
4. Insert the memory card with the A-B logo pointing left.
5. Release the latch and make sure it slides over the memory card.



Remove a CF Card

Follow these steps to remove the memory card.

1. If the OK status indicator is flashing green, wait until it turns solid green.



2. Open the door of the controller.
3. Push and hold the latch to the left.
4. Push the eject button and remove the card.
5. Release the latch.

Make Communication Connections

1756-L7*x*S controllers feature a USB port. See Connect to the 1756-L7xS Controller's USB Port.

1756-L6*x*S controllers feature a serial port. See Connect to the 1756-L6xS Controller's Serial Port on page 36.

Connect to the 1756-L7*x*S Controller's USB Port

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

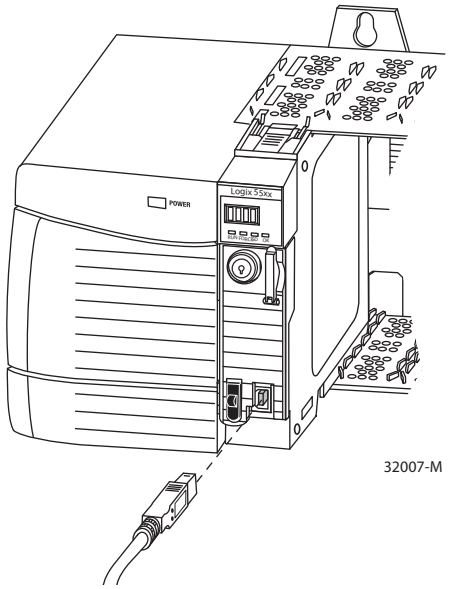
To use the USB port of the controller, you must have RSLinx software, version 2.59 or later, installed on your workstation. Use a USB cable to connect your workstation to the USB port. With this connection, you can upgrade firmware and download programs to the controller directly from your workstation.

ATTENTION: The USB port is intended for temporary local programming purposes only and not intended for 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 Connection



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.

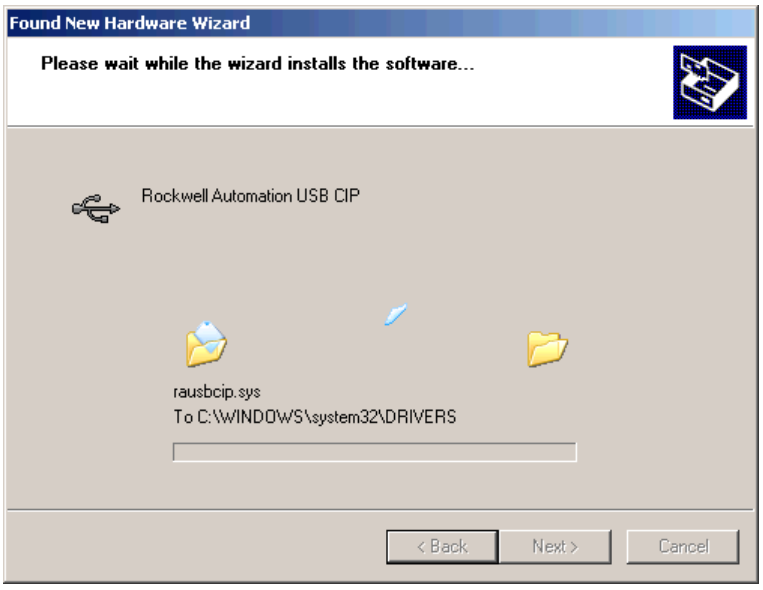
1. Connect your controller and workstation by using a USB cable.
2. On the Found New Hardware Wizard dialog box, click any of the Windows Update connection options and click Next.



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.

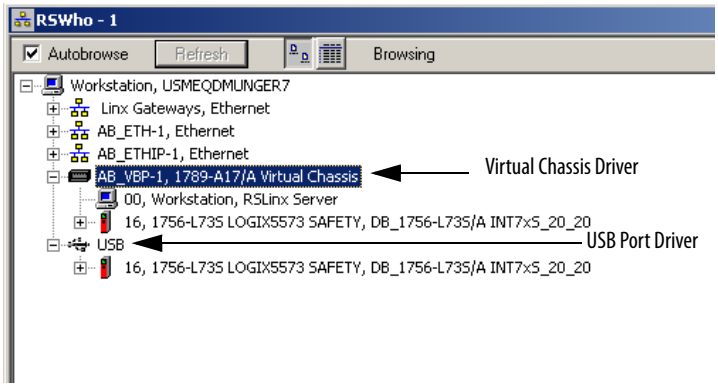
   The software is installed.



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.



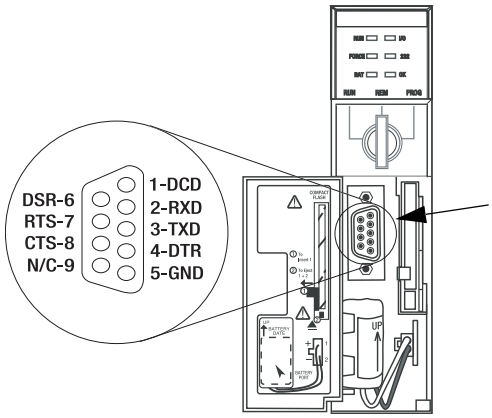
Connect to the 1756-L6*x*S Controller's Serial Port

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

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

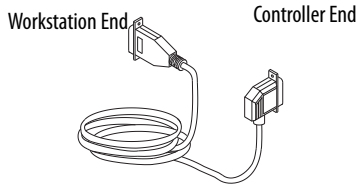
Use the serial port on the 1756-L6*x*S controller for RS-232 communication.

Figure 4 - Serial Port



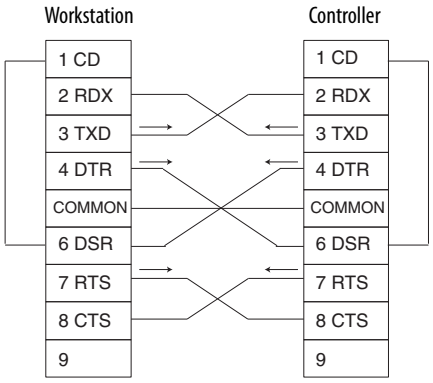
To connect a workstation to the serial port, use one of these cables:

- 1756-CP3 serial cable
- 1747-CP3 cable from the SLC product family (If you use this cable, the controller door may not close.)



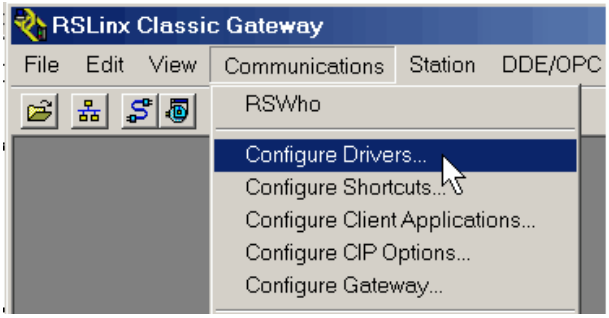
If you make your own serial cable, follow these guidelines.

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

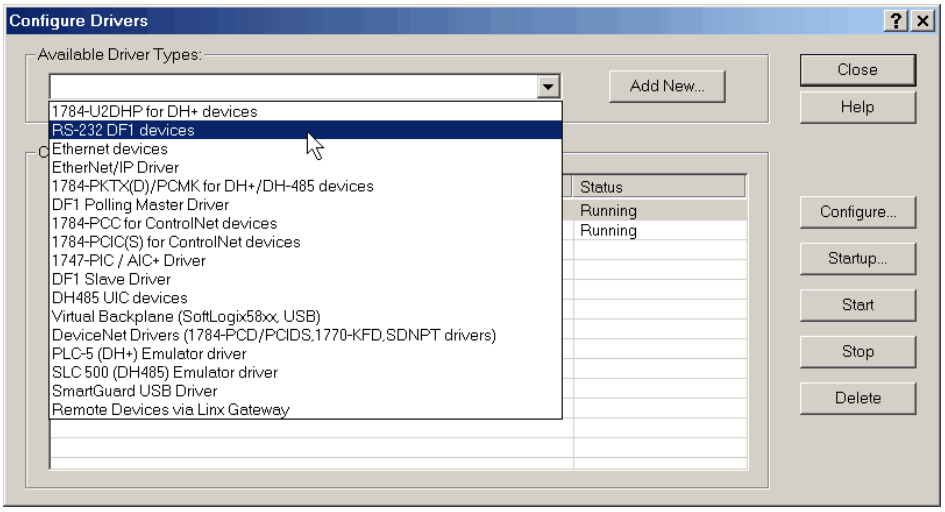


Follow these steps to use RSLinx software to configure the RS-232 DF1 device driver for serial communication.

1. In RSLinx software, from the Communications menu, choose Configure Drivers.

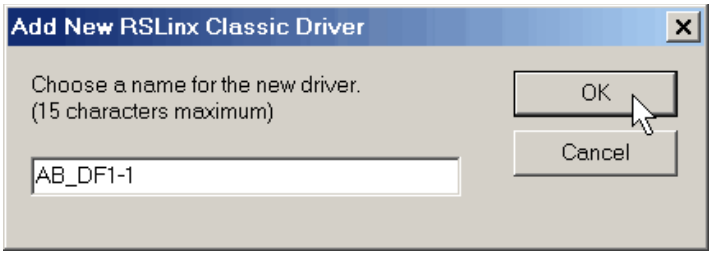


The Configure Drivers dialog box appears.



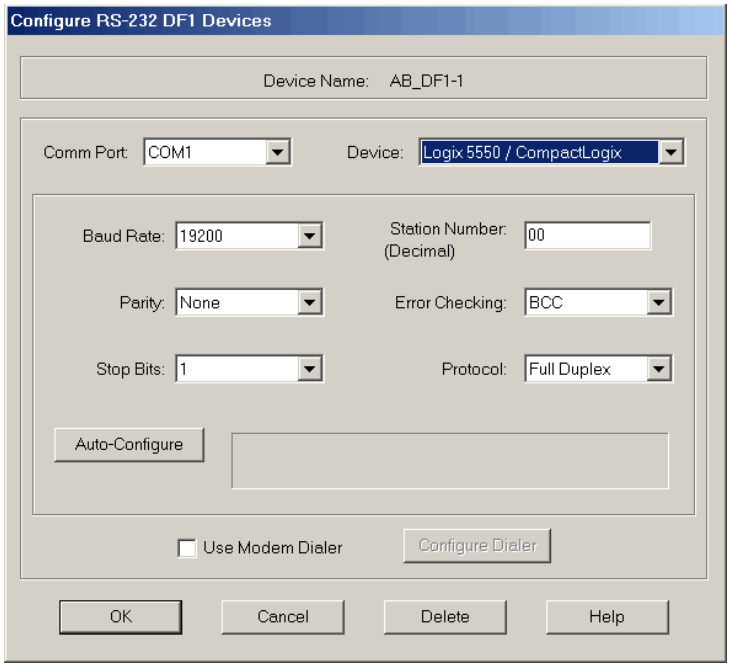
2. From the Available Driver Types pull-down list, choose the RS-232 DF1 device driver.
3. Click Add New.

   The Add New RSLinx Driver dialog box appears.



4. Type the driver name and click OK.
5. Specify the serial port settings.
   a. From the Comm Port pull-down menu, choose the serial port on the workstation to which the cable is connected.
   b. From the Device pull-down menu, choose Logix 5550/CompactLogix.

c. Click Auto-Configure.



6. If the auto configuration is successful, click OK.

   If the auto configuration is not successful, verify that the correct Comm Port was selected.

7. Click Close.

Update the Controller

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

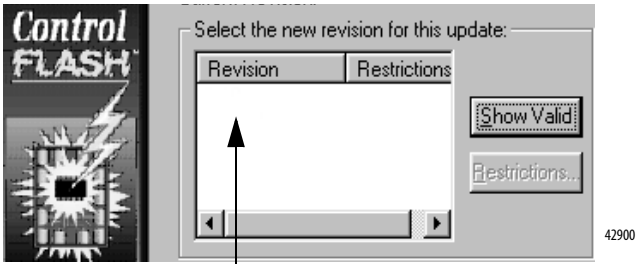
You can upgrade your firmware by using either ControlFLASH™ software, which is packaged with RSLogix 5000 software or by using the AutoFlash feature of RSLogix 5000 software.

Using ControlFLASH Software to Update Firmware

With ControlFLASH software, version 8 or later (RSLogix 5000 software, version 18 or later) software, the safety partner updates automatically, when the primary controller is updated.

IMPORTANT	On 1756-L7*x*S controllers, 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 to which you want to update the controller 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.

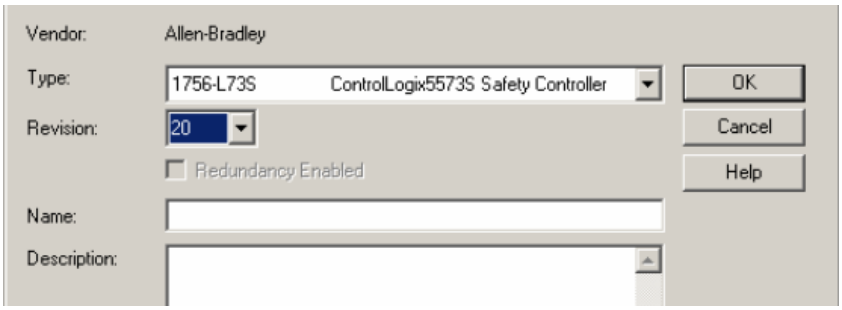
TIP	If the ControlFLASH update of the controller is interrupted, the 1756-L7*x*S controller reverts to boot firmware, that is firmware revision 1.*xxx*.

9. Click OK.
10. Close ControlFLASH software.

Using AutoFlash to Update Firmware

To update your controller firmware with the AutoFlash feature of RSLogix 5000 software, follow these steps.

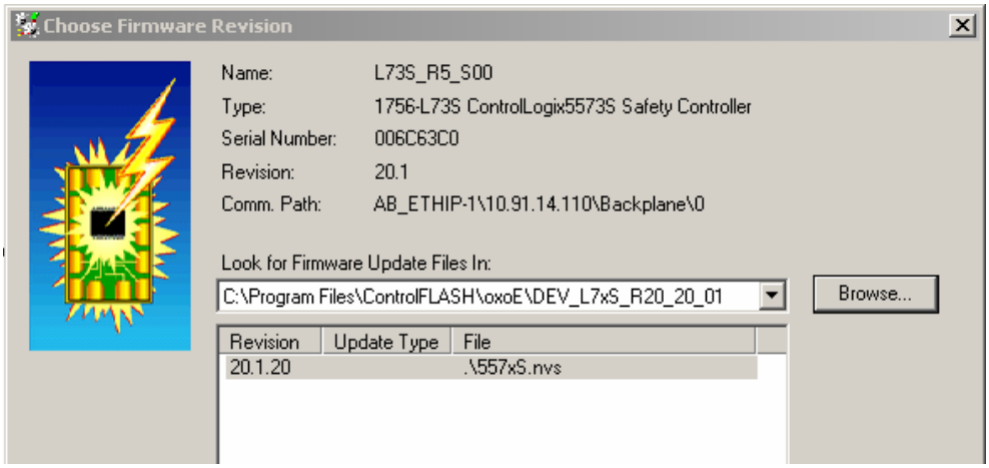
1. Verify that the appropriate network connection is made and your network driver is configured in RSLinx software.
2. Use RSLogix 5000 programming software to create a controller project at the version you need.



3. Click RSWho to specify the controller path.



4. Select your controller and click Update Firmware.
5. Select the firmware revision to update to.



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 may complete other tasks in RSLogix 5000 software.

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

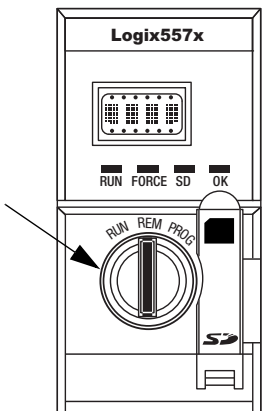
Use the Keyswitch to Change the Operation Mode

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

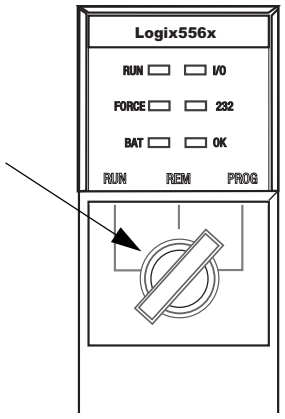
- Program (PROG)
- Remote (REM)
- Run (RUN)

Figure 5 - Controller Keyswitch

1756-L7*x*S



1756-L6*x*S



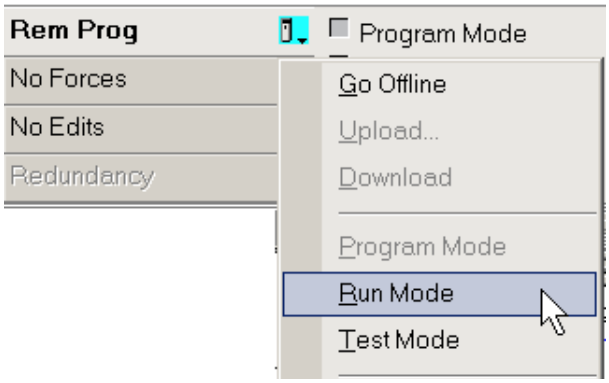
Use RSLogix 5000 Software to Change the Operation Mode

Depending on the mode of the controller you specify by using the keyswitch, you can change the operation mode of the controller using RSLogix 5000 software.

After you are online with the controller and the controller keyswitch is set to Remote (REM or the center position), you can use the Controller Status menu in the upper-left corner of the RSLogix 5000 software window to specify these operation modes:

- Remote Program
- Remote Run
- Remote Test

Figure 6 - Operation Mode via RSLogix 5000 Software



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

Uninstall an Energy Storage Module (ESM)

1756-L7*x*S 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 1756-L7*x*S controllers lose 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 a 1756-L7xS 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, use only 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 µJoule 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 keyswitch.

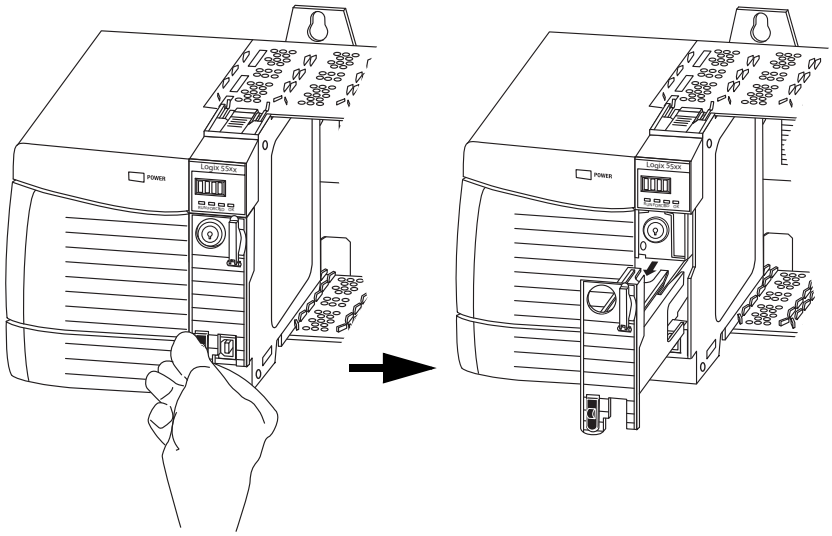
IMPORTANT The next step depends on which of the following conditions applies to your application:

- If you are removing the ESM from a powered 1756-L7*x*S(XT) controller, go to step 2.
- If you are removing the ESM from a 1756-L7*x*S(XT) 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.



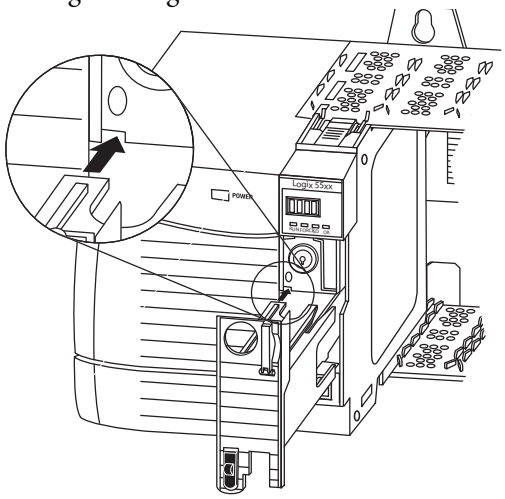
Install an Energy Storage Module (ESM)

Table 10 - 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 may 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.

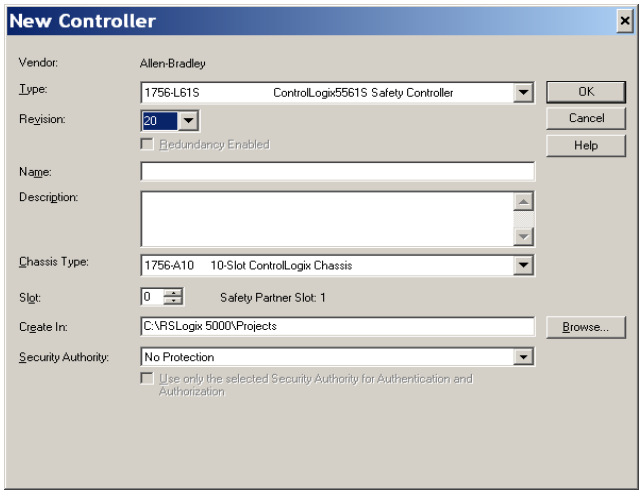
Configure the Controller

Topic	Page
Create a Controller Project	47
Set Passwords for Safety-locking and -unlocking	49
Handling I/O Module Replacement	51
Enable Time Synchronization	51
Configure a Peer Safety Controller	52

Create a Controller Project

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

1. Create a project in RSLogix 5000 software by clicking the New button on the main toolbar.
2. From the Type pull-down menu, choose a GuardLogix controller:
   - 1756-L61S ControlLogix5561S Controller
   - 1756-L62S ControlLogix5562S Controller
   - 1756-L63S ControlLogix5563S Controller
   - 1756-L71S ControlLogix5571S Controller
   - 1756-L72S ControlLogix5572S Controller
   - 1756-L73S ControlLogix5573S Controller



3. Enter the major revision of firmware for the controller.

4. Type a name for the controller.

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

5. Select the chassis size.

6. Enter the slot number of the controller.

   The New Controller 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.

7. Specify the folder in which to store the safety controller project.

8. For RSLogix 5000, version 20 or later, choose a Security Authority option.

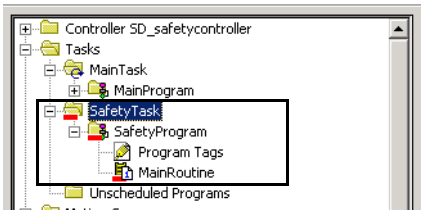
   For detailed information on security, refer to the Logix5000 Controllers Security Programming Manual, publication 1756-PM016.

9. Click OK.

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

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

Figure 7 - Safety Task in the Controller Organizer



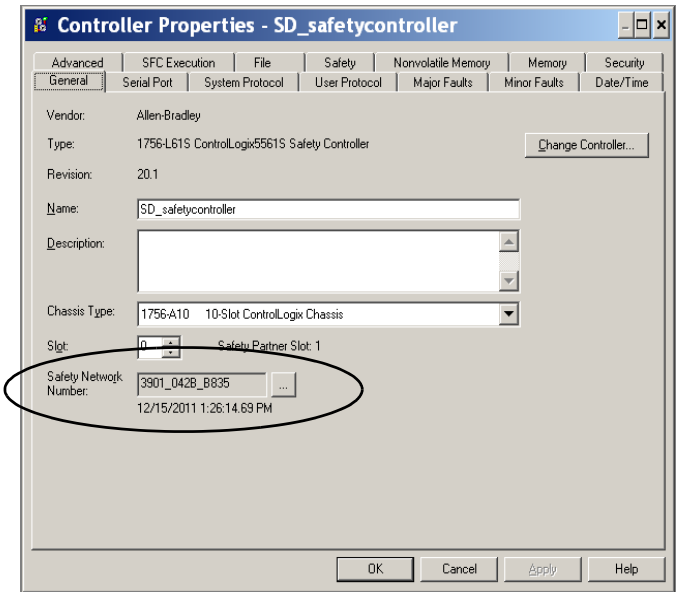
A red bar under the icon distinguishes safety programs and routines from standard project components in the RSLogix 5000 Controller Organizer.

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

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

Figure 8 - Safety Network Number



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

See Appendix C, Change Controller Type in RSLogix 5000 Projects, 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 SNN

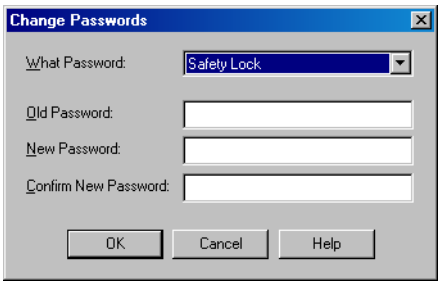
Set Passwords for Safety-locking and -unlocking

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

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

Follow these steps to set passwords.

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

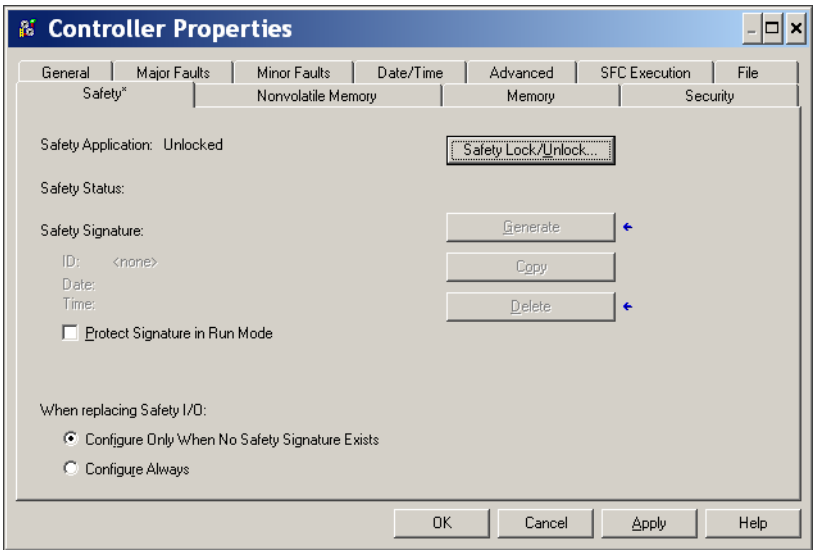


3. Type the old password, if one exists.
4. Type and confirm the new password.
5. Click OK.

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

Protecting the Safety Task Signature in Run Mode

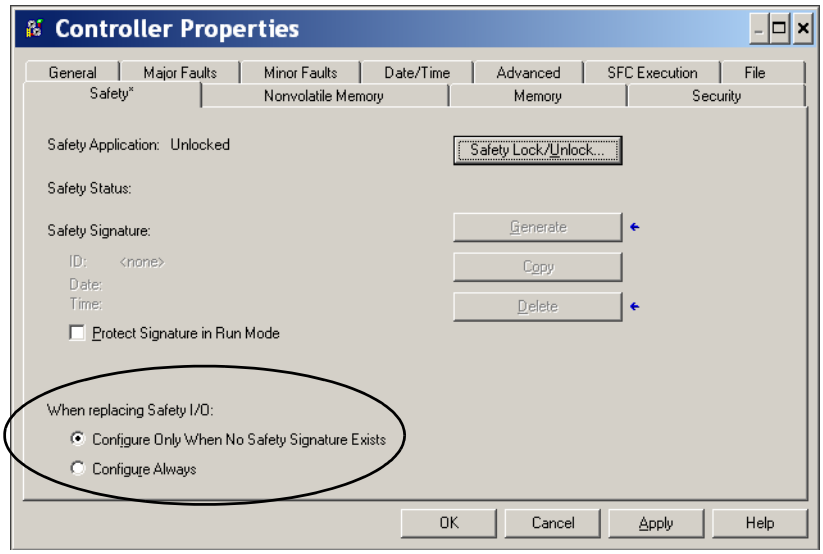
You can prevent the safety task signature from being either generated or deleted while the controller is in Run or Remote Run mode, regardless of whether the safety application is locked or unlocked, by checking Protect Signature in Run Mode on the Safety tab of the Controller Properties dialog box.



Handling I/O Module Replacement

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

Figure 9 - I/O Module Replacement Options



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

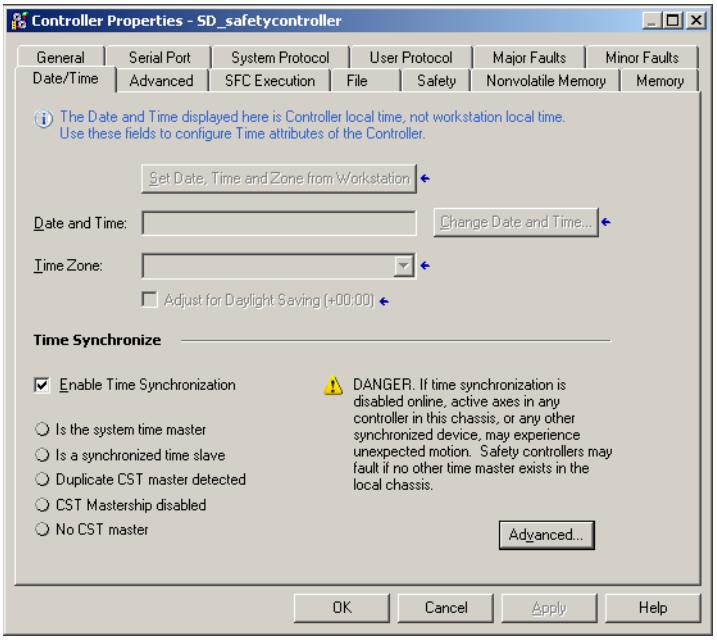
See Chapter 5, Add, Configure, Monitor, and Replace CIP Safety I/O for more information.

Enable Time Synchronization

In a GuardLogix controller system, one device in the local chassis must be designated as the coordinated system time (CST) master. To allow the controller to become the CST master, enable Time Synchronization on the Date/Time tab of the Controller Properties dialog box. Time Synchronization provides a standard mechanism to synchronize clocks across a network of distributed devices.

(1) The safety task signature is a number used to uniquely identify each project's logic, data, and configuration, thereby protecting the system's safety integrity level (SIL). See Safety Task Signature on page 16 and Generate a Safety Task Signature on page 106 for more information.

Figure 10 - 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 97.

Communicate over Networks

Topic	Page
The Safety Network	53
EtherNet/IP Communication	59
ControlNet Communication	63
DeviceNet Communication	65
Serial Communication	67
Additional Resources	68

The Safety Network

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

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

Managing the Safety Network Number (SNN)

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

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

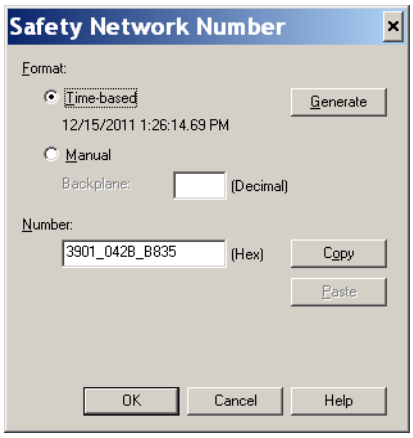
TIP Multiple safety network numbers can be assigned to a CIP Safety subnet or a ControlBus chassis that contains more than one safety device. **However, for simplicity, we recommend that each CIP Safety subnet have one, and only one, unique SNN.**

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

Time-based Safety Network Number

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

Figure 11 - Time-based Format



Manual Safety Network Number

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

Figure 12 - Manual Entry



Assigning the Safety Network Number (SNN)

You can allow RSLogix 5000 software to automatically assign an SNN, or you can assign the SNN manually.

Automatic Assignment

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

Manual Assignment

The manual option is intended for routable CIP Safety systems where the number of network subnets and interconnecting networks is small, and where users might like to manage and assign the SNN in a logical manner pertaining to their specific application.

See Changing the Safety Network Number (SNN) on page 55.

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

Automatic Versus Manual

For typical users, the automatic assignment of an SNN is sufficient. However, manual manipulation of the SNN is required if the following is true:

- Safety consumed tags are used.
- The project consumes safety input data from a module whose configuration is owned by some other device.
- A safety project is copied to another hardware installation within the same routable CIP Safety system.

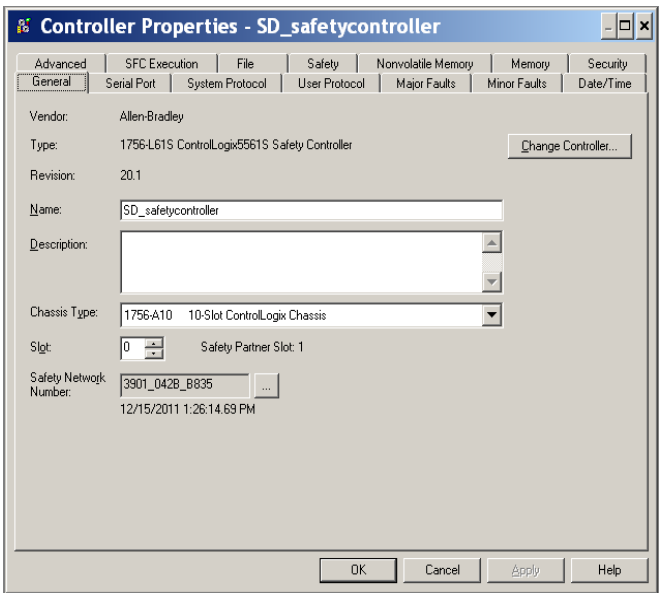
Changing the Safety Network Number (SNN)

Before changing the SNN you must do the following:

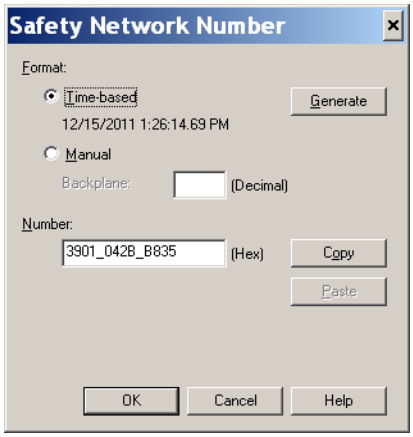
- Unlock the project, if it is safety-locked.
  See Safety-lock the Controller on page 105.
- Delete the safety task signature, if one exists.
  See Delete the Safety Task Signature on page 108.

Change the Safety Network Number (SNN) of the Controller

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



3. Click Time-based and then Generate.



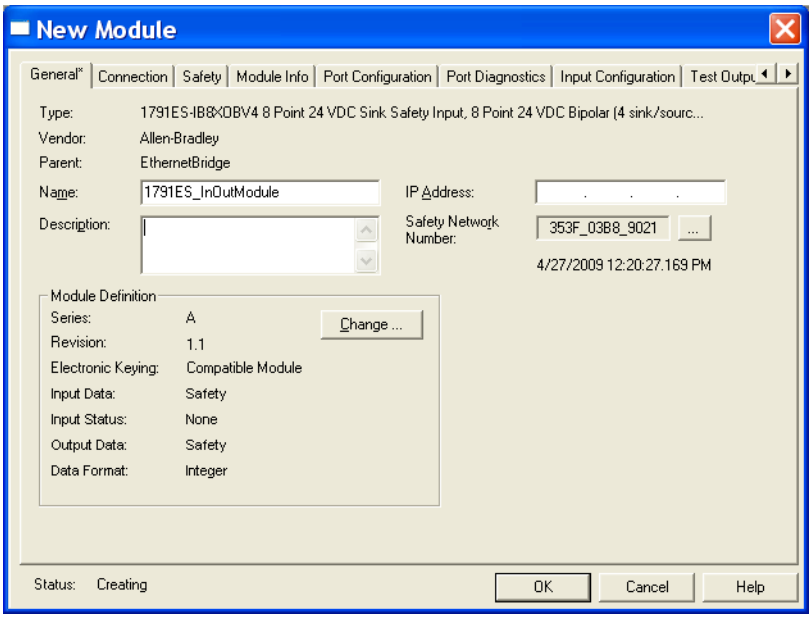
4. Click OK.

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

This example uses an EtherNet/IP network.

1. Find the first EtherNet/IP communication module in the I/O Configuration tree.

2. Expand the safety I/O modules available through the EtherNet/IP communication module.
3. Double-click the first safety I/O module to view the General tab.

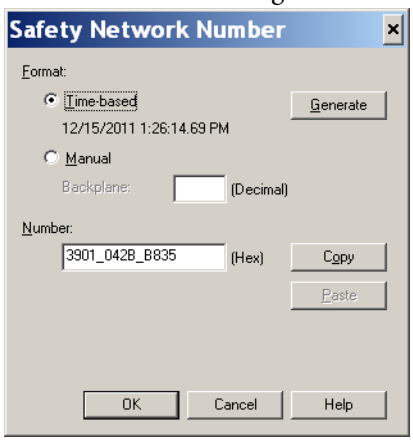


4. Click ... to the right of the safety network number to open the Safety Network Number dialog box.
5. Choose Time-based and click Generate to generate a new SNN for that EtherNet/IP network.
6. Click OK.
7. Click Copy to copy the new SNN to the Windows Clipboard.
8. Open the General Tab of the Module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

Copy and Paste a Safety Network Number (SNN)

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

1. In the software configuration tool of the module's configuration owner, open the Safety Network Number dialog box for the module.



2. Click Copy.
3. Click the General tab on the Module Properties dialog box of the I/O module in the I/O Configuration tree of the consuming controller project. This consuming controller is not the configuration owner.
4. Click ... to the right of the safety network number to open the Safety Network Number dialog box.
5. Click Paste.
6. Click OK.

EtherNet/IP Communication

For EtherNet/IP network communication in a GuardLogix system, you have several modules to choose from. For CIP Safety communication, including Safety I/O module control, choose any of the modules shown in Table 12, except the 1756-EWEB module, which 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 modules (requires an adapter for distributed I/O). • Communicate with other EtherNet/IP devices (messages). • Serve as a pathway for data sharing between Logix5000 controllers (produce/consume). • 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. • Provide a temporary configuration connection via the USB port. • Configure IP addresses quickly by using rotary switches.
1756-EN2F	• Perform the same functions as a 1756-EN2T module. • Connect fiber media by an LC fiber connector on the module.
1756-EN2TXT	• Perform the same functions as a 1756-EN2T module. • Operate in extreme environments with -25…70 °C (-13…158 °F) temperatures.
1756-EN2TR	• Perform the same functions as a 1756-EN2T module. • Support communication on a ring topology for a Device Level Ring (DLR) single-fault tolerant ring network.
1756-EN3TR	• Perform the same functions as the 1756-EN2TR module. • Three ports for DLR connection.
1756-EWEB	• Provide customizable web pages for external access to controller information. • Provide remote access via an Internet browser to tags in a local ControlLogix controller. • Communicate with other EtherNet/IP devices (messages). • Bridge EtherNet/IP nodes to route messages to devices on other networks. • Support Ethernet devices that are not EtherNet/IP-based with a socket interface. 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 software products are available for EtherNet/IP networks.

Table 13 - Software for EtherNet/IP Modules

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

Producing and Consuming Data via an EtherNet/IP Network

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

Connections over the EtherNet/IP Network

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

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

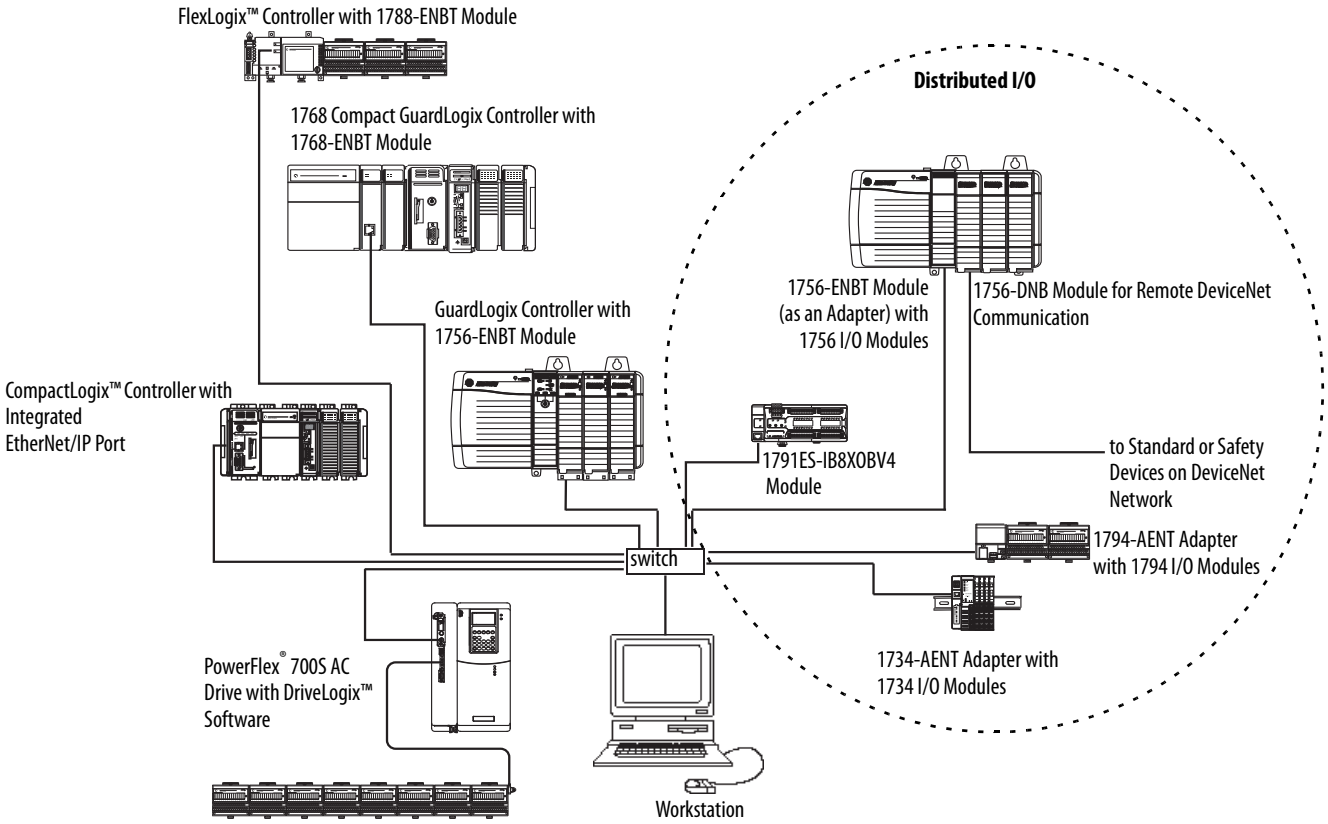
The EtherNet/IP communication modules support 128 Common Industrial Protocol (CIP) connections over an EtherNet/IP network.

EtherNet/IP Communication Example

This example illustrates the following:

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

Figure 13 - EtherNet/IP Communication Example

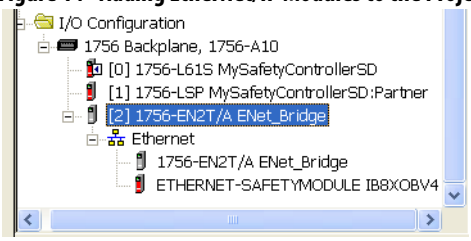


EtherNet/IP Connections for CIP Safety I/O Modules

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

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

Figure 14 - Adding EtherNet/IP Modules to the Project



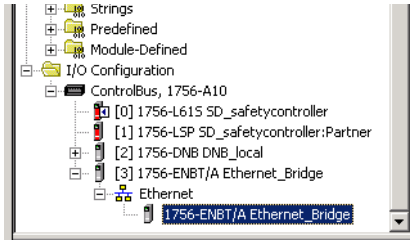
Standard EtherNet/IP Connections

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: • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223…255.*xxx.xxx.xxx*
Subnet Mask	Subnet addressing is an extension of the IP address scheme that allows a site to use one network ID for multiple physical networks. Routing outside of the site continues by dividing the IP address into a net ID and a host ID via the class. Inside a site, the subnet mask is used to redivide the IP address into a custom network ID portion and host ID portion. This field is set to 0.0.0.0 by default. If you change the subnet mask of an already-configured module, you must cycle power for the change to take effect.
Gateway	A gateway connects individual physical networks into a system of networks. When a node needs to communicate with a node on another network, a gateway transfers the data between the two networks. This field is set to 0.0.0.0 by default.

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



3. Use RSLogix 5000 software 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 modules • Requires an adapter for distributed I/O on ControlNet links • Communicates with other ControlNet devices (messages) • Shares standard data with other Logix5000 controllers (produce/consume) • Bridges ControlNet links to route messages to devices on other networks	1756-CNB
• Performs same functions as a 1756-CNB module • Also supports redundant ControlNet media	1756-CNBR
• Performs the same functions supported by the 1756-CNB module with higher performance • Supports CIP Safety communication	1756-CN2
• Performs same functions as a 1756-CN2 module • Also supports redundant ControlNet media	1756-CN2R
• Perform the same functions as a 1756-CN2R module • Operate in extreme environments with -25…70 °C (-13…158 °F) temperatures	1756-CN2RXT

These software products are available for ControlNet networks.

Table 15 - Software for ControlNet Modules

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

The ControlNet communication modules provide the following:

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

Producing and Consuming Data via a ControlNet Network

The 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 (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, which is the requested packet interval (RPI). For example, a connection to an I/O module is a scheduled connection because you repeatedly receive data from the module at a specified interval. Other scheduled connections include connections to the following: • Communication devices • Produced/consumed tags 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 a MSG instruction). Unscheduled messaging lets you send and receive data when needed. Unscheduled connections use the remainder of network bandwidth after scheduled connections are allocated. 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.

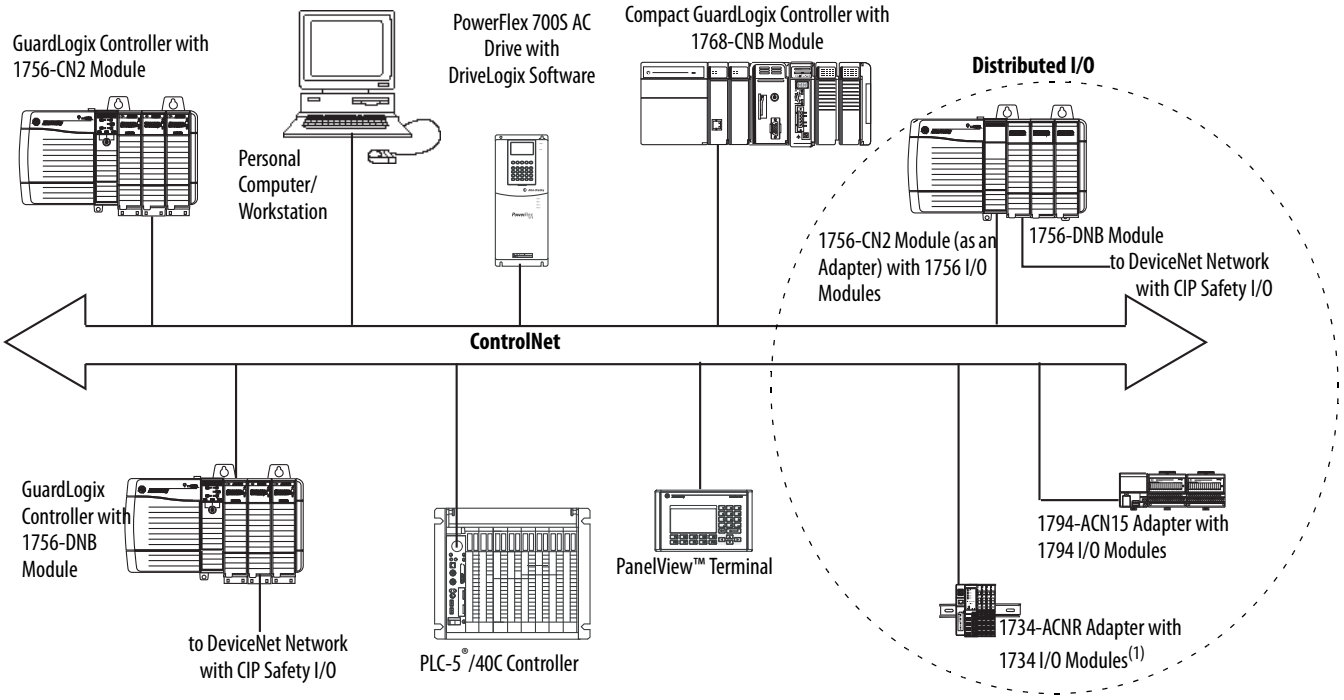
ControlNet Communication Example

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 15 - 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 modules over a ControlNet network, add a ControlNet bridge, a ControlNet adapter, and I/O modules to the controller's I/O Configuration folder.

DeviceNet Communication

To communicate and exchange data with CIP Safety I/O modules 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 software products are used with the DeviceNet networks and 1756-DNB module.

Table 17 - Software for Use with DeviceNet Networks

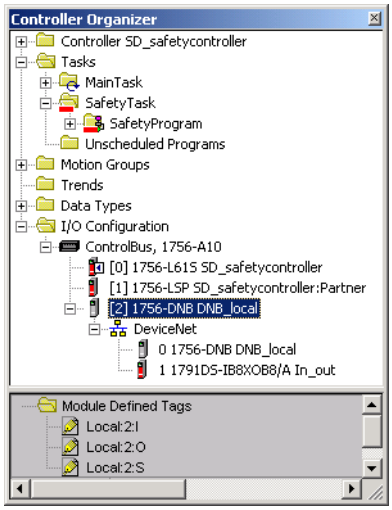
Software	Is used to	Required/Optional
RSLogix 5000	• Configure ControlLogix projects. • Define DeviceNet communication.	Required
RSNetWorx™ for DeviceNet	• Configure DeviceNet devices. • Define the scan list for those devices.	
RSLinx Classic or RSLinx Enterprise	• Configure communication devices. • Provide diagnostics. • Establish communication between devices.	

DeviceNet Connections for CIP Safety I/O Modules

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

CIP Safety I/O modules 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. When you add a CIP Safety I/O module, RSLogix 5000 software automatically creates controller-scoped safety data tags for that module.

Figure 16 - 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, RSLogix 5000 software automatically creates a set of standard tags for the input, output, and status data of the network.

Serial Communication

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

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

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

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

Table 18 - Serial Communication Modes

Use this mode	For
DF1 Point-to-point	Communication between the controller and one other DF1-protocol-compatible device. This is the default System mode. This mode is typically used to program the controller through its serial port.
DF1 Master	Control of polling and message transmission between the master and slave nodes. The master/slave network includes one controller configured as the master node and as many as 254 slave nodes. Link slave nodes by using modems or line drivers. A master/slave network can have node numbers from 0…254. Each node must have a unique node address. Also, at least 2 nodes must exist to define your link as a network (1 master and 1 slave station are the two nodes).
DF1 Slave	A controller operating as a slave station in a master/slave serial communication network. When there are multiple slave stations on the network, link slave stations by using modems or line drivers to the master. When you have a single slave station on the network, you do not need a modem to connect the slave station to the master. You can configure the control parameters for no handshaking. You can connect 2…255 nodes to one link. In DF1 Slave mode, a controller uses DF1 half-duplex protocol. One node is designated as the master and it controls who has access to the link. All the other nodes are slave stations and must wait for permission from the master before transmitting.
DH-485	Communicating with other DH-485 devices multi-master, token passing network allowing programming and peer-to-peer messaging.

Additional Resources

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

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

Topic	Page
Adding CIP Safety I/O Modules	69
Configure CIP Safety I/O Modules via RSLogix 5000 Software	70
Setting the Safety Network Number (SNN)	71
Using Unicast Connections on EtherNet/IP Networks	71
Setting the Connection Reaction Time Limit	71
Understanding the Configuration Signature	75
Reset Safety I/O Module Ownership	76
Addressing Safety I/O Data	76
Monitor Safety I/O Module Status	77
Resetting a Module to Out-of-box Condition	79
Replacing a Module by Using RSLogix 5000 Software	79
Replacing a POINT Guard I/O Module By Using RSNetWorx for DeviceNet Software	86

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

- Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001
- Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001
- POINT Guard I/O™ Safety Modules Installation and User Manual, publication 1734-UM013
- RSLogix 5000 software online help

Adding CIP Safety I/O Modules

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

- Node address for DeviceNet networks

  You cannot set the node address of an CIP Safety I/O module on DeviceNet networks via RSLogix 5000 software. Module node addresses are set via rotary switches on the modules.

- IP address for EtherNet/IP networks

  To set the IP address, you can adjust the rotary switches on the module, use DHCP software, available from Rockwell Automation, or retrieve the default address from nonvolatile memory.

- Safety network number (SNN)

  See page 71 for information on setting the SNN.

- Configuration signature

  See page 75 for information on when the configuration signature is set automatically and when you need to set it.

- Reaction time limit

  See page 71 for information on setting the reaction time limit.

- Safety input, output, and test parameters

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

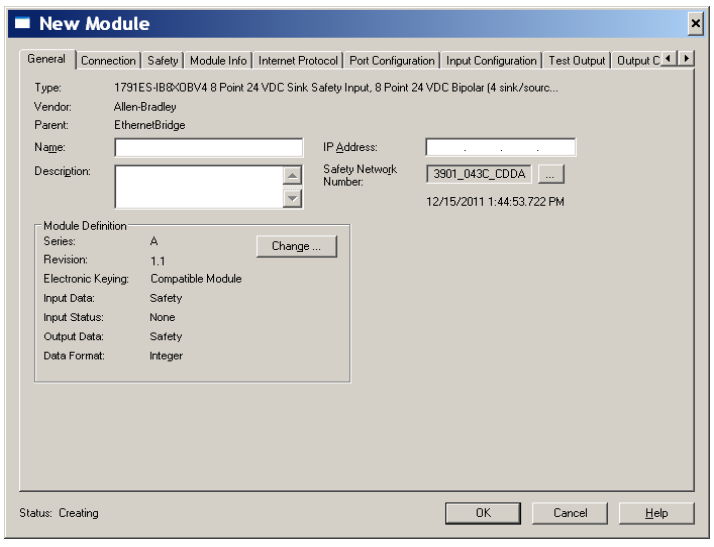
TIP Safety I/O modules support standard and safety data. Module configuration defines what data is available.

Configure CIP Safety I/O Modules via RSLogix 5000 Software

Add the CIP Safety I/O module to the communication module under the I/O Configuration folder of the RSLogix 5000 project.

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

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



   a. Modify the Module Definition settings, if required, by clicking Change.

b. Type a name for the new module.

c. Enter the node address or IP address of the module on its connecting network.

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

d. Modify the safety network number (SNN), if required, by clicking the ... button.

   See page 71 for details.

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

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

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

   See page 71 for details.

Setting the Safety Network Number (SNN)

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

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

See Assigning the Safety Network Number (SNN) on page 55.

Using Unicast Connections on EtherNet/IP Networks

In RSLogix 5000 software, version 20 or later, you can configure EtherNet/IP I/O modules to use unicast connections. Unicast connections are point-to-point connections between a source and a destination node. You do not have to enter a minimum or maximum RPI range or default value for this type of connection.

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

Setting the Connection Reaction Time Limit

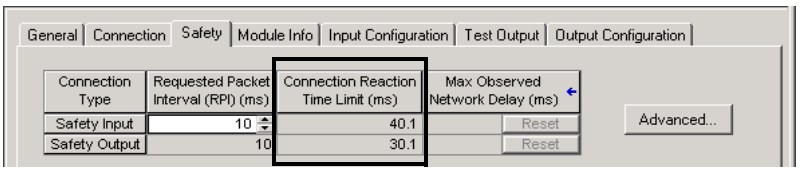
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. The Connection Reaction Time Limit is determined by the following equations:

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 17 - Connection Reaction Time Limit



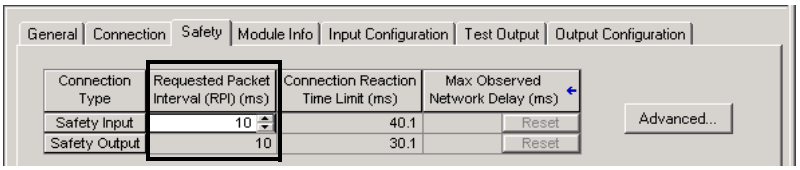
Specify the Requested Packet Interval (RPI)

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

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

The Connection Reaction Time Limit is adjusted immediately when the RPI is changed via RSLogix 5000 software.

Figure 18 - 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 90 for more information on the safety task period.

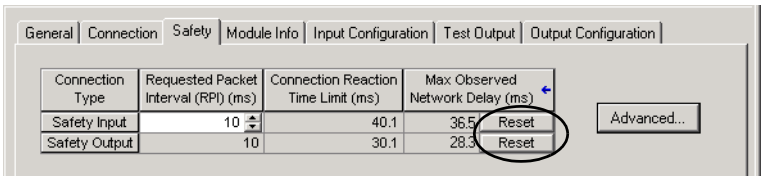
For typical applications, the default RPI is usually sufficient. For more complex requirements, use the Advanced button to modify the Connection Reaction Time Limit parameters, as described on page 73.

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

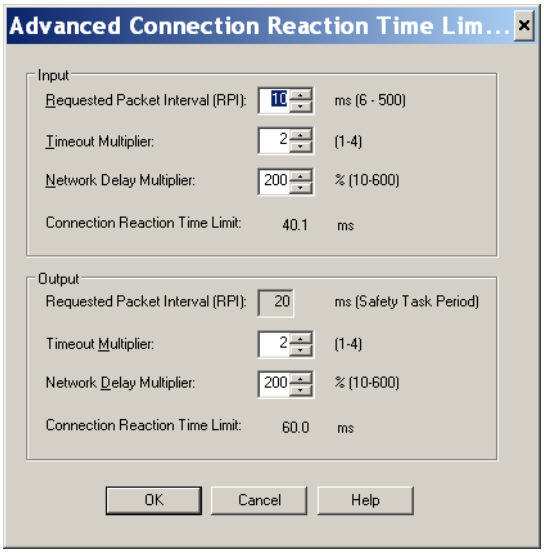
Figure 19 - Resetting the Max Observed Network Delay



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

Setting the Advanced Connection Reaction Time Limit Parameters

Figure 20 - Advanced Configuration



Timeout Multiplier

The Timeout Multiplier determines the number of RPIs to wait for a packet before declaring a connection timeout. This translates into the number of messages that may be lost before a connection error is declared.

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

Network Delay Multiplier

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

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

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

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

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

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

EXAMPLE	**Calculate the Approximate Output Network Delay Multiplier**
	If:
	Input RPI = 10 ms Input Network Delay Multiplier = 200% Safety Task Period = 20 ms
	Then, the Output Network Delay Multiplier equals:
	200% 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 19 - Additional Resources

Resource	Description
GuardLogix Controllers Systems Safety Reference Manual, publication 1756-RM093	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	

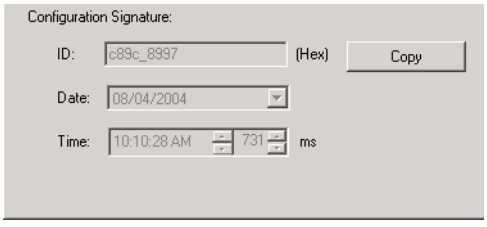
Understanding the Configuration Signature

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

Configuration via RSLogix 5000 Software

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

Figure 21 - View and Copy the Configuration Signature



Different Configuration Owner (listen only connection)

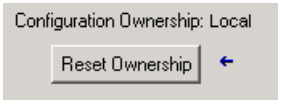
When the I/O module configuration is owned by another controller, you need to copy the module configuration signature from its owner's project and paste it into the Safety tab of the Module Properties dialog box.

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

Reset Safety I/O Module Ownership

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

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



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

Addressing Safety I/O Data

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

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

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

Modulename:Type.Member

Table 20 - CIP Safety I/O Module Address Format

Where	Is	
Modulename	The name of the CIP Safety I/O module	
Type	Type of data	
	Input: I	
	Output: O	
Member	Specific data from the I/O module	
	Input-only Module:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Output-only Module:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	Combination I/O:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Table 21 - Additional 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 modules

Monitor Safety I/O Module Status

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

These publications provide information on I/O module troubleshooting:

- Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001
- Guard I/O EtherNet/IP Modules User Manual, publication 1791ES-UM001
- POINT Guard I/O Safety Modules Installation and User Manual, publication 1734-UM013

Table 22 - Status Indicator Operation

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.	
Network Status (NS)	Off	Device is not online or may not have power.		
	Green, On	Device is online; connections are established.		
	Green, Flashing	Device is online; no connections established.		
	Red, Flashing	Communication timeout.	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.	RSLogix 5000 software 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 by RSLogix 5000 software.		
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.

Resetting a Module to Out-of-box Condition

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

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

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

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

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

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



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

Replacing a Module by Using RSLogix 5000 Software

You can use RSLogix 5000 software to replace a Guard I/O module on an Ethernet network. To replace a Guard I/O module on a DeviceNet network, your choice of software depends on the type of module.

Table 23 - Software

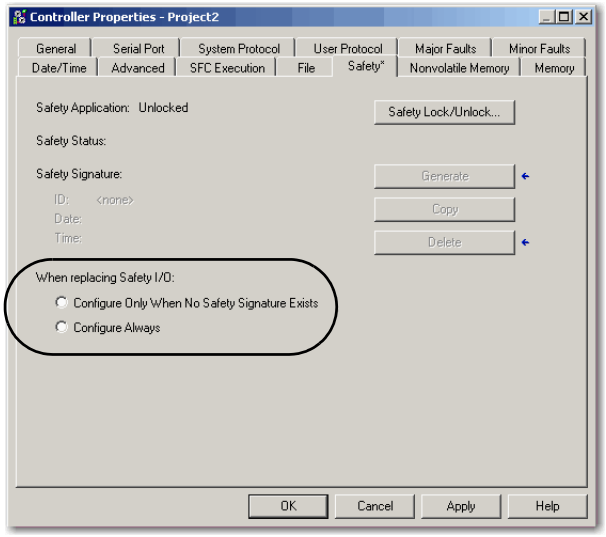
If you are using a	Use	See
1791DS Guard I/O module with 1756-DNB adapter	RSLogix 5000 software	below
1734 POINT Guard I/O module with a 1734-PDN adapter	RSNetWorx for DeviceNet software	Replacing a POINT Guard I/O Module By Using RSNetWorx for DeviceNet Software on page 86

If you are relying on a portion of the CIP Safety system to maintain SIL 3 behavior during module replacement and functional testing, the Configure Always feature may not be used. Go to Replacement with 'Configure Only When No Safety Signature Exists' Enabled on page 80.

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 module, the Configure Always feature may be used. Go to Replacement with 'Configure Always' Enabled on page 84.

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

Figure 22 - Safety I/O Module Replacement



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

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

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

Table 24 - Replacing a Module

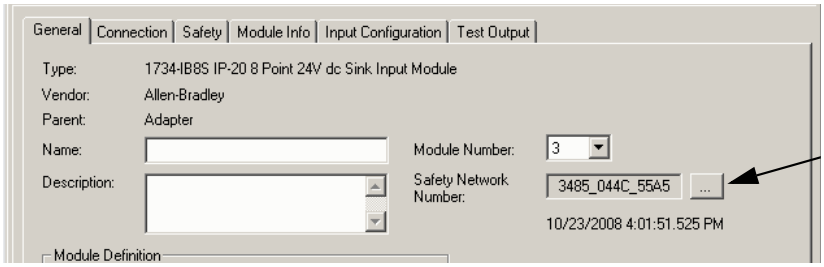
GuardLogix Safety Signature Exists	Replacement Module Condition	Action Required
No	No SNN (Out-of-box)	None. The module is ready for use.
Yes or No	Same SNN as original safety task configuration	None. The module is ready for use.

Table 24 - Replacing a Module

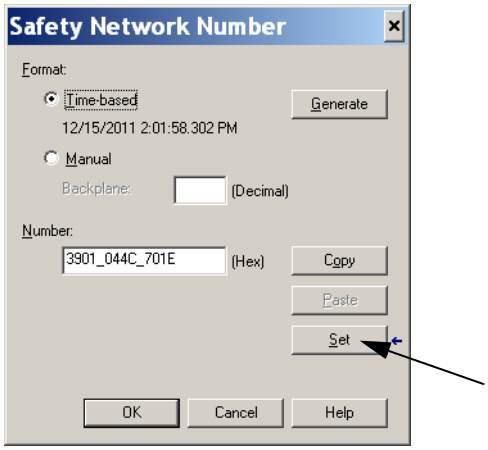
GuardLogix Safety Signature Exists	Replacement Module Condition	Action Required
Yes	No SNN (Out-of-box)	See Scenario 1 - Replacement Module is Out-of-box and Safety Signature Exists on page 81.
Yes	Different SNN from original safety task configuration	See Scenario 2 - Replacement Module SNN is Different from Original and Safety Signature Exists on page 82.
No		See Scenario 3 - Replacement Module SNN is Different from Original and No Safety Signature Exists on page 84.

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

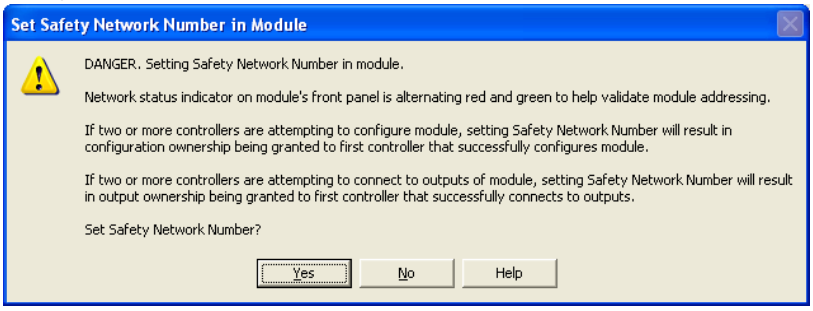
1. Remove the old I/O module and install the new module.
2. Right-click the replacement POINT Guard I/O module and choose Properties.
3. Click ... to the right of the safety network number to open the Safety Network Number dialog box.



4. Click Set.



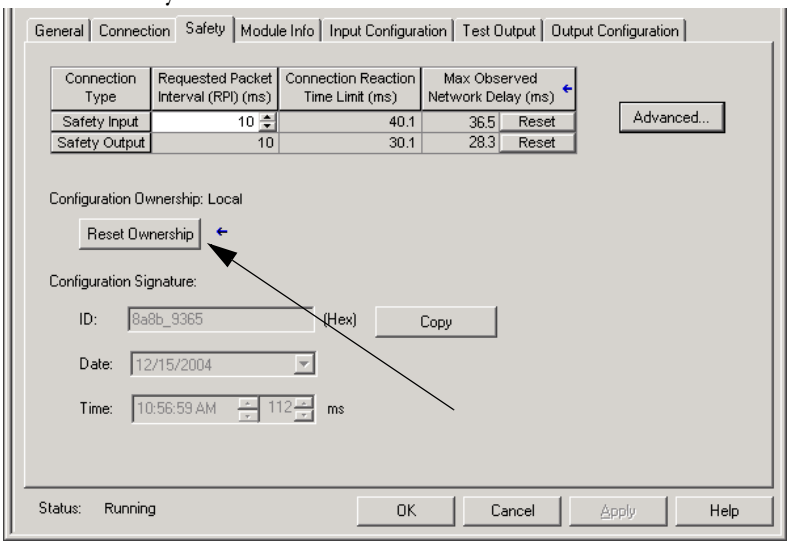
5. Verify that the Network Status (NS) status indicator is alternating red/green on the correct module before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement module.



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

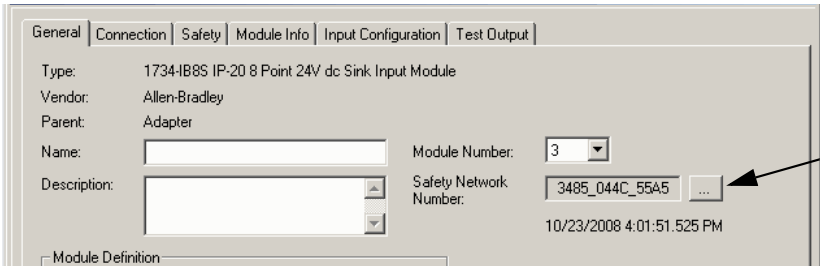
Scenario 2 - Replacement Module SNN is Different from Original and Safety Signature Exists

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

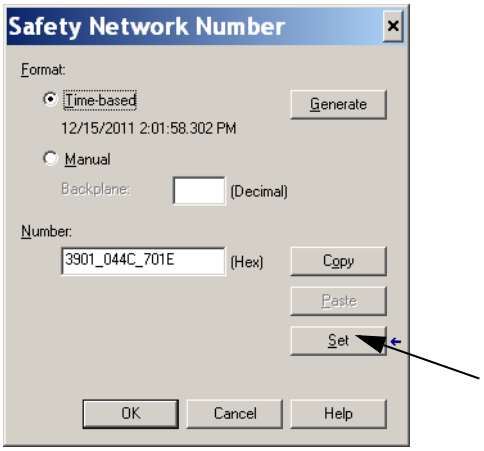


4. Click Reset Ownership.
5. Click OK.
6. Right-click your controller and choose Properties.

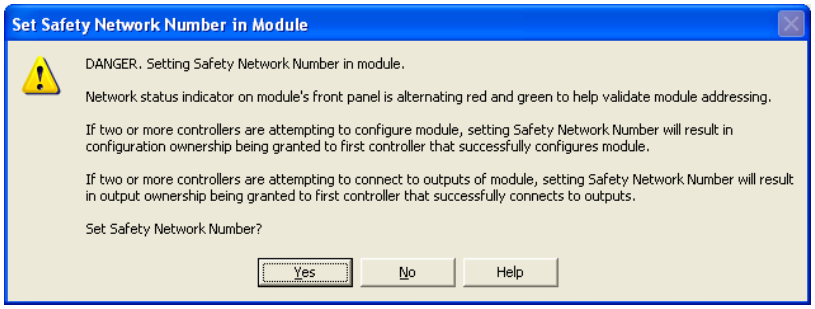
7. Click ... to the right of the safety network number to open the Safety Network Number dialog box.



8. Click Set.



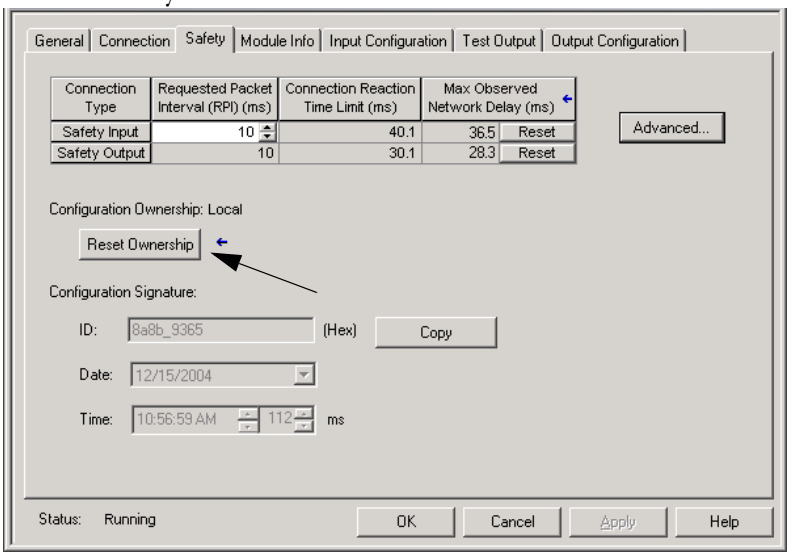
9. Verify that the Network Status (NS) status indicator is alternating red/green on the correct module before clicking Yes on the confirmation dialog box to set the SNN and accept the replacement module.



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

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

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



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

Replacement with 'Configure Always' Enabled

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

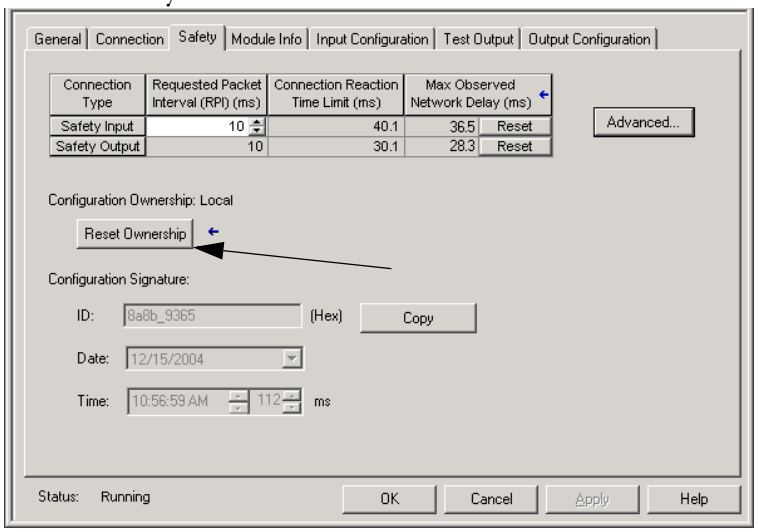
Do not place modules that are in the out-of-box condition on a CIP Safety network when the Configure Always feature is enabled, except while following this replacement procedure.

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

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

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

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



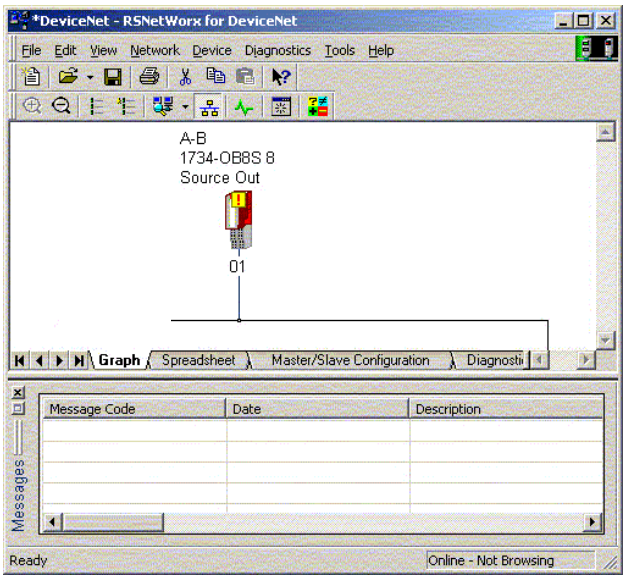
4. Click Reset Ownership.
5. Click OK.
6. Follow your company-prescribed procedures to functionally test the replaced I/O module and system and to authorize the system for use.

Replacing a POINT Guard I/O Module By Using RSNetWorx for DeviceNet Software

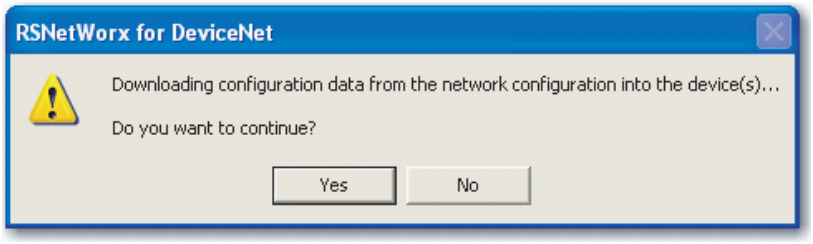
Follow these steps to replace a POINT Guard I/O module when the module and the controller are on a DeviceNet network.

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

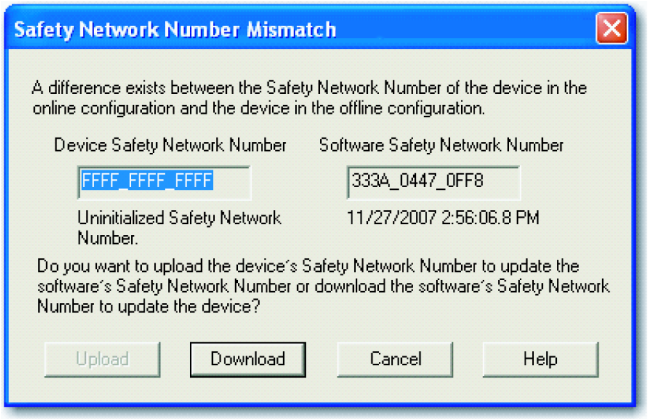
   If the replacement module is out-of-box or has an SNN that does not match the original module, the module appears with an exclamation mark.



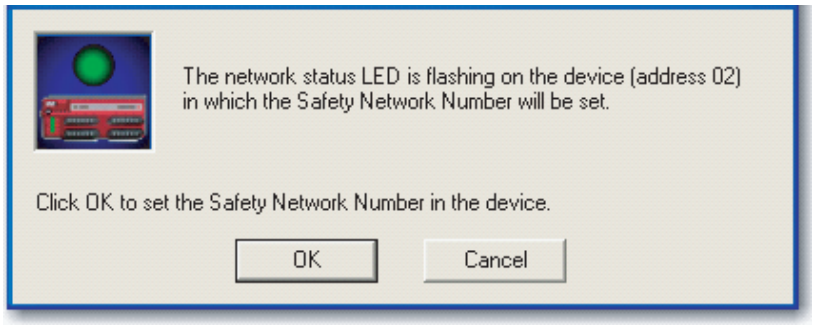
3. Right-click the module and choose Download to Device.



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



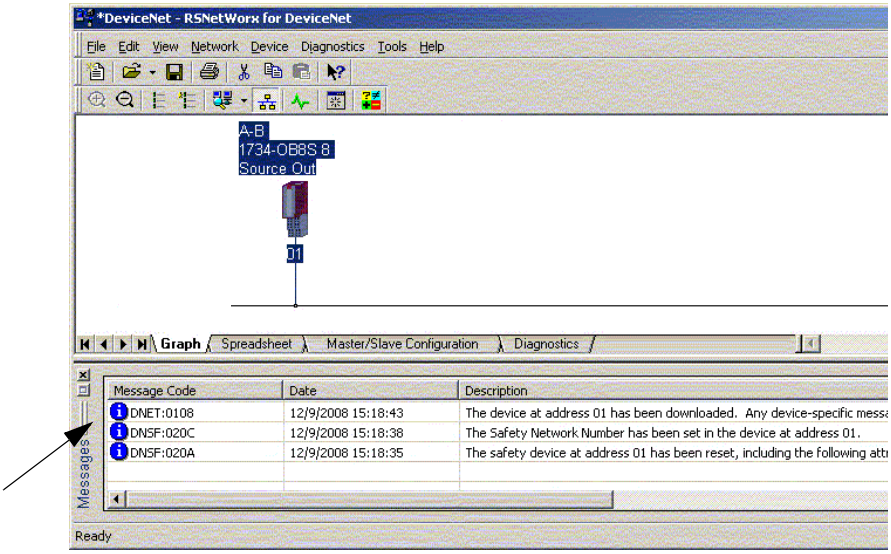
6. Verify that the (NS) Network Status indicator is flashing on the correct module and click OK to set the SNN on that device.



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



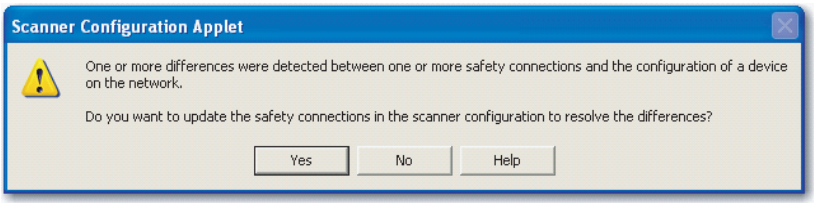
Once the download is completes successfully, the main project view displays this message: 'The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.'



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.

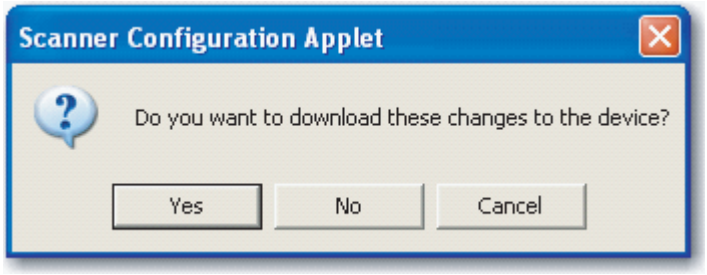
If you download this configuration to a temporary setup, place the module on the network and it automatically connects to the controller.

If the configuration downloaded to the module was not from the original DNT file, the configuration signature will not match the original. Even if you recreate the same parameters in a new DNT file, the time and date portions of the signature will be 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, you should 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 SmartGuard 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.

Develop Safety Applications

Topic	Page
The Safety Task	90
Safety Programs	92
Safety Routines	92
Safety Tags	92
Produced/Consumed Safety Tags	97
Safety Tag Mapping	102
Safety Application Protection	105
Software Restrictions	108

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

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

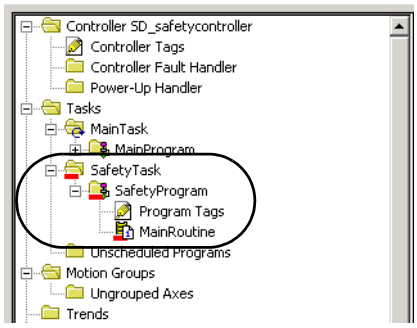
The Safety Reference Manual addresses the following:

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

The Safety Task

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

Figure 23 - Safety Task in the Controller Organizer



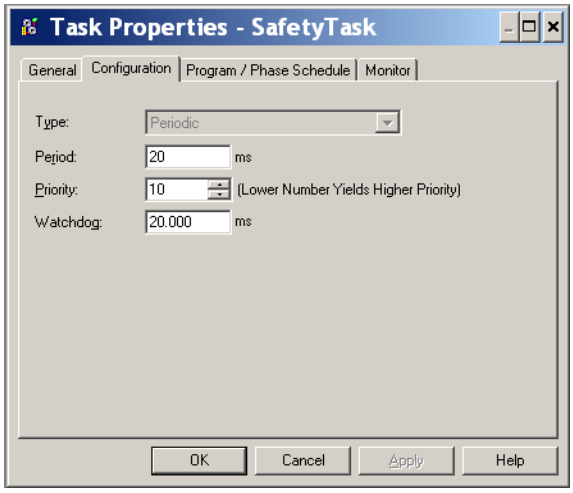
Within the safety task, you can use multiple safety programs, composed of multiple safety routines. The GuardLogix controller supports one safety task. The safety task cannot be deleted.

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

Figure 24 - Configuring the Safety Task Period



The safety task should be a high priority. You specify the safety task period (in ms) and the safety task watchdog (in ms). The safety task period is the period at which the safety task executes. The safety task watchdog is the maximum time allowed from the start of safety task execution to its completion.

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

The safety task period directly affects system reaction time.

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

Safety Task Execution

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

- The safety task does not begin executing until the primary controller and 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 102 for information on safety tag mapping.

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

Safety Programs

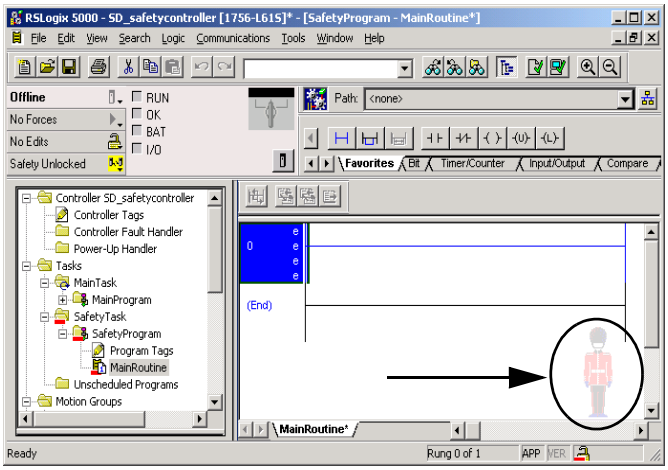
Safety programs have all the attributes of standard programs, except that they can only be scheduled in the safety task and can only contain safety components. Safety programs can only contain safety routines, one of which must be designated as the main routine, and one of which may be designated as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

Safety programs cannot contain standard routines or standard tags.

Safety Routines

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

TIP RSLogix 5000 software uses a watermark feature to visually distinguish a safety routine from a standard routine.



Safety Tags

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

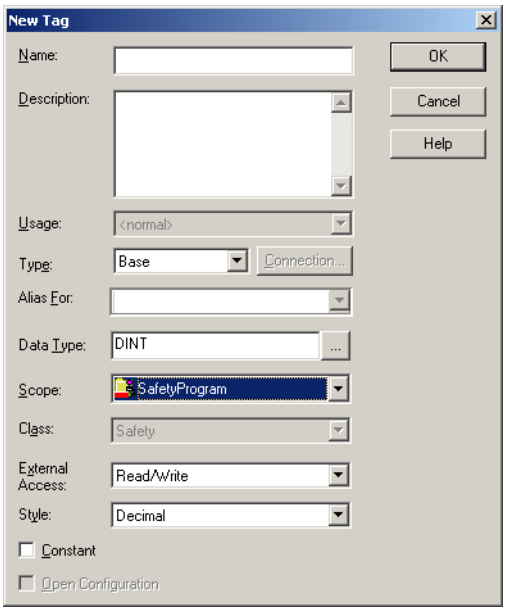
When you create a tag, you assign the following properties:

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

You can also specify if the tag value should be a constant.

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

Figure 25 - Creating a New Tag



Tag Type

Table 25 defines the four types of tags: base, alias, produced, and consumed.

Table 25 - Four Tag Types

Tag Type	Description
Base	These tags store values for use by logic within the project.
Alias	A tag that references another tag. An alias tag can refer to another alias tag or a base tag. An alias tag can also refer to a component of another tag by referencing a member of a structure, an array element, or a bit within a tag or member. **IMPORTANT:** Aliasing between standard and safety tags is prohibited in safety applications. Instead, standard tags can be mapped to safety tags using safety tag mapping. See Safety Tag Mapping on page 102.
Produced	A tag that a controller makes available for use by other controllers. A maximum of 15 controllers can simultaneously consume (receive) the data. A produced tag sends its data to one or more consuming tags without using logic. Produced tag data is sent at the RPI of the consuming tag.
Consumed	A tag that receives the data of a produced tag. The data type of the consumed tag must match the data type of the produced tag. The requested packet interval (RPI) of the consumed tag determines the period at which the data updates.

Data Type

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

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

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

Only these data types are permitted for safety tags.

Table 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

REAL data types are valid in 1756-L7*x*S controller projects, but are not valid in 1756-L6*x*S or 1768-L4*x*S controller projects.

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

Scope

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

Controller-scoped Tags

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

- More than one program in the project
- To produce or consume data
- To communicate with a PanelView/HMI terminal
- In safety tag mapping
  See Safety Tag Mapping on page 102 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 127	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.

RSLogix 5000 software can modify constant standard tags, and safety tags provided a safety task signature is not present. Safety tags cannot be modified if a safety task signature is present.

External Access

External Access defines the level of access that is allowed for external devices, such as an HMI, to see or modify tag values. Access via RSLogix 5000 software is not affected by this setting. The default value is read/write.

Table 28 - External Access Levels

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

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

Produced/Consumed Safety Tags

To transfer safety data between GuardLogix controllers, you use produced and consumed safety tags. Produced and consumed tags require connections. The default connection type for produced and consumed tags is unicast in version 19 and later of RSLogix 5000 software.

Table 29 - Produced and Consumed Connections

Tag	Connection Description
Produced	A GuardLogix controller can produce (send) safety tags to other 1756 or 1768 GuardLogix controllers. The producing controller uses a single connection for each consumer.
Consumed	GuardLogix controllers can consume (receive) safety tags from other 1756 or 1768 GuardLogix controllers. Each consumed tag consumes one connection.

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

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

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

Configure the Peer Safety Controllers' Safety Network Numbers

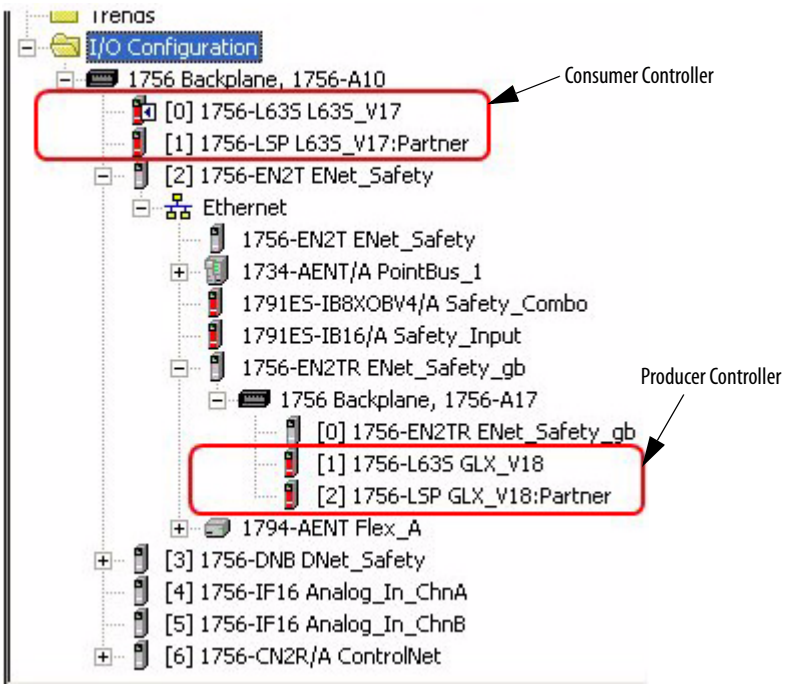
The peer safety controller is subject to the same configuration requirements as the local safety controller. The peer safety controller must also have a safety network number (SNN). The SNN of the peer safety controller depends upon its placement in the system.

Table 30 - SNN and Controller Placement

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

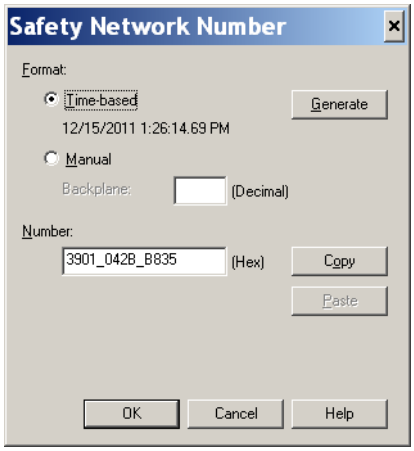
Follow these steps to copy and paste the SNN.

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



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

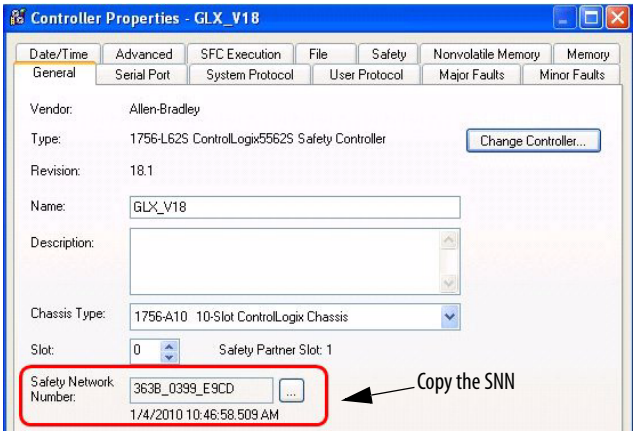
TIP An SNN can be copied and pasted by using the buttons on the Safety Network Number dialog box. Open the respective Safety Network Number dialog boxes by clicking ... to the right of the SNN fields in the properties dialog boxes.



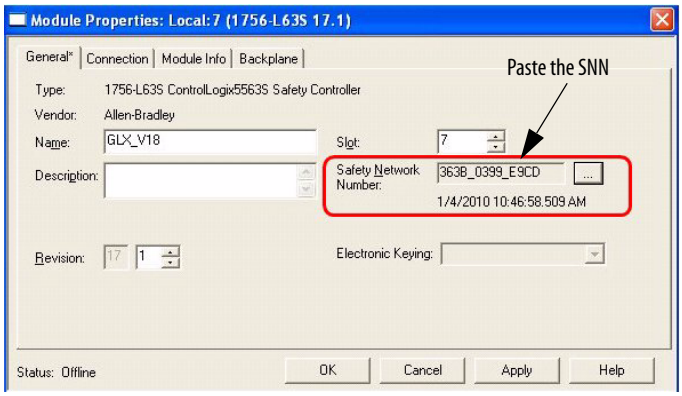
4. In the consumer controller's project, right-click the producer controller and choose Module Properties.

5. Paste the producer controller's SNN into the SNN field.

Producer Controller Properties Dialog Box in Producer Project



Module Properties Dialog Box in Consumer Project



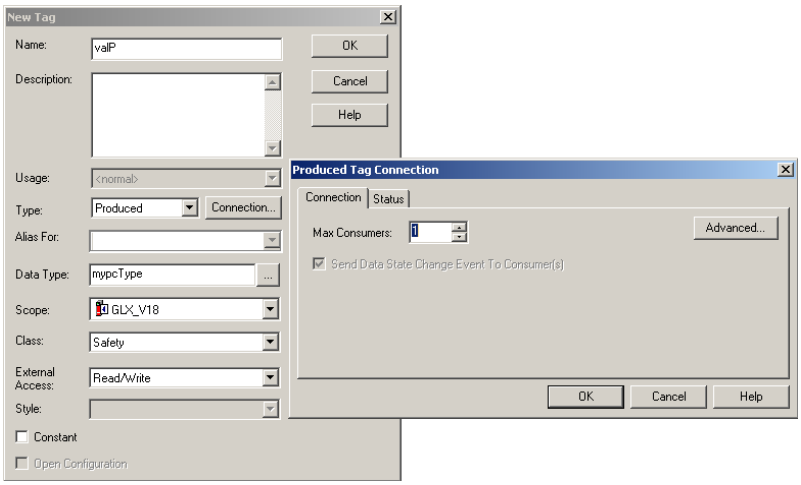
Produce a Safety Tag

Follow this procedure to produce a safety tag.

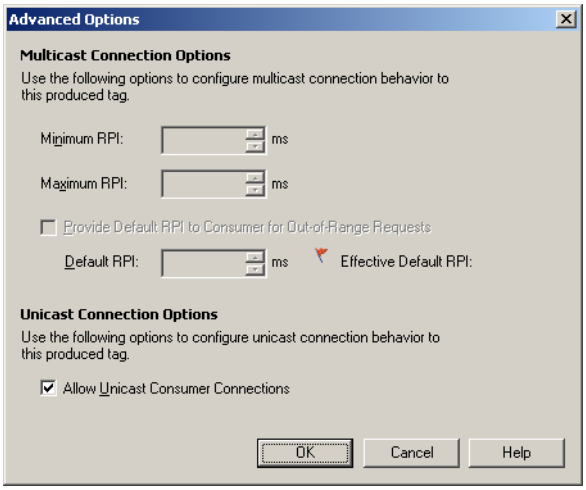
1. In the producing controllers project, create a user-defined data type defining the structure of the data to be produced.

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

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



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



6. Click OK.

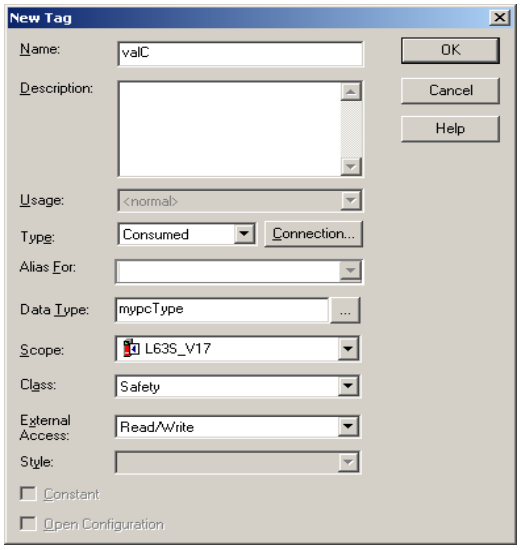
Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

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

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

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



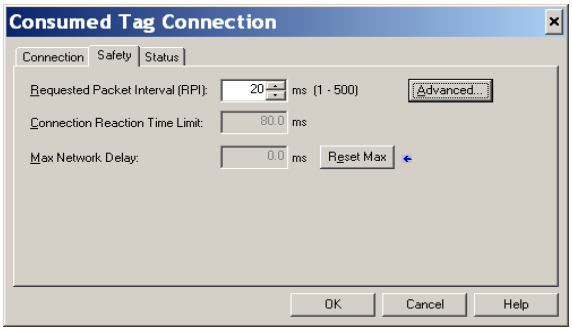
4. Click Connection to open the Consumed Tag Connection dialog box.



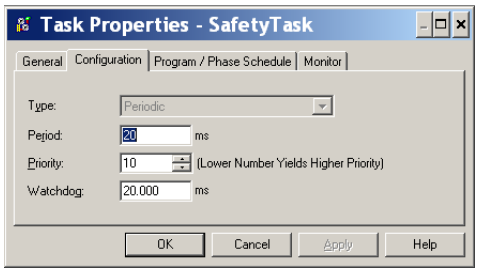
5. Select the controller that produces the data.
6. Enter the name of the produced tag.
7. Click the Safety tab.
8. Enter the requested packet interval (RPI) for the connection in 1 ms increments.

   The default is 20 ms.

Consumer's Project



Producer's Project

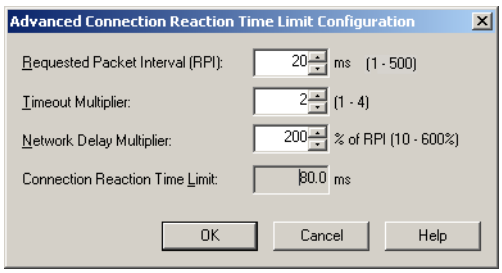


The RPI specifies the period at which data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.

The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, an acceptable Connection Reaction Time Limit can be achieved by adjusting the RPI.

The Max Network Delay is the maximum observed transport delay from the time the data was produced until the time the data was received. When online, you can reset the Max Network Delay by clicking Reset Max.

9. If the Connection Reaction time limit is acceptable, click OK; or for more complex requirements, click Advanced to set the Advanced Connection Reaction Time Limit parameters.



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

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

Table 31 - Additional Resources

Resource	Description
Pages 71…75	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 may not map a standard tag to a safety tag that has been designated as a constant.
- Tag mapping cannot be modified when the following is true:
  - The project is safety-locked.
  - A safety task signature exists.
  - The keyswitch is in RUN position.
  - A nonrecoverable safety fault exists.
  - An invalid partnership exists between the primary controller and safety partner.

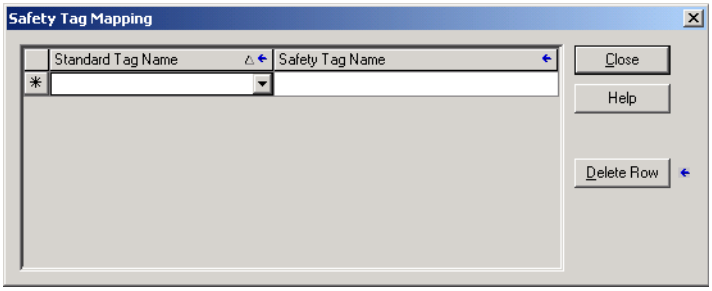


ATTENTION: When using standard data in a safety routine, you are responsible for providing a reliable means of ensuring that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 3/PLe safety output with standard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

Refer to the GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093, for more information.

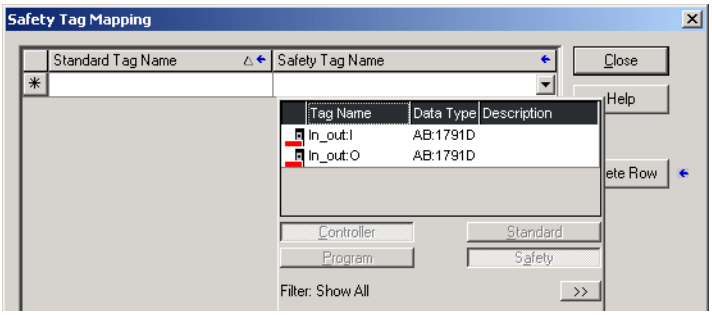
Create Tag Mapping Pairs

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



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

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



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

Monitor Tag Mapping Status

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

Table 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) 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 103.

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.

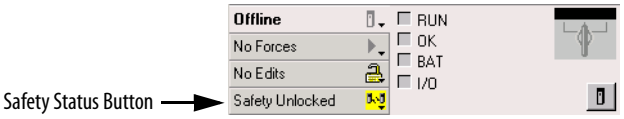
Safety-lock the Controller

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 may be present.

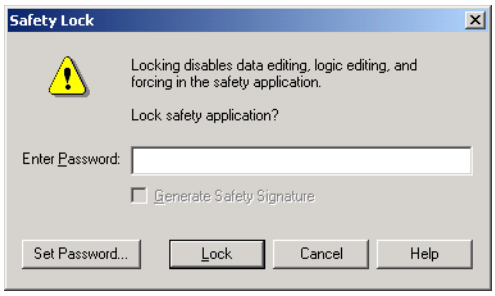
Safety-locked or -unlocked status cannot be changed when the keyswitch is in the RUN position.

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 26 - 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 49.

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

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

Generate a Safety Task Signature

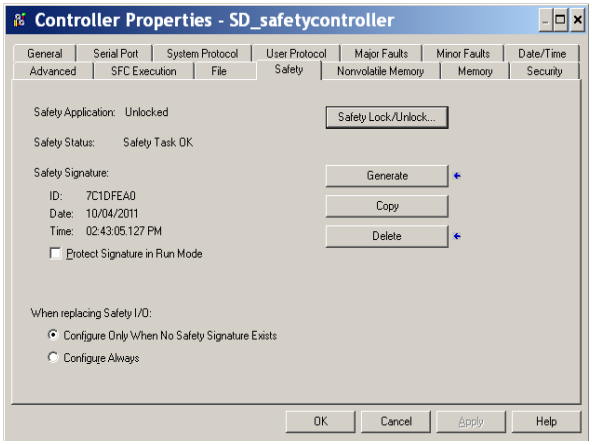
Before verification testing, you must generate the safety task signature. You can generate the safety task signature only when online with the safety-unlocked GuardLogix controller in Program mode, and with no safety forces, pending online safety edits, or safety faults. The safety status must be Safety 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 126) or on the Safety tab of the Controller Properties dialog box, as shown on page 107.

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

Figure 27 - 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 keyswitch in RUN.
- The controller is in Run or Remote Run mode with run mode protection enabled.



ATTENTION: If you delete the safety task signature, you must retest and revalidate your system to meet SIL 3/PLe.

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

Software Restrictions

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

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

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

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

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

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

Go Online with the Controller

Topic	Page
Connecting the Controller to the Network	109
Understanding the Factors that Affect Going Online	111
Download	113
Upload	115
Go Online	116

Connecting 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
Serial	1756-CP3 or 1747-CP3 cable	Connect to the 1756-L6xS Controller's Serial Port on page 36
USB	USB 2.0 cable	Connect to the 1756-L7xS Controller's USB Port on page 34
EtherNet/IP	EtherNet/IP module in an open slot in the same chassis as the controller	Connect Your EtherNet/IP Device and Computer on page 110
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 110
ControlNet	1756-CN2 module in an open slot in the same chassis as the controller	

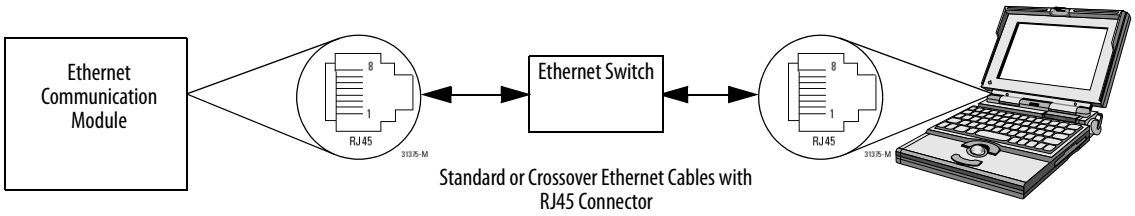
Connect Your EtherNet/IP Device and Computer

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 28 - 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.

Configuring 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

RSLogix 5000 software determines whether you can go online with a target controller based on whether the offline project is new or whether changes occurred in the offline project. If the project is new, you must first download the project to the controller. If changes occurred to the project, you are prompted to upload or download. If no changes occurred, you can go online to monitor the execution of the project.

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

Project to Controller Matching

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

If the Project to Controller Match feature is enabled in the offline project, RSLogix 5000 software compares the serial number of the controller in the offline project to that of the connected controller. If they do not match, you must cancel the download/upload, connect to the correct controller, or confirm that you are connected to the correct controller, which updates the serial number in the project to match the target controller.

Firmware Revision Matching

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

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

TIP You can also upgrade the firmware by choosing ControlFLASH™ from the Tools menu in RSLogix 5000 software.

Safety Status/Faults

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

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

Safety Task Signature and Safety-locked and -unlocked Status

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

On Upload

If the controller has a safety task signature, the safety task signature and the safety task lock status are uploaded with the project. For example, if the project in the controller was safety-unlocked, the offline project remains safety-unlocked following the upload, even if it was locked prior to the upload.

Following an upload, the safety task signature in the offline project matches the controller's safety task signature.

On Download

The existence of a safety task signature, and the controller's safety-lock status, determines whether or not a download can proceed.

Table 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. If the offline project is not safety-locked, but the controller is, the download is blocked and you must first unlock the controller to allow the download to proceed.
	Safety task signatures do not match.	You must first safety-unlock the controller to allow the download to proceed. If the controller had a safety task signature, it is automatically deleted, and the entire project is downloaded. Safety lock status matches the status in the offline project.

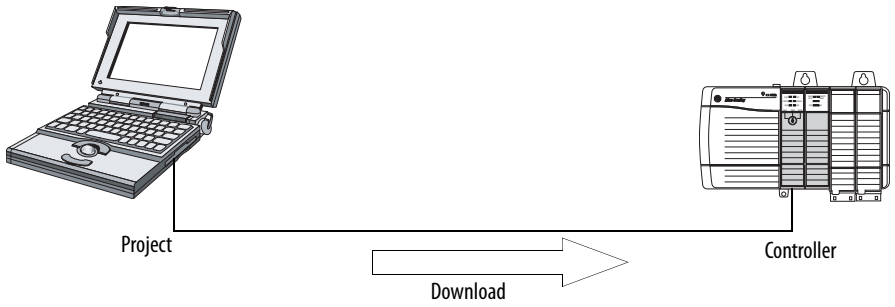
IMPORTANT During a download to a controller that is safety-unlocked, if firmware in the controller is different than in the offline project, do one of the following:

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

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

Download

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



1. Turn the keyswitch of the controller to REM.
2. Open the RSLogix 5000 project that you want to download.
3. Define the path to the controller.
   a. Click Who Active .
   b. Select the controller.
      To open a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
4. Click Download.

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

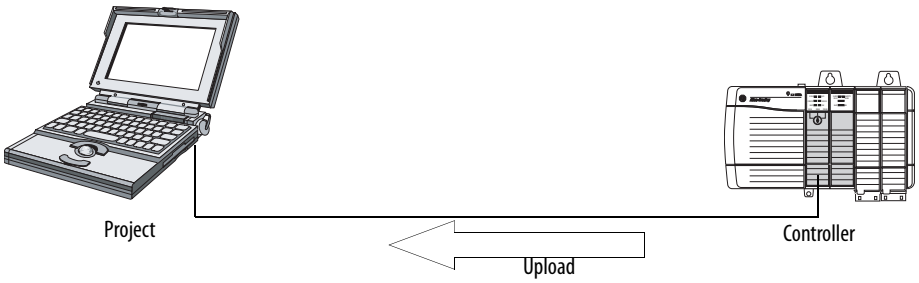
5. Follow the directions in this table to complete the download based on the software's response.

If the software indicates	Then
Download to the controller.	Choose Download. The project downloads to the controller and RSLogix 5000 software goes online.
Unable to download to the controller. Mismatch between the offline project and the controller serial number. Selected controller may be the wrong controller.	Connect to the correct controller or verify that this is the correct controller. If it is the correct controller, select the Update project serial number checkbox to allow the download to proceed. The project serial number is modified to match the controller serial number.
Unable to download to the controller. The major revision of the offline project and the controller's firmware are not compatible.	Choose Update Firmware. Choose the required revision and click Update. Confirm your selection by clicking Yes.
Unable to download to controller. The 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. Confirm your selection by clicking Yes.
Unable to download to controller. Safety partnership has not been established.	Cancel this download process and attempt a new download.
Unable to download to controller. Incompatible safety task signature cannot be deleted while the project is safety-locked.	Cancel the download. To download the project, you must safety-unlock the offline project, delete the safety task signature, and download the project. **IMPORTANT:** The safety system requires revalidation.
Cannot download in a manner that preserves the safety task signature. Controller's firmware minor revision is not compatible with safety task signature in offline project.	• If the firmware minor revision is incompatible, to preserve the safety task signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project. • To proceed with the download despite the safety task signature incompatibility, click Download. The safety task signature is deleted. **IMPORTANT:** The safety system requires revalidation.
Unable to download to controller. Controller is locked. Controller and offline project safety task signatures do not match.	Choose Unlock. The Safety Unlock for Download dialog box appears. If the Delete Signature checkbox is selected and you choose Unlock, you must confirm the deletion by selecting Yes.
A nonrecoverable safety fault will occur in the safety controller. No designated coordinated system time (CST) master exists.	Check Enable Time Synchronization and click Download to proceed.

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

Upload

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



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

   If the project to controller match is enabled, RSLogix 5000 software checks whether the serial number of the open project and the serial number of the controller match.

   If the controller serial numbers do not match, you can do one of the following:
   - Cancel the upload and connect to a matching controller. Then, start the upload procedure again.
   - Select a new project to upload into or select another project by choosing Select File.
   - Update the project serial number to match the controller by checking the Update Project Serial Number checkbox and choosing Upload.
5. The software checks whether the open project matches the controller project.
   a. If the projects do not match, you must select a matching file or cancel the upload process.
   b. If the projects match, the software checks for changes in the offline (open) project.

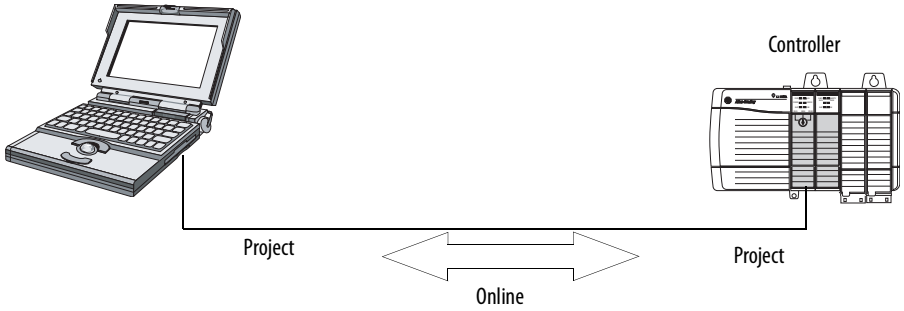
6. The software checks for changes in the offline project.
   a. If there are no changes in the offline project, you can go online without uploading. Click Go Online.
   b. If there are changes in the open project that are not present in the controller, you can choose to upload the project, cancel the upload, or select another file.

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

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

Go Online

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



1. Define the path to the controller.
   a. Click Who Active .
   b. Select the controller.
      To expand a level, click the + sign. If a controller is already selected, make sure that it is the correct controller.
2. Click Go Online.

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

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

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

When the controller and RSLogix 5000 software are online, the safety-locked status and safety task signature of the controller match the controller's project. The safety-lock status and safety task signature of the offline project are overwritten by the controller. If you do not want the changes to the offline project to be permanent, do not save the project file following the go online process.

Notes:

Store and Load Projects Using Nonvolatile Memory

Topic	Page
Using Memory Cards for Nonvolatile Memory	119
Storing a Safety Project	120
Loading a Safety Project	121
Use Energy Storage Modules (1756-L7xS controllers only)	122
Estimate the ESM Support of the WallClockTime	124
Manage Firmware with Firmware Supervisor	124

Using Memory Cards for Nonvolatile Memory

GuardLogix controllers, revision 18 or later, 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 RSLogix 5000 software

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

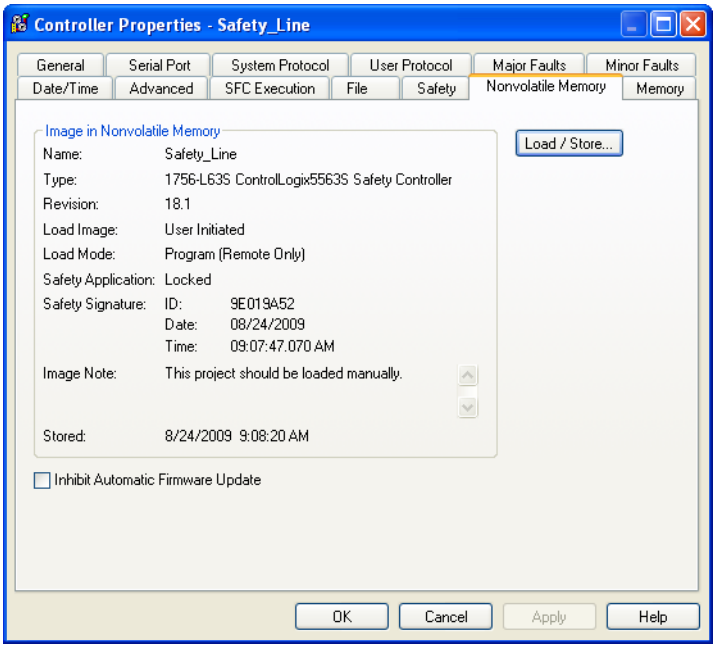
- Changes that you make after you store the project are not reflected in nonvolatile memory.
- If you make changes to the project but do not store those changes, you overwrite them when you load the project from nonvolatile memory. If this occurs, you have to upload or download the project to go online.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

If a memory card is installed, you can view the contents of the card on the

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.

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 29 - Nonvolatile Memory Tab



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

Storing a Safety Project

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

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

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

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

When you store a safety application project on a memory card, we recommend you select Program (Remote Only) as the Load mode, that is, the mode the controller should enter following the load.

Loading a Safety Project

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

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

You have several options for when (under what conditions) to load a project into the user memory of the controller.

Table 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. • The controller loads the stored project and firmware at every powerup regardless of the firmware or application on the controller. The load occurs whether or not the controller is safety-locked or has a safety task signature. • You can always use RSLogix 5000 software 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. • The controller updates the firmware on the primary controller or the safety partner, if required. The application stored in nonvolatile memory is also loaded and the controller enters the selected mode, either Program or Run. • You can always use RSLogix 5000 software to load the project.
Only through RSLogix 5000 software	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. • Loading a project to a safety-locked controller is allowed only when the safety task signature of the project stored in nonvolatile memory matches the project on the controller. • If the signatures do not match or the controller is safety-locked without a safety task signature, you are prompted to first unlock the controller. **IMPORTANT:** When you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety task signature are set to the values contained in nonvolatile memory once the load is complete. • If the firmware on the 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 may be overwritten by firmware on the memory card.

Use Energy Storage Modules (1756-L7*x*S controllers only)

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

- Provide power to 1756-L7*x*S controllers 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 1756-L7*x*S 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 The 1756-L7*x*S controllers come with this ESM installed.
1756-ESMNSE(XT)	Capacitor-based ESM without WallClockTime backup power Use this ESM if your application requires that the installed ESM deplete its residual stored energy to 200 µJ or less before transporting it into or out of your application. Additionally, you can use this ESM with a 1756-L73S (8MB) or smaller memory-sized controller only.
1756-ESMNRM(XT)	Secure capacitor-based ESM (non-removable) 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 Use this ESM if your application requires that the installed ESM deplete its residual stored energy to 200 µJ or less before transporting it into or out of your application. 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

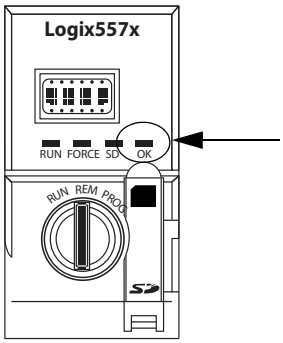
Follow these steps to save the program to NVS memory when the controller loses power.

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 30 - 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 allows it, follow these steps to clear the program from the 1756-L7*x*S 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

	Hold-up Time (in days)		
Temperature	**1756-ESMCAP(XT)**	**1756-ESMNRM(XT) 1756-SPESMNRM(XT)**	**1756-ESMNSE(XT) 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

Beginning with RSLogix 5000 software, version 18, 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 the ControlFLASH utility.

Firmware Supervisor supports non-modular distributed I/O products that sit directly on the network without an adapter, including CIP Safety I/O modules on EtherNet/IP networks. CIP Safety I/O modules on DeviceNet networks and POINT Guard I/O modules are not yet supported.

Follow these steps to enable Firmware Supervisor.

1. On the Controller Properties dialog box, click the Nonvolatile Memory tab.
2. Click Load/Store.
3. From the Automatic Firmware Updates pull-down menu, choose Enable and Store Files to Image.

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

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

Monitor Status and Handle Faults

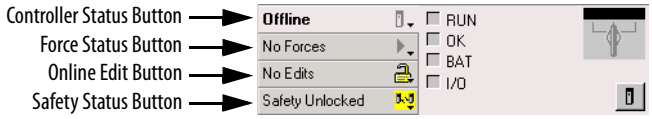
Topic	Page
Viewing Status via the Online Bar	125
Monitoring Connections	126
Monitoring Safety Status	128
Controller Faults	128
Developing a Fault Routine	131

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

Viewing Status via the Online Bar

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

Figure 31 - 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 32 - 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 Partner Unavailable Hardware Incompatible 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. 

Monitoring Connections

You can monitor the status of standard and safety connections.

All Connections

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

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



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

See Safety Connections.

Safety Connections

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

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

The ConnectionFaulted value indicates whether the safety connection between the safety producer and the safety consumer is Valid (0) or Faulted (1). If ConnectionFaulted is set to Faulted (1) as a result of a loss of the physical connection, the safety data is reset to zero.

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

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

Monitoring Status Flags

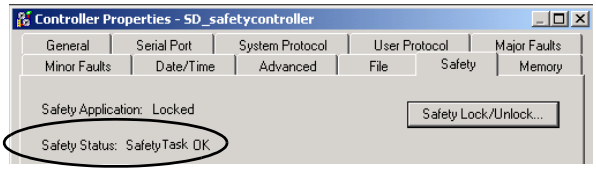
Logix controllers, including GuardLogix controllers, support status keywords that you can use in your logic to monitor certain events.

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

Monitoring Safety Status

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

Figure 33 - Safety Task Status



These are the possible values for safety status:

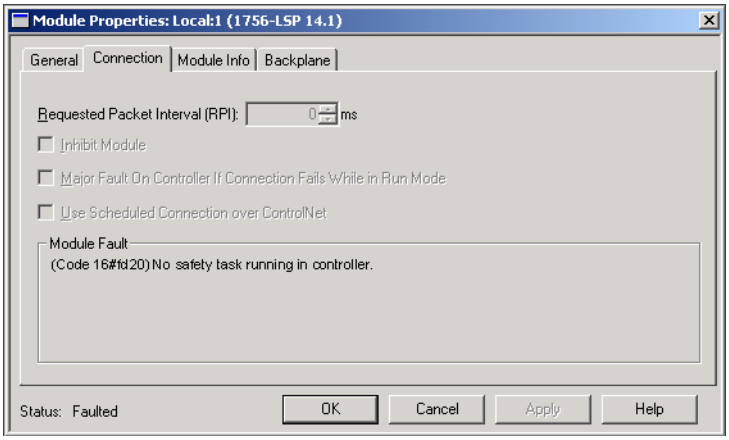
- Safety partner is missing or unavailable.
- Safety partner hardware is incompatible with primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety task OK.

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

See Major Safety Faults (Type 14) on page 130 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 34 - 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 CIP Safety I/O modules are placed in the safe state. Recovery requires that you download the application program again.

Nonrecoverable Safety Faults in the Safety Application

If a nonrecoverable safety fault occurs in the safety application, safety logic and the safety protocol are terminated. Safety task watchdog 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 the safety fault does not clear it! If you override the safety fault, it is your responsibility to prove that doing so maintains safe operation.

You must provide proof to your certifying agency that allowing a portion of the system to continue to operate maintains safe operation.

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

Recoverable Faults in the Safety Application

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

When a recoverable fault is cleared programmatically, the safety task is allowed to continue without interruption.

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

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

Viewing Faults

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

The status display on 1756-L7*x*S controllers also shows fault codes with a brief status message, as described beginning on page 137.

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. If a safety task signature exists, safety memory is re-initialized and the safety task begins executing. If a safety task signature does not exist, you must re-download the program to allow the safety task to run. 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. 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. If a safety task signature exists, safety memory is re-initialized via the safety task signature and the safety task begins executing. If a safety task signature does not exist, you must download the program again to allow the safety task to run.
08	Coordinated system time (CST) not found.	Nonrecoverable	Clear the fault. Configure a device to be the CST master.
09	Safety partner nonrecoverable controller fault.	Nonrecoverable	Clear the fault and download the program. If the problem persists, replace the safety partner.

A recoverable minor fault type (10), code 11, occurs when the 1756-LSP safety partner's battery is missing or requires replacement.

See Appendix B for information on replacing the battery.

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

Developing a Fault Routine

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

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



ATTENTION: You must provide proof to your certifying agency that allowing a portion of the system to continue to operate maintains safe operation.

The controller supports two levels for handling major faults:

- Program Fault Routine
- Controller Fault Handler

Both routines can use the GSV and SSV instructions as described on page 132.

Program Fault Routine

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

Controller Fault Handler

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

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

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

Use GSV/SSV Instructions

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

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

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

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

For safety objects, the Table 42 shows which attributes you can get values for by using the GSV instruction, and which attributes you are allowed to set by using the SSV instruction, in the safety and standard tasks.



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

Table 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.	✓		✓	
	MaximumInterval	DINT[2]	The max time interval between successive executions of this task.			✓	✓
	MaximumScanTime	DINT	Max recorded execution time (ms) for this task.			✓	✓
	MinimumInterval	DINT[2]	The min time interval between successive executions of this task.			✓	✓
	Priority	INT	Relative priority of this task as compared to other tasks. Valid values are 0…15.	✓		✓	
	Rate	DINT	Period for the task (in ms), or timeout value for the task (in ms).	✓		✓	
	Watchdog	DINT	Time limit (in ms) for execution of all programs associated with this task.	✓		✓	
Safety Program	Instance	DINT	Provides the instance number of the program object.	✓		✓	
	MajorFaultRecord[1]	DINT[11]	Records major faults for this program.	✓	✓	✓	
	MaximumScanTime	DINT	Max recorded execution time (ms) for this program.			✓	✓
Safety Routine	Instance	DINT	Provides the instance number for this routine object. Valid values are 0…65,535.	✓			

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 Controller	SafetyLocked	SINT	Indicates whether the controller is safety-locked or -unlocked.	✓		✓	
	SafetyStatus[2]	INT	Specifies the safety status as the following: • Safety task OK. (1000000000000000) • Safety task inoperable. (1000000000000001) • Partner missing. (0000000000000000) • Partner unavailable. (0000000000000001) • Hardware incompatible. (0000000000000010) • Firmware incompatible. (0000000000000011)			✓	
	SafetySignatureExists	SINT	Indicates whether the safety task signature is present.	✓		✓	
	SafetySignatureID	DINT	32-bit identification number.			✓	
	SafetySignature	String[3]	32-bit identification number.			✓	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Records safety task faults.			✓	
AOI (Safety)	LastEditDate	LINT	Date and time stamp of the last edit to an Add-On Instruction definition.			✓	
	SignatureID	DINT	ID number.			✓	
	SafetySignatureID	DINT	32-bit identification number.			✓	

(1) See Access FaultRecord Attributes on page 133 for information on how to access this attribute.
(2) See Capture Fault Information on page 134 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

Topic	Page
1756-L6xS Controller Status Indicators	135
1756-L7xS Controllers Status Indicators	136
1756-L7xS Controller Status Display	137

1756-L6*x*S Controller Status Indicators

Primary controller and safety partner status is displayed by LED status indicators.

Table 44 - 1756-L6*x*S Status Indicator Descriptions

Indicator	Status	Primary Controller Description	Safety Partner Description
RUN	Off	No user tasks running. Controller is in PROGram mode.	N/A
	Green	Controller is in RUN mode.	N/A
SAFE RUN	Off	N/A	The user safety task or safety outputs are disabled. The controller is in the PROGram mode, Test mode, or the safety task is faulted.
	Green	N/A	The user safety task and safety outputs are enabled. The safety application is executing. Safety task signature is present.
	Green, Flashing	N/A	The user safety task and safety outputs are enabled. The safety application is executing. Safety task signature is not present.
FORCE	Off	No forces, standard or safety, are enabled on the controller.	N/A
	Amber	Standard and/or safety forces have been enabled.	N/A
	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.	N/A
BAT	Off	The battery is able to support memory.	The battery is able to support memory.
	Red	The battery is not able to support memory.	The battery is not able to support memory.
OK	Off	No power is applied.	No power is applied.
	Green	The controller is operating with no faults.	The safety partner 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.	N/A
	Red	Powering up or nonrecoverable controller fault.	Powering up or nonrecoverable controller fault.
I/O[(1)]	Off	No activity. No I/O is configured.	N/A
	Green	The controller is communicating to all configured I/O devices, both standard and safety.	N/A
	Green, Flashing	One or more I/O devices is not responding.	N/A
	Red, Flashing	Controller is not communicating to configured I/O.	N/A

Table 44 - 1756-L6*x*S Status Indicator Descriptions

Indicator	Status	Primary Controller Description	Safety Partner Description
RS232	Off	There is no activity.	N/A
	Green	Data is being received or transmitted.	N/A
SAFETY TASK	Off	N/A	No partnership established. Primary controller is missing, is not functioning properly, or its firmware revision is incompatible with that of the safety partner.
	Green	N/A	Safety controller status is OK. The coordinated system time (CST) is synchronized and safety I/O connections are established.
	Green, Flashing	N/A	Safety controller status is OK. The coordinated system time (CST) is not synchronized on the primary controller or the safety partner.
	Red	N/A	Partnership was lost and a new partnership has not been established. Primary controller is missing, is not functioning properly, or its firmware revision is incompatible with that of the safety partner.
	Red, Flashing	N/A	Safety task is Inoperable.

(1) I/O includes produced/consumed tags from other controllers.

1756-L7*x*S Controllers Status Indicators

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

Table 45 - 1756-L7*x*S 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. **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. **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.

Table 45 - 1756-L7*x*S Primary Controller Status Indicator Descriptions

Indicator	Status	Description
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. • 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 • A nonrecoverable major fault occurred and the program was cleared from memory. • The charge of the capacitor in the Energy Storage Module (ESM) is being discharged upon powerdown. • The controller is powered but inoperable. • The controller is loading a project to nonvolatile memory.

The 1756-L7SP safety partner has an OK status indicator.

Table 46 - 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.

1756-L7*x*S Controller Status Display

The 1756-L7*x*S 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 may show the following messages. The safety partner displays 'L7SP'.

Table 47 - 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 48 are typically indicated upon powerup, powerdown, and while the controller is running. These messages indicate the status of the controller and the ESM.

Table 48 - General Status Display

Message	Interpretation
No message is indicated	The controller is off, or a major nonrecoverable fault (MNRF) has occurred. 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 136) for additional status information. Allow the save to 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 136) for additional status information. Allow the load to 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 136) for additional status information. 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. To load a project, use RSLogix 5000 software to download the project to the controller, or use a 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 RSLogix 5000 software.
BUSY	The I/O modules associated with the controller are not yet fully-powered. Allow time for powerup and I/O module self-testing.
Corrupt Certificate Received	The security certificate associated with the firmware is corrupted. 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. 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. Insert a compatible ESM, and, if using a capacitor-based ESM, do not remove power until the ESM is charged.
ESM Incompatible	The ESM is incompatible with the memory size of the controller. 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. 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. Replace the ESM.
ESM Charging	The capacitor-based ESM is charging. Do not remove power until charging is complete.
Flash in Progress	A firmware upgrade initiated via ControlFLASH or AutoFlash utilities is in progress. 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. Upgrade controller firmware.
SD Card Locked	An SD card that is locked is installed.

Fault Messages

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

Table 49 - Fault Messages(1)

Message	Interpretation
Major Fault T*XX*:C*XX message*	A major fault of Type *XX* and Code *XX* has been detected. For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, 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. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleName #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The name of the faulted module, as configured in the I/O Configuration tree of RSLogix 5000 software, is indicated with the fault code and brief description of the fault. For example, I/O Fault My_Module #0107 Connection Not Found indicates that a connection to the module named 'My_Module' is not open. Take corrective action specific to the type of fault indicated.
I/O Fault *ModuleParent:X #XXXX message*	An I/O fault has occurred on a module in a remote chassis. The module's parent name is indicated because no module name is configured in the I/O Configuration tree of RSLogix 5000 software. In addition, the fault code is indicated with a brief description of the fault. 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. 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. 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. 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 50 on page 140 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 50 - 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	Keyswitch 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 RSLogix 5000 software.

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 51 - 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 Settable	#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
—	

Maintain the Battery

Topic	Page
Estimate Battery Life	143
When to Replace the Battery	145
Replace the Battery	145
Store Replacement Batteries	147

GuardLogix 1756-L6*x*S primary controllers and 1756-LSP safety partners contain a lithium battery which may need to be replaced. GuardLogix 1756-L7*x*S controllers and 1756-L7SP safety partners do not have a battery.

Estimate Battery Life

Battery life is dependent upon chassis temperature, project size, and how often you cycle power to the controller. Battery life is not dependent upon whether or not the controller has power.

Before BAT Indicator Turns On

Use this table to estimate the worst case time before the BAT indicator turns red.

Table 52 - Battery Indicator Estimate (worst-case)

Temperature 2.54 cm (1 in.) Below Chassis	Power Cycles per Day	Project Size			
		1 MB	2 MB	4 MB	8 MB
0…40 °C (32…104 °F)	3	3 years	3 years	26 months	20 months
	2 or less	3 years	3 years	3 years	31 months
41…45 °C (105…113 °F)	3	2 years	2 years	2 years	20 months
	2 or less	2 years	2 years	2 years	2 years
46…50 °C (114…122 °F)	3 or less	16 months	16 months	16 months	16 months
51…55 °C (123…131 °F)	3 or less	11 months	11 months	11 months	11 months
56…60 °C (132…140 °F)	3 or less	8 months	8 months	8 months	8 months

EXAMPLE Under the following conditions, the battery will last at least 20 months before the BAT indicator turns red:

- Maximum temperature 2.54 cm (1 in.) below the chassis is 45 °C (113 °F).
- Power is cycled three times per day.
- The controller contains a 8 MB project.

After BAT Indicator Turns On

IMPORTANT If the BAT indicator turns on for the first time when you apply power to the controller, the battery life is less than Table 53 indicates. There is always a small constant drain on the battery. Some of the battery life may have been used while the controller was off and unable to turn on the BAT indicator.

Table 53 - Battery Life After the BAT Indicator Turns Red (worst-case)

Temperature, Max. 25.4 mm (1 in.) Below the Chassis	Power Cycles	Project Size			
		1 MB	2 MB	4 MB	8 MB
0…20 °C (0…68 °F)	3 per day	26 weeks	18 weeks	12 weeks	9 weeks
	1 per day	26 weeks	26 weeks	26 weeks	22 weeks
	1 per month	26 weeks	26 weeks	26 weeks	26 weeks
21…40 °C (70…104 °F)	3 per day	18 weeks	14 weeks	10 weeks	8 weeks
	1 per day	24 weeks	21 weeks	18 weeks	16 weeks
	1 per month	26 weeks	26 weeks	26 weeks	26 weeks
41…45 °C (106…113 °F)	3 per day	12 weeks	10 weeks	7 weeks	6 weeks
	1 per day	15 weeks	14 weeks	12 weeks	11 weeks
	1 per month	17 weeks	17 weeks	17 weeks	17 weeks
46…50 °C (115…122 °F)	3 per day	10 weeks	8 weeks	6 weeks	6 weeks
	1 per day	12 weeks	11 weeks	10 weeks	9 weeks
	1 per month	12 weeks	12 weeks	12 weeks	12 weeks
51…55 °C (124…131 °F)	3 per day	7 weeks	6 weeks	5 weeks	4 weeks
	1 per day	8 weeks	8 weeks	7 weeks	7 weeks
	1 per month	8 weeks	8 weeks	8 weeks	8 weeks
56…60 °C (133…140 °F)	3 per day	5 weeks	5 weeks	4 weeks	4 weeks
	1 per day	6 weeks	6 weeks	5 weeks	5 weeks
	1 per month	6 weeks	6 weeks	6 weeks	6 weeks

When to Replace the Battery

When the battery is about 95% discharged, the controller provides the following warnings:

- The BAT indicator on the front of the controller turns on (solid red).
- A minor fault occurs (type 10, code 10 for the controller).

ATTENTION: To prevent your battery from leaking potentially dangerous chemicals, replace your battery according to the following schedule, even if the BAT indicator is off.

Table 54 - Battery Replacement Schedule

If the temperature 2.54 cm (1 in.) below the chassis is	Replace the battery every
-25…35 °C(-13…95 °F)	No replacement required
36…40 °C (96.8…104 °F)	3 years
41…45 °C (105.8…113 °F)	2 years
46…50 °C (114.8…122 °F)	16 months
51…55 °C (123.8…131 °F)	11 months
56…70 °C (132.8…158 °F)	8 months

IMPORTANT Because the GuardLogix controller is a 1oo2 controller (two processors), we strongly recommend that you replace both controller batteries at the same time.

Replace the Battery

This controller contains a lithium battery, which is intended to be replaced during the life of the product. You must follow specific precautions when handling or disposing of a battery.

ATTENTION: The controller uses a lithium battery that contains potentially dangerous chemicals.

Before handling or disposing of a battery, review Guidelines for Handling Lithium Batteries, publication AG-5.4.

WARNING: When you connect or disconnect the battery, 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.

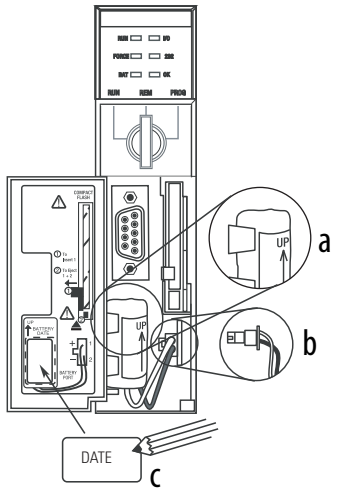
IMPORTANT If you remove the battery and later lose power, the project in the controller will be lost.

Follow this procedure to replace the battery.

1. Turn on the chassis power.
2. Does the battery show signs of leakage or damage?

If	Then
Yes	Before handling the battery, review Guidelines for Handling Lithium Batteries, publication AG-5.4
No	Go to the next step.

3. Remove the old battery.
4. Install a new 1756-BA2 battery.
   a. Insert the battery as shown.
   b. Connect the battery:
      + Red
      - Black
   c. Write the date you installed the battery on the battery label and attach the label to the inside of the controller door.



ATTENTION: Install only a 1756-BA2 battery. If you install a different battery, you may damage the controller.

5. Determine if the BAT indicator on the front of the controller is off.

If	Then
Yes	Go to the next step.
No	1. Check that the battery is correctly connected to the controller. 2. If the BAT indicator remains on, install another 1756-BA2 battery. 3. If the BAT indicator remains on after installing the alternate battery in step 2, contact your Rockwell Automation representative or local distributor.

6. Dispose of the old battery in accordance with local regulations.

WARNING: Do not incinerate or dispose of lithium batteries in general trash collection. They may explode or rupture violently. Follow all local regulations for disposal of these materials. You are legally responsible for hazards created during disposal of your battery.



ATTENTION: This product contains a sealed lithium battery that may need to be replaced during the life of the product.

At the end of its life, the battery contained in this product should be collected separately from any unsorted municipal waste.

The collection and recycling of batteries helps protect the environment and contributes to the conservation of natural resources as valuable materials are recovered.

Store Replacement Batteries

ATTENTION: A battery may leak potentially dangerous chemicals if stored improperly. Store batteries in a cool, dry environment. We recommend 25 °C (77 °F) with 40…60% relative humidity. You may store batteries for up to 30 days at temperatures between -45…85 °C (-49…185°F), such as during transportation. To avoid possible leakage, do not store batteries above 60 °C (140 °F) for more than 30 days.

Additional Resources

See Guidelines for Handling Lithium Batteries, publication AG-5.4, for more information on handling, storing, and disposing of lithium batteries.

Notes:

Change Controller Type in RSLogix 5000 Projects

Topic	Page
Changing from a Standard to a Safety Controller	149
Changing from a Safety to a Standard Controller	150
Changing from a 1756 GuardLogix Controller to a 1768 Compact GuardLogix Controller or Vice Versa	151
Changing from a 1756-L7xS Controller to a 1756-L6xS or 1768-L4xS Controller	151
Additional Resources	151

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

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

Changing from a Standard to a Safety Controller

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

Changing from a Safety to a Standard Controller

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

- The safety partner, 1756-LSP, is deleted from the I/O chassis.
- Safety I/O modules and their tags are deleted.
- The safety task, programs, and routines are changed to a standard task, programs, and routines.
- All safety tags, except safety consume tags, are changed to standard tags. Safety consume tags are deleted.
- Safety tag mappings are deleted.
- The safety network number (SNN) is deleted.
- Safety-lock and -unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, those new features are visible in the Controller Properties dialog box.

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

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

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

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

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

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

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

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

Changing from a 1756-L7*x*S Controller to a 1756-L6*x*S or 1768-L4*x*S Controller

Floating-point instructions, such as FAL, FLL, FSC, SIZE, CMP, SWPB, and CPT are supported in 1756-L7*x*S controllers, but not in 1756-L6*x*S and 1768-L4*x*S controllers. If your safety program contains these instructions, verification errors will occur when changing from a 1756-L7*x*S controller to a 1756-L6*x*S or 1768-L4*x*S controller.

Additional Resources

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

Notes:

History of Changes

With the availability of new controllers, modules, applications, and RSLogix 5000 software features, this manual has been revised to include updated information. This appendix briefly summarizes changes that have been made with each prior revision of this manual.

Reference this appendix if you need to determine what changes have been made across multiple revisions. This may be especially useful if you are deciding to update your hardware or software based on information added with previous revisions of this manual.

1756-UM020H-EN-P April 2012

Corrected list of supported power supplies.

1756-UM020G-EN-P, February 2012

- Added information on 1756-L7*x*S and 1756-L73SXT controllers
- Updated list of Additional Resources
- Added a chapter on installing the controller
- Added information on using unicast connections for I/O modules on EtherNet/IP networks
- Added installation information
- Added information on Run mode protection for the safety task signature
- Updated I/O replacement procedures to include various replacement scenarios
- Updated Requested Packet Interval maximum value
- Added DCA_INPUT and DCAF_INPUT data types to list of valid types for safety tags
- Restructured information on produced and consumed safety tags and configuring peer safety controllers so that all information is together in Chapter 6
- Added information on the impact of a locked SD card on a firmware update
- Added information on using the Energy Storage Module (ESM) for nonvolatile memory
- Moved status indicator description tables to an appendix and added troubleshooting information

- Updated information on when to replace the battery on 1756-L6*x*S controllers
- Added information on changing to a 1756-L7*x*S controller
- Added History of Changes appendix

1756-UM020F-EN-P, August 2010

- GuardLogix controllers are supported in RSLogix 5000, version 19
- Default connection type for produced and consumed safety tags is unicast

1756-UM020E-EN-P, January 2010

- High-integrity and safety Add-On Instructions added to list of supported RSLogix 5000 features
- Enabling time synchronization
- Updated the examples of changing the safety network number (SNN) of safety I/O modules on the CIP safety network to show EtherNet/IP safety I/O modules
- Clarified information on Ethernet addressing
- Controlnet connections for distributed I/O modules
- Defining a tag as a constant
- Setting the external access level for tag data
- Updated procedures for producing and consuming safety tags
- Restriction for mapping constant value tags
- Updated table of software responses during download
- GSV/SSV accessibility for AOI Safety object
- Store and load projects using nonvolatile memory
- Updated battery disposal information
- Changing from a 1756 GuardLogix to a 1768 Compact GuardLogix controller or vice versa

1756-UM020D-EN-P, July 2008

- Updated Additional Resources table to include new manuals
- Information on the 1756-L63S controller
- General information on programming by using RSLogix 5000 software, version 17, including supported software versions and enhancements
- Using a 1756-EN2T module in a GuardLogix-based system
- Information Guard I/O EtherNet/IP safety modules
- Updated list of valid data types for safety tags
- Safety-lock and -unlock actions are logged
- Safety signature creation and deletion are logged
- Download process now includes check for Coordinated System Time (CST) master
- Updated safety task inoperable fault code description
- Safety signature value is accessible via GSV instruction

- Data Type information for attributes accessible via GSV and SSV instructions
- Accessing fault information using GSV instruction
- Updated certification information
- Updated information on estimating battery life
- Updated information on proper battery disposal

1756-UM020C-EN-P, December 2006

- Understanding a GuardLogix controller's data flow capabilities
- The controller does not support OS upgrades by using CompactFlash
- The safety task does not support Add-On Instructions or FactoryTalk® Alarms and Events software
- The maximum RPI for safety connections has changed from 500 ms to 100 ms
- The list of invalid data types for safety programs has been replaced by a list of valid data types
- Revised description of safety produced and consumed connections
- Revised description of the effect of the safety-lock feature and the safety signature on download
- UL NRGF certification added
- Probability of failure on demand (PFD) and probability of failure per hour (PFH) values added to controller specifications

1756-UM020B-EN-P, October 2005

RSLogix 5000 programming software, version 14.01 and later, no longer compares hardware series between the safety partner and the primary controller or between the controller and the safety signature in the project.

1756-UM020A-EN-P, January 2005

Initial release.

Numerics

1747-CP3 37, 109
1747-KY 26
1756-Axx 27
1756-BA2 26, 27, 146
1756-CN2 63
1756-CN2R 63
1756-CN2RXT 63
1756-CNB 63
1756-CNBR 63
1756-CP3 26, 37, 109
1756-DNB 65, 66, 109
1756-EN2F 59
1756-EN2T 59
1756-EN2TR 59
1756-EN2TXT 59
1756-EN3TR 59
1756-ENBT 59
1756-ESMCAP 26, 44, 46, 122, 124
1756-ESMCAPXT 26, 44, 46, 122, 124
1756-ESMNRM 26, 44, 46, 122, 124
1756-ESMNRMXT 26, 46, 122, 124
1756-ESMNSE 26, 44, 46, 122, 124
1756-ESMNSEXT 26, 46, 122, 124
1756-EWEB 59
1756-PA72 27
1756-PA75 27
1756-PAXT 27
1756-PB72 27
1756-PB75 27
1756-PBXT 27
1756-SPESMCAP 26, 44
1756-SPESMNRM 26, 46, 122
1756-SPESMNRMXT 26, 46, 122
1756-SPESMNSE 26, 44, 46, 122
1756-SPESMNSEXT 26, 44, 46, 122
1768 Compact GuardLogix controller 151
1784-CF128 26
1784-SD1 26
1784-SD2 26

A

Add-On Instructions 21, 150
address
  CIP Safety I/O module 77
advanced connection reaction time 73
alert symbol 126
alias tags 93
attributes
  safety object 132
AutoFlash
  firmware update 41
automatic firmware updates 124

B

base tags 93
BAT indicator 125, 144, 146
battery 26
  connect 27, 28, 145, 146
  disconnect 145, 146
  disposal 147
  fault 125, 130
  installation 146
  life 143, 144
  replacement procedure 145
  replacement schedule 145
  storage 147

C

CF card
  See CompactFlash card.
Change Controller button 49
changing controllers 149-150
chassis 19
  catalog numbers 27
CIP Safety 12, 53, 85
CIP Safety I/O
  adding 69
  configuration signature 75
  monitor status 77
  node address 69
  reset ownership 76
  status data 77
class 96
clear
  faults 129
  program 123
communication 20
  ControlNet network 63
  DeviceNet network 65
  EtherNet/IP network 59
  modules 20
  serial network 67
Compact GuardLogix controller 151
CompactFlash card 26, 29
  insert 32
  remove 33
  See also memory card.
configuration owner 76
  identifying 76
  resetting 76, 79
configuration signature
  components 75
  copy 75
  definition 75
configure always 84
  checkbox 51

connection
ControlNet network 64
EtherNet/IP network 60
monitor 126
scheduled 64
status 127
unscheduled 64
USB 34
connection reaction time limit 71, 101
CONNECTION_STATUS 97, 127
ConnectionFaulted bit 127
constant value tag 96
consume tag data 100
consumed tag 93, 97
control and information protocol
definition 12
ControlFLASH software 39, 111, 121, 124
controller
change type 149-??, 149-151
configuration 47
extreme environment 12
fault handler 131
feature differences 11
installation 28
logging
safety lock, unlock 105
safety task signature 107
match 111
mode 42
operating mode 42, 43
properties 48
serial number 111
serial number mismatch 114, 117
controller-scoped tags 95
ControlNet
communication modules 20
configure driver 110
connections 64, 110
example 64
module 63, 109
overview 63
scheduled 64
software 63
unscheduled 64
coordinated system time 114, 137
copy
safety network number 58
safety task signature 107
create a project 47

D

data types
CONNECTION_STATUS 97
delete
safety task signature 108
DeviceNet
communication 65
configure driver 110
connections 66, 110
module 109
software 66
DF1 67
DH-485 67
diagnostic coverage 12
DNT file 87, 88
download
effect of controller match 111
effect of firmware revision match 111
effect of safety status 111
effect of safety task signature 112
effect of safety-lock 112
process 113-114
driver
ControlNet 110
DeviceNet 110
EtherNet/IP 110
USB 35

E

editing 107
electronic keying 124
electrostatic discharge 25
enclosure 23
energy storage module 26
1756-ESMCAP 26
charging 28, 46
definition 12
hold-up time 124
install 46
non-volatile storage 122
uninstall 44
environment 23
ESM
See energy storage module
EtherNet/IP
CIP Safety I/O modules 61
communication modules 20
configure driver 110
connection use 60
connections 60, 110
example 61
example configuration 61
module 109
module capability 59
modules 59
network parameters 62
overview 59
software 60
standard I/O modules 62
external access 92, 96
extreme environment
chassis 27
controller 12
power supply 27
system components 12

F

fault
clear 129
messages 139
nonrecoverable controller 129
nonrecoverable safety 128, 129
recoverable 129, 139
routines 131-133
fault codes
I/O messages 140
major safety faults 130
status display 130
firmware revision
management 124
match 111
mismatch 112, 114, 117
update 39, 41
Firmware Supervisor 124
firmware upgrade kit 111, 124
forcing 107

G

gateway 62
general status messages 138
get system value (GSV)
accessibility 132
definition 12
using 132
go online 116
factors 111
Guard I/O module
replacement 79-88
GuardLogix controllers
differences 11

H

hazardous location approval
Europe 25
North America 24
HMI devices 16
hold-up time
energy storage module 124

I

I/O
fault codes 140
indicator 126
module replacement 51
IP address 62, 70

K

keyswitch 19, 42

L

listen only connection 76
lithium battery 145, 147
load a project 121
on corrupt memory 121
on power up 121
user initiated 121
lock
See safety-lock.
Logix-XT system components
See extreme environment.

M

major faults tab 130
Major Recoverable Fault
messages 139
major recoverable faults 139
major safety faults 130
MajorFaultRecord 133
maximum observed network delay 72
reset 101
memory
capacity 18
card 18
memory card 119, 120, 121, 124
installation 29
removal 29
message
status display 138
messages
fault 139
general status 138
safety status 137
minor faults tab 130
mode
operating 42
module
ControlNet 20
DeviceNet 20
EtherNet/IP 20, 59
properties
connection tab 76
status indicator 78
monitor
connections 126
status 77
morphing
See changing controllers.
multicast 12

N

network delay multiplier 74, 102
network status
indicator 78, 82, 83, 87
new controller dialog box 47
node address 69
nonrecoverable controller fault 129
nonrecoverable safety fault 128, 129
re-starting the safety task 129

nonvolatile memory 119-124
tab 120

O

online bar 125
operating mode 42
out-of-box 81
reset module 79
ownership
configuration 76
resetting 76

P

password
set 49
valid characters 50
paste
safety network number 58
peer safety controller
configuration 52
location 97
sharing data 97
SNN 97, 98
Performance Level 12, 15
power supply
catalog numbers 19, 27
primary controller
description 18
hardware overview 18
modes 19
user memory 18
probability of failure on demand (PFD)
definition 12
probability of failure per hour (PFH)
definition 12
produce a tag 99
produce and consume tags 60, 63, 97
produced tag 93, 97
program fault routine 131
Program mode 42
programming 107
program-scoped tags 95
project to controller match 111
protect signature in run mode 50
protecting the safety application 105-108
RSLogix Security 106
safety task signature 106
safety-lock 105

R

RAM capacity 18
reaction time 91
reaction time limit
CIP Safey I/O 71
REAL data types 94
recoverable fault 129, 139
clear 129
Remote mode 42, 43
removal and insertion under power 24
replace
configure always enabled 84
configure only… enabled 80
Guard I/O module 79-88
replacement schedule
battery 145
requested packet interval 97
CIP Safety I/O 72
consumed tag 101
consumed tags 93
definition 12
produced tag data 93
reset
module 79
ownership 76, 79
restrictions
programming 108
safety tag mapping 103
software 108
when safety signature exists 107
when safety-locked 105
RIUP
See removal and insertion under power
RPI
See requested packet interval
RS-232 DF1 Device driver 37
RSLinx Classic software
version 21
RSLogix 5000 software
reset module 79
restrictions 108
versions 21
RSLogix Security 106
RSNetWorx for DeviceNet software
replace module 86
Run mode 42
run mode protection 106, 108
RunMode bit 127

S

safe state 15

safety network number 53
assignment 53
automatic assignment 55
changing controller SNN 56
changing I/O SNN 56
copy 58
copy and paste 58
definition 12
description 15
formats 53
managing 53
manual 54
manual assignment 55
mismatch 86
modification 55
paste 58
set 71
time-based 54
view 48
safety object
attributes 132
safety partner
configuration 19
description 19
status 128
status indicators 135
safety programs 92
safety projects
features 21
safety routine 92
using standard data 103
safety status
button 106, 126
effect on download 111
programming restrictions 108
safety task signature 106
view 111, 125, 128
safety tab 106, 107, 128
configuration signature 75
connection data 72
generate safety task signature 107
module replacement 80
safety-lock 106
safety-lock controller 106
unlock 106
view safety status 111, 128
safety tags
controller-scoped 95
create 93
description 92
mapping 102-104
safety-program-scoped 95
valid data types 94
safety task 90
execution 91
priority 90
watchdog time 90
safety task period 72, 91, 97
safety task signature 96
copy 107
delete 108
description 16
effect on download 112
effect on upload 112
generate 106
restricted operations 107
restrictions 108
storing a project 121
view 125
safety-lock 105
controller 106
effect on download 112
effect on upload 112
icon 105
password 106
SafetyTaskFaultRecord 133
safety-unlock
controller 106
icon 105
save program
non-volatile memory 122
scan times
reset 108
scheduled connections 64
SD card
See Secure Digital card.
Secure Digital card 26, 29
install 31
remove 30
See also memory card.
serial
cable 26
communication 67
driver 37
network 67
software 67
port 36
configuration 67
connection 36
serial number 111
set system value (SSV)
accessibility 132
using 132
slot number 48
SNN
See safety network number
software
ControlNet network 63
DeviceNet networks 66
EtherNet/IP network 60
restrictions 108
USB 34
standard data in a safety routine 103
status
display 137-142
fault messages 139
indicators 135-137
messages 137
messages, display 138
safety partner 128
status flags 127

status indicators
I/O modules 78
store a project 120
subnet mask 62

T

tags
alias 93
base 93
class 96
constant value 96
consumed 93, 97
controller-scoped 95
data type 94
external access 92, 96
naming 76
overview 92
produced 93, 97
produced/consumed safety data 94, 95
program-scoped 95
safety I/O 94, 95
scope 95
See also, safety tags.
type 93
terminology 12
time synchronization 51, 114
timeout multiplier 73, 102

U

unicast 12
connections 71, 97, 100
unlock controller 106
unscheduled connections 64
update
firmware 39, 41
updates 18
upload
effect of controller match 111
effect of safety task signature 112
effect of safety-lock 112
process 115
USB
cable 34, 109
connection 34
driver 35
port 34
software required 34
type 34
user memory 18
user program storage 18
UV radiation 25

V

verification errors
changing controller type 151
view
safety status 111

W

WallClockTime 122, 124
energy storage module 124
object 46
watchdog time 90

X

XT
See extreme environment.

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 manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect[SM] support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/support/.

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/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to 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/.

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1756-UM020I-EN-P - August 2012
Supersedes Publication 1756-UM020H-EN-P - April 2012

Copyright © 2012 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP