

Allen-Bradley

GuardLogix Controllers

**(Catalog Numbers 1756-L61S,
1756-L62S, 1756-LSP)**

User Manual

**Rockwell
Automation**

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.ab.com/manuals/gi>) 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.

IMPORTANT

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

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
 - recognize the consequence
-

Allen-Bradley, ControlLogix, and RSLink are registered trademarks of Rockwell Automation, Inc.

RSLogix and RSNetWorx for DeviceNet are trademarks of Rockwell Automation, Inc.

DeviceNet is a trademark of the Open DeviceNet Vendor Association.

ControlNet is a trademark of ControlNet International, Ltd.

Windows is a registered trademark of Microsoft Corporation.

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 have included change bars as shown to the right of this paragraph.

For information about	See
RSLogix 5000 programming software, revision 14.01 and higher, no longer compares hardware series between the Safety Partner and Primary Controller or between the controller and the Safety Signature in the project. References to this comparison have been removed from the pages indicated.	pages 1-3, 6-7, 6-8, 6-9, 6-12, and 7-2

Preface

Who Should Use this Manual	P-1
Purpose of this Manual	P-1
Related Documentation	P-2
Common Techniques Used in this Manual	P-2
Understanding Terminology	P-3

Chapter 1

GuardLogix System Overview

Understand the Safety Concept	1-1
Safety Application Requirements.	1-1
Safety Application Characteristics	1-1
Distinguish Between Standard and Safety Components	1-2
HMIs	1-3
Select GuardLogix System Hardware	1-3
Primary Controller	1-3
Safety Partner	1-4
Chassis	1-5
Power Supply	1-5
Select Safety I/O	1-5
Communicate Over Networks	1-6
Program Your System	1-7

Chapter 2

Configure the GuardLogix Controller

Create a New Controller	2-1
Set Passwords for Safety-Locking and -Unlocking	2-4
Handle I/O Module Replacement.	2-5
Select the CST Master	2-5
Configure Project to Controller Matching	2-6
Configure a Peer Safety Controller	2-7

Chapter 3

Communicate Over Networks

The Safety Network.	3-1
Understand CIP Safety Protocol	3-1
Manage the Safety Network Number.	3-1
Assign the SNN	3-3
Change the SNN	3-3
EtherNet/IP Communications.	3-6
Produce and Consume Data via EtherNet/IP	3-6
EtherNet/IP in a GuardLogix System	3-7
DeviceNet Communications.	3-8
DeviceNet Safety Connections	3-9
Standard DeviceNet Connections	3-9
Serial Communications	3-10

**Add, Configure, Monitor, and
Replace DeviceNet Safety I/O****Chapter 4**

Add DeviceNet Safety I/O	4-1
Configure DeviceNet Safety I/O Modules via RSLogix 5000	4-2
Set the Safety Network Number	4-3
Set the Connection Reaction Time Limit	4-4
Specify the Requested Packet Interval	4-4
Understand the Maximum Observed Network Delay	4-5
Set the Advanced Connection Reaction Time Limit Parameters	4-6
Understand the Configuration Signature	4-8
Configured Via RSLogix 5000	4-8
Different Configuration Owner	4-8
Reset Safety I/O Module Ownership	4-8
Address Safety I/O Data	4-9
Monitor Safety I/O Module Status	4-9
Via LEDs	4-10
Monitor Input and Output Status Data	4-11
Replace a DeviceNet Safety I/O Module	4-11
Prepare the I/O Module	4-11
I/O Replacement with <i>Configure Always</i> Disabled	4-12
I/O Replacement Using <i>Configure Always</i> Feature	4-14

Develop Safety Applications**Chapter 5**

The Safety Task	5-2
Safety Task Period Specification	5-2
Safety Task Execution	5-3
Safety Programs	5-4
Safety Routines	5-4
Safety Tags	5-5
Tag Type	5-6
Data Type	5-6
Scope	5-7
Class	5-8
Produced/Consumed Safety Tags	5-9
Produce a Safety Tag	5-9
Consume Safety Tag Data	5-10
Safety Tag Mapping	5-14
Restrictions	5-14
Create Tag Mapping Pairs	5-15
Monitor Tag Mapping Status	5-16
Safety Application Protection	5-16
Safety-Lock the Controller	5-16
Generate a Safety Signature	5-18
Software Restrictions	5-20

Go Online with the Controller	Chapter 6	
	Connect the Controller to the Network.	6-1
	Connect the Controller via a Serial Network	6-2
	Connect Your EtherNet/IP Device and Computer	6-2
	Connect Your DeviceNet Scanner or ControlNet Communication Module and Your Computer	6-3
	Configure the Network Driver	6-3
	Configure a Serial Communications Driver	6-3
	Configure an EtherNet/IP, DeviceNet, or ControlNet Driver	6-4
	Understand the Factors that Affect Going Online	6-4
	Project to Controller Matching	6-5
	Firmware Revision Matching.	6-5
	Safety Partner Status/Faults.	6-6
	Safety Signature and Safety-Locked/-Unlocked Status. . .	6-6
	Download	6-8
	Upload	6-10
	Go Online	6-11
Monitor Status and Handle Faults	Chapter 7	
	Monitor Controller Status.	7-1
	Controller LEDs	7-1
	Online Bar.	7-3
	Monitor Connections.	7-4
	All Connections	7-4
	Safety Connections.	7-4
	Monitor Status Flags	7-5
	Monitoring Safety Status	7-5
	GuardLogix Controller Faults	7-6
	Non-Recoverable Controller Faults	7-6
	Non-Recoverable Safety Faults in the Safety Application	7-6
	Recoverable Faults in the Safety Application	7-7
	View Faults	7-7
	Fault Codes	7-7
	Developing a Fault Routine	7-8
	Program Fault Routine	7-9
	Controller Fault Handler.	7-9
	Using GSV/SSV Instructions	7-10
Controller Specifications	Appendix A	
	Certifications.	A-1
	General Specifications.	A-1
	Environmental Specifications	A-2
	Environment and Enclosure Information	A-3
	North American Hazardous Location Approval	A-4

Maintain the Battery

Appendix B

Estimate Battery Life B-1

 Before BAT LED Turns On B-1

 After BAT LED Turns ON B-2

When to Replace the Battery B-3

Replace the Battery B-3

Storing Replacement Batteries B-5

Change Controllers

Appendix C

From Standard to Safety C-1

From Safety to Standard C-2

Index

Read this preface to familiarize yourself with the rest of the manual. It provides information concerning:

- who should use this manual
- the purpose of this manual
- related documentation
- conventions used in this manual
- terminology used in this manual

Who Should Use this Manual

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.

Purpose of this Manual

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

For detailed information on related topics like programming your GuardLogix controller, SIL 3 requirements, or information on ControlLogix components, see the list of 'Related Documentation' below.

Related Documentation

The table below provides a listing of publications that contain important information about GuardLogix Controller systems.

For	Read this document	Publication
Information on installing the GuardLogix Controller	GuardLogix Controller Installation Instructions	1756-IN045
Detailed requirements for achieving and maintaining SIL 3 with the GuardLogix Controller System	GuardLogix Controllers Systems Safety Reference Manual	1756-RM093
Information on the GuardLogix Safety Application Instruction Set	GuardLogix Safety Application Instruction Set Reference Manual	1756-RM095
Information on installing DeviceNet Safety I/O Modules	DeviceNet Safety I/O Installation Instructions	1791DS-IN001
Information on using DeviceNet Safety I/O Modules	DeviceNet Safety I/O User Manual	1791DS-UM001
Information on the Logix5000 Instruction Set	Logix5000™ General Instruction Set Reference Manual	1756-RM003
Information on programming Logix5000 controllers, including managing project files, organizing tags, programming and testing routines, and handling faults	Logix™ Common Procedures Programming Manual	1756-PM001
Information on using ControlLogix in non-safety applications.	ControlLogix System User Manual	1756-UM001
Information on using the 1756-DNB module in a Logix5000 control system	DeviceNet Modules in Logix5000 Control Systems User Manual	DNET-UM004
Information on using the 1756-ENBT module in a Logix5000 control system	EtherNet/IP Modules in Logix5000 Control Systems User Manual	ENET-UM001
Information on using the 1756-CNB module in Logix5000 control systems	ControlNet Modules in Logix5000 Control Systems User Manual	CNET-UM001
Information on estimating the execution time and memory use for instructions	Logix5000™ Controllers Execution Time and Memory Use Reference Manual	1756-RM087
Information on using RSLogix 5000 Import/Export Utility	Logix™ Import Export Reference Manual	1756-RM084

If you would like a manual, you can:

- download a free electronic version from the internet at **www.rockwellautomation.com/literature**.
- purchase a printed manual by contacting your local Allen-Bradley distributor or Rockwell Automation sales office.

Common Techniques Used in this Manual

The following conventions are used throughout this manual:

- Bulleted lists, such as this one, provide information, not procedural steps.
- Numbered lists provide sequential steps or hierarchical information.
- Italic type is used for emphasis.

Understanding Terminology

The following table defines acronyms used in this manual.

Acronym:	Full Term:	Definition:
1oo2	One Out of Two	Refers to the behavioral design of a multi-processor system.
CIP	Common Industrial Protocol	A communications protocol designed for industrial automation applications.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
EN	European Norm.	The official European Standard
GSV	Get System Value	A ladder logic instruction that retrieves controller status information.
PC	Personal Computer	Computer used to interface with, and control, a Logix system via RSLogix 5000 programming software.
PFD	Probability of Failure on Demand	The average probability of an operational system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of an operational system to have a dangerous failure occur per hour.
RPI	Requested Packet Interval	When communicating over a network, this is the expected rate in time for production of data.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	A ladder logic instruction that sets controller system data.
—	Standard	Any object, task, tag, program, component, etc. in your project that is not a safety-related item (i.e. 'standard' controller refers generically to a ControlLogix controller).

GuardLogix System Overview

This chapter introduces you to the GuardLogix Controller System and provides an overview of the system's safety concept and hardware components.

For the following information	See page
Understand the Safety Concept	1-1
Distinguish Between Standard and Safety Components	1-2
Select GuardLogix System Hardware	1-3
Select Safety I/O	1-5
Communicate Over Networks	1-6
Program Your System	1-7

Understand the Safety Concept

Safety Application Requirements

The GuardLogix Controller system is certified for use in safety applications up to and including Safety Integrity Level (SIL) 3 and Category (CAT) 4 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 criteria.

For SIL 3 and CAT 4 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 number 1756-RM093. You must read, understand, and fulfill these requirements prior to operating a GuardLogix controller-based SIL 3 or CAT 4 safety system.

Safety Application Characteristics

GuardLogix-based safety applications require the use of at least one Safety Network Number (SNN) and a Safety Signature. Both affect controller and I/O configuration and network communications, as discussed later in this manual.

Safety Network Number

The Safety Network Number (SNN) must be a unique number that identifies safety subnets. Each safety subnet that the GuardLogix controller uses for safety communications must have a unique Safety Network Number (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 the Safety Network Number, see 'Manage the Safety Network Number' on page 3-1 of this manual. Also refer to the *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093.

Safety Signature

The Safety Signature consists of an ID number, Date, and Time which uniquely identifies the safety portion of a project. This includes all safety logic, data, and configuration. The GuardLogix system uses the Safety Signature to determine the project's integrity and to allow you to verify that the correct project is downloaded to the target controller. See 'Generate a Safety Signature' on page 5-18 for more information.

Creating, recording, and verifying the Safety Signature is a mandatory part of the safety application development process. Refer to the *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093, for details.

Distinguish 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 **www.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 uses a 'safety' class attribute which is visible whenever Safety Task, safety program, or safety routine properties are displayed.

The GuardLogix controller does not allow writes to safety tag data from external HMI devices or via message instructions from peer controllers. RSLogix 5000 can write safety tag data when the controller is Safety-Unlocked, does not have a Safety Signature, and is operating without any safety faults.

For more information... The *ControlLogix Systems User Manual*, publication number 1756-UM001, provides information on using ControlLogix in standard (non-safety) applications.

HMIs

HMI devices can be used with GuardLogix. HMIs can access standard tags just as with any ControlLogix processor. However, HMIs cannot write to safety tags; safety tags are read-only for HMIs.

Select GuardLogix System Hardware

The GuardLogix controller is made up of a Primary Controller (1756-L6xS) and a Safety Partner (1756-LSP), which function together in a 1oo2 architecture. The GuardLogix system supports SIL 3 and CAT 4 safety applications.

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.

Primary Controller

The Primary Controller, catalog number 1756-L6xS, 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:

- I/O control
- Logic
- Timing
- Counting
- Report generation
- Communications
- Arithmetic Computations
- Data file manipulation

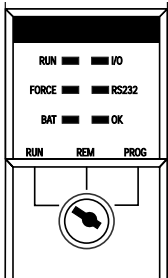
The Primary Controller consists of a central processor, I/O interface and memory. Two different catalog numbers are available with the following memory capacities:

Catalog Number	RAM Capacity	
	Standard Tasks and Components	Safety Task and Components
1756-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB

The GuardLogix controller does not support user program storage or retrieval using CompactFlash.

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.



Safety Partner

The Safety Partner, catalog number 1756-LSP, is a co-processor that provides redundancy for safety-related functions in the system.

The Safety Partner does not have a keyswitch or RS-232 communications port. Its configuration and operation are controlled by the Primary Controller.

For more information... The *GuardLogix Controller Installation Instructions*, publication number 1756-IN045, provides detailed information on installing the Primary Controller and Safety Partner.

Chassis

The chassis provides physical connections between modules and the GuardLogix controller. ControlLogix chassis types are described below.

Catalog Number	Available Slots	Series	Refer to these Installation Instructions
1756-A4	4	B	1756-IN080
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		

Power Supply

ControlLogix power supplies suitable for use in SIL 3 applications include:

Catalog Number	Description	Series	Refer to these Installation Instructions
1756-PA72	AC power supply	C	1756-IN596
1756-PB72	DC power supply		
1756-PA75	AC power supply	B	
1756-PB75	DC power supply		
1756-PA75R ⁽¹⁾	AC power supply (redundant)	A	1756-IN573
1756-PB75R ⁽¹⁾	DC power supply (redundant)		

(1) A 1756-PSCA or 1756-PSCA2 redundant power supply chassis adapter is required for use with redundant power supplies.

No extra configuration or wiring is required for SIL 3 operation of the power supplies.

Select Safety I/O

Safety input and output devices can be connected to DeviceNet Safety I/O, allowing output devices to be controlled by the GuardLogix controller system via DeviceNet Safety communications. The following

table provides an overview of the available DeviceNet Safety I/O modules and lists related documentation.

Catalog Number	Description	I/O Type	User Manual	Installation Instructions
1791DS-IB12	Safety Input Module	12 safe inputs	1791DS-UM001	1791DS-IN001
		4 test outputs		
1791DS-IB8XOB8	Safety Input/Solid-State Output Module	8 safe inputs		
		8 safe outputs		
		4 test outputs		
1791DS-IB4XOW4	Safety Input/Relay Output Module	4 safe inputs		
		4 safe relay outputs		
		4 test outputs		

Communicate Over Networks

The GuardLogix controller supports communications which allow it to:

- control and distribute remote safety I/O on the DeviceNet Safety network
- produce and consume safety tag data between GuardLogix controllers across an Ethernet/IP network or within the same ControlLogix chassis
- access RSLogix 5000 programming software via serial connection or an 1756-ENBT module or 1756-CNB module
- support standard ControlNet communications

The 1756-DNB DeviceNet module provides the interface between the GuardLogix controller and devices on the DeviceNet Safety Network.

1756-ENBT modules provide a communication bridge between two controller pairs via the EtherNet/IP network.

For more information:

- See Chapter 3 of this manual for more information on network communications.
- The *DeviceNet Modules in Logix5000 Control Systems User Manual*, publication number DNET-UM004, provides detailed information on configuring a DeviceNet network, communicating with devices over DeviceNet, troubleshooting, and optimizing network performance.
- The *EtherNet/IP Modules in Logix5000 Control Systems User Manual*, publication number ENET-UM001, provides detailed information on configuring the 1756-ENBT module, interlocking and data transfer between controllers on the EtherNet/IP network, managing connections, and diagnostics.
- The *ControlNet Modules in Logix5000 Control Systems User Manual*, publication number CNET-UM001, provides detailed information on using the 1756-CNB module.

Program Your System

RSLogix 5000 is the programming tool for GuardLogix controller applications. Programs scheduled under the Safety Task, as well as programs in standard tasks, support only ladder logic.

Initially, safety projects do not support:

- Function Block Diagrams (FBD)
- Sequential Function Chart (SFC) Routines
- Structured Text
- Integrated Motion
- Event Tasks
- Equipment Phase Routines
- Redundancy

A safety routine may include only Safety Application Instructions and a specific subset of the standard ladder logic Instruction Set.

For more information...

- The *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093, lists both the Safety Application instructions and the subset of standard ladder logic instructions that are appropriate for safety applications.
- The *GuardLogix Safety Application Instruction Set Reference Manual*, publication number 1756-RM095, provides detailed information on the safety application instructions.
- The *Logix5000™ General Instruction Set Reference Manual*, publication number 1756-RM003, provides details on the standard Logix instructions.
- Chapter 5 of this manual, and the *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093, contain more information on developing safety applications.

Configure the GuardLogix Controller

This chapter provides information on creating a GuardLogix controller project and configuring safety-related parameters.

For information on how to	See page
Create a New Controller	2-1
Set Passwords for Safety-Locking and -Unlocking	2-4
Handle I/O Module Replacement	2-5
Select the CST Master	2-5
Configure Project to Controller Matching	2-6
Configure a Peer Safety Controller	2-7

Create a New Controller

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

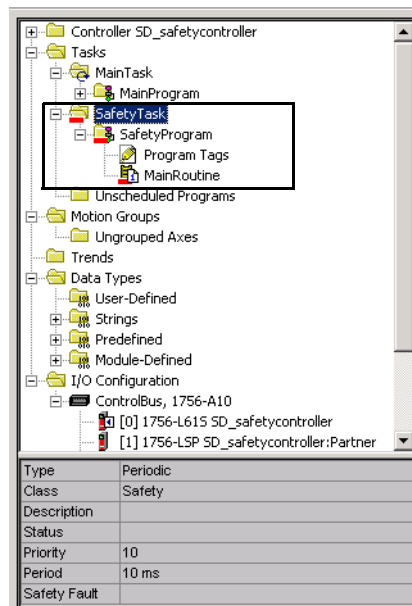
1. Create a new project in RSLogix 5000 by clicking on the *New* button or selecting *New...* from the *File* menu.
2. Specify the general configuration for the controller.

The screenshot shows the 'New Controller' dialog box with the following configuration:

- Vendor: Allen-Bradley
- Type: 1756-L61S ControlLogix5561S Safety Controller
- Revision: 14
- Redundancy Enabled: ☐
- Name: (empty text box)
- Description: (empty text box)
- Chassis Type: 1756-A10 10-Slot ControlLogix Chassis
- Slot: 0
- Safety Partner Slot: 1
- Create In: c:\RSLogix 5000\Projects

- a. Select a GuardLogix controller from the *Type* pulldown menu:
 - 1756-L61S ControlLogix 5561S Controller, or
 - 1756-L62S ControlLogix 5562S Controller
- b. Enter the major revision of firmware for the controller.

- c. 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.
 - d. Select the chassis size.
 - e. Enter the slot number of the controller. The *New Controller* dialog 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 will be prompted to re-enter a valid slot number.
 - f. Specify the folder in which to store the safety controller project.
3. RSLogix 5000 automatically creates a Safety Task and a safety program. A main ladder logic safety routine called 'MainRoutine' is also created within the safety program.

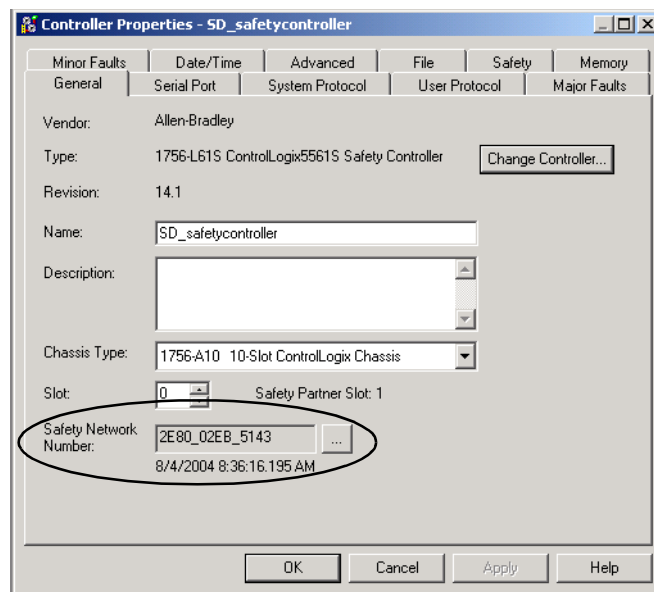


A red bar under the folder icon distinguishes safety components from standard components in the RSLogix 5000 Controller Organizer.

For more information on the Safety Task, safety programs, and safety routines, see Chapter 5, 'Develop Safety Applications'.

4. When a new safety project is created, RSLogix 5000 also automatically creates a time-based Safety Network Number (SNN). This SNN, which represents the time at which the new controller was created, defines the local chassis backplane as a safety subnet. It can be viewed and modified via the *General* tab on the *Controller Properties* dialog, as shown below.

For most applications, this automatic, time-based SNN is sufficient. However, there are cases in which manipulation of SNNs is required. See Chapter 3 for more information on managing the SNN.



TIP

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

See Appendix C, 'Change Controllers', for details on the ramifications of changing controllers.

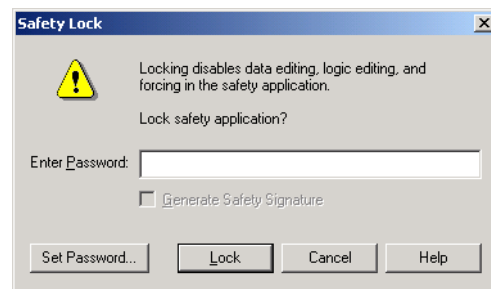
Set Passwords for Safety-Locking and -Unlocking

Safety-Locking the controller protects 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 either online or offline.

The Safety-Lock and -Unlock feature uses two separate passwords. Passwords are optional.

To set passwords:

1. Click on the *Lock/Unlock...* button on the *Safety* tab of the *Controller Properties* dialog, or select *Safety Lock/Unlock...* from the *Tools > Safety* menu to launch the *Safety Lock* dialog.



2. Click on *Set Password...*

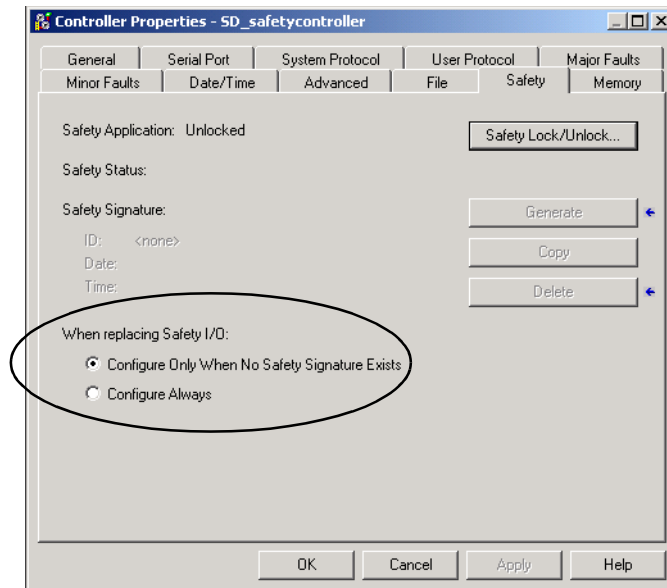


3. Select either *Safety Lock* or *Safety Unlock* from the *What Password* pulldown menu.
4. Enter the old password, if one exists. Then, enter and confirm the new password.

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

Handle I/O Module Replacement

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



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 'Replace a DeviceNet Safety I/O Module' on page 4-11 for more information.

Select the CST Master

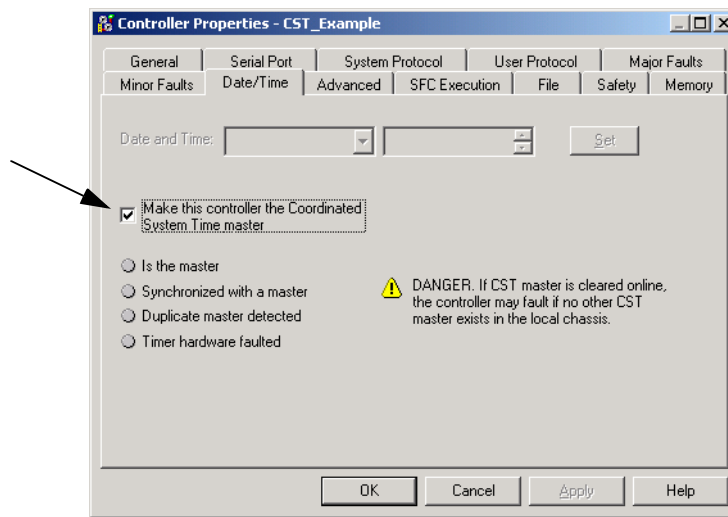
One device in the local chassis must be designated as the Coordinated System Time (CST) master. The CST master should be a GuardLogix controller.

IMPORTANT

If a CST master does not exist, a non-recoverable safety fault will occur when the controller is put into Run mode. See 'GuardLogix Controller Faults' on page 7-6 for more information on faults.

(1) The Safety Signature is a number used by the GuardLogix system to uniquely identify each project's logic, data, and configuration, thereby protecting the system's safety integrity level (SIL). See 'Safety Signature' on page 1-2 and 'Generate a Safety Signature' on page 5-18 for more information.

You can set the controller as the CST master using the *Date/Time* tab on the *Controller Properties* dialog, as shown below.

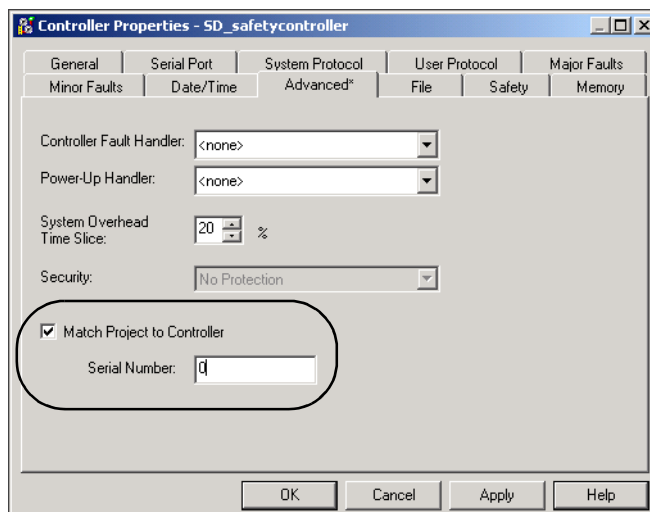


When online, this tab also indicates whether the controller is synchronized with a CST master.

Configure Project to Controller Matching

RSLogix 5000 version 14 and higher allows you to link your project to a specific controller, for the purposes of going online, downloading, and uploading. If you enable this option, each time you initiate one of these activities, RSLogix 5000 checks that the serial number configured in the project matches the serial number of the controller to which it is connected.

To enable this feature, check the Match Project to Controller option on the *Advanced* tab of the *Controller Properties* dialog and enter your controller's serial number.



Configure a Peer Safety Controller

You can add a peer safety controller to the I/O configuration folder of your GuardLogix safety project to allow tags to be consumed.

The peer GuardLogix safety controller is subject to the same configuration requirements as the local GuardLogix safety controller.

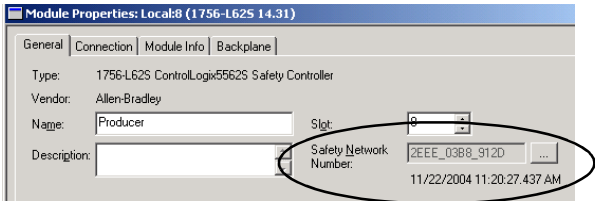
The peer safety controller must also have an SNN. The SNN of the peer safety controller depends upon its placement in the system.

If the peer safety controller is:	Then the peer controller's SNN:
placed in the local chassis	defaults to the local GuardLogix controller's SNN.
the first module configured on the remote network	is a new, time-based SNN.
not the first module configured on the remote network	defaults to the SNN of the lowest addressed module on the remote bus.

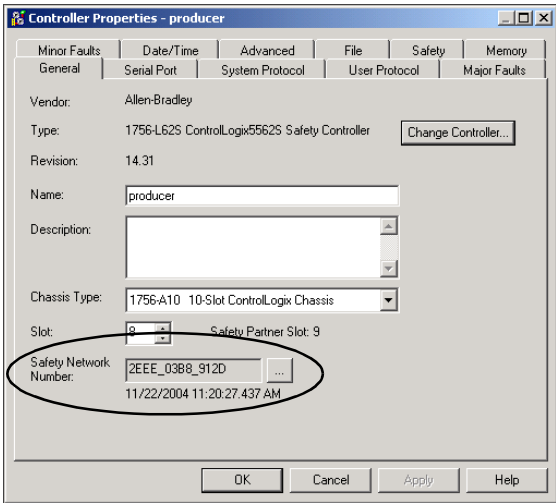
To share data between peer controllers, you produce and consume controller-scoped tags. Produced/consumed tag pairs must be of the same data type. To share data between peer safety controllers, the following additional requirements must be met:

- The SNN entered on the producer controller's *Module Properties* dialog in the consumer's safety project must match the SNN that is configured in the producer controller's project, as shown on the producer controller's *Controller Properties* dialog.


Producer Module Properties Dialog in Consumer Project

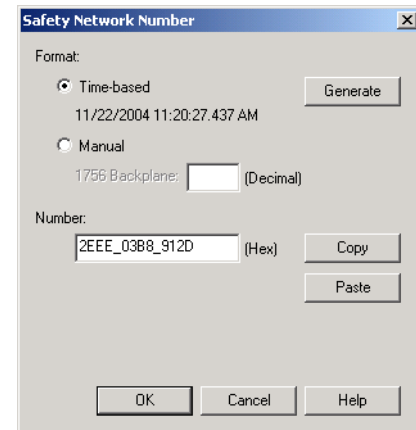


Producer Controller Properties in Producer Project

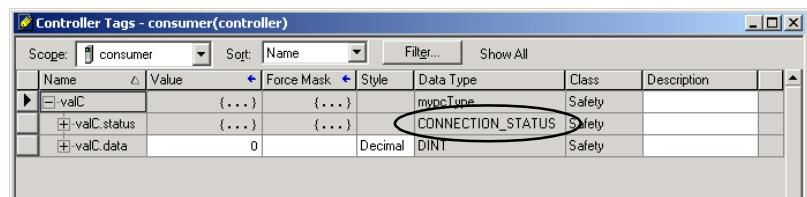


TIP

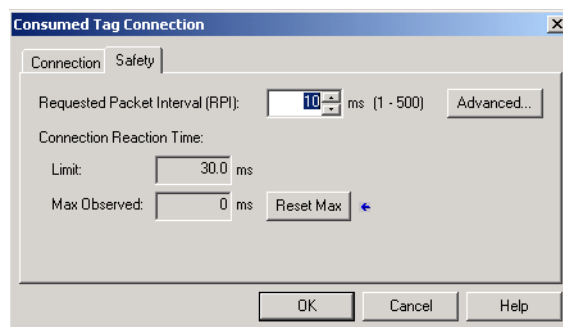
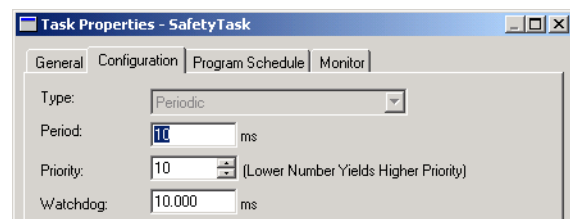
SNNs can be copied and pasted using the buttons on the *Safety Network Number* dialog. Open the respective *Safety Network Number* dialogs by clicking on the  buttons to the right of the SNN fields in the properties dialogs.



- For produced and consumed safety tags, you must create a user-defined data type. The first member of the tag structure must be a pre-defined data type called `CONNECTION_STATUS`, as shown below.



- The RPI of the consumed safety tag must match the Safety Task Period of the producing safety project.

Consumer's Project**Producer's Project**

Set the RPI via the *Safety* tab on the *Consumed Tag Connection* dialog. Open this dialog by right-clicking on the consumed tag and selecting the edit option from the context menu.

To view or edit the Safety Task Period, right-click on the producing Safety Task and select *Properties*. Then, select the *Configuration* tab.

For more information...

- See Chapter 5, 'Develop Safety Applications', for more information on the Safety Task Period and on configuring produced/consumed tags.
- See 'Safety Connections' on page 7-4, for more information on the CONNECTION_STATUS data type.
- Refer to the *Logix5000™ Controllers Common Procedures Programming Manual*, publication number 1756-PM001, for more information on producing and consuming tags and on creating user-defined data types.

Communicate Over Networks

This chapter examines the Safety Network and Safety Network Number (SNN), as well as Ethernet/IP, DeviceNet, and serial communications.

For information about	See page
The Safety Network	3-1
EtherNet/IP Communications	3-6
DeviceNet Communications	3-8
Serial Communications	3-10

The Safety Network

Understand CIP Safety Protocol

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

To maintain high integrity when routing through non-certified bridges, switches, or routers, each end node within a routable CIP Safety Control System must have a unique reference. This unique reference is a combination of a Safety Network Number (SNN) and the Node Address of the network device.

Manage the Safety Network Number

Safety Network Numbers assigned to each safety network or network segment must be unique. You must ensure that unique Safety Network Numbers (SNNs) are assigned to the following:

- each DeviceNet network that contains safety nodes.
- each chassis that contains one or more safety devices.

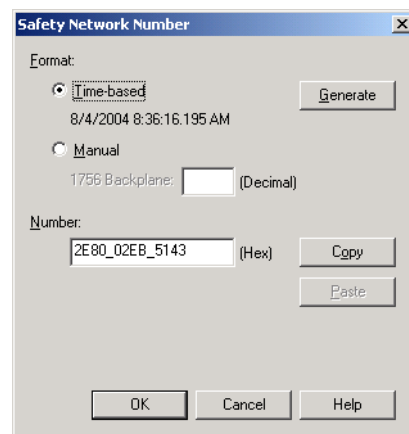
TIP

Multiple SNNs 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 Safety Network Number (SNN) can be either software-assigned (time-based) or user-assigned (manual). These two formats of the SNN are described in the following sections.

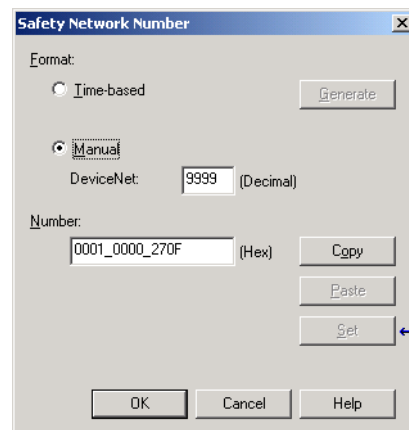
Time-based SNN

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



Manual SNN

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



Assign the SNN

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 node address on that CIP Safety network.

Manual Assignment

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

IMPORTANT

If you assign SNNs manually, take care to ensure that system expansion does not result in duplication of SNN and Node Address combinations.

Automatic vs. Manual

For typical users, the automatic assignment of SNNs is sufficient. However, manual manipulation of SNN's is required in the following situations:


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

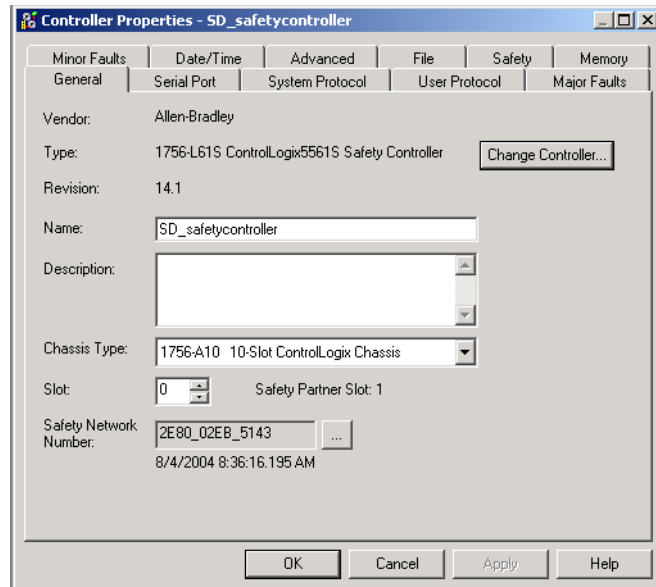
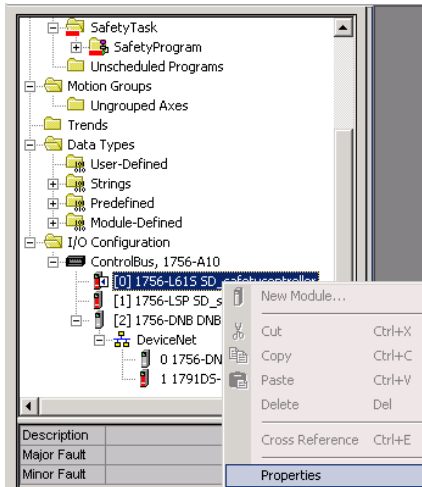
Change the SNN

Before changing the SNN you must:

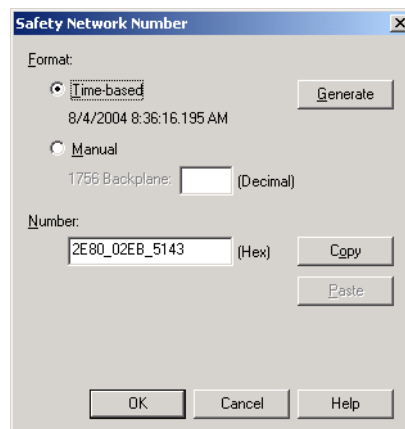
- Unlock the project, if it is safety-locked. See ‘Safety-Lock the Controller’ on page 5-16.
- Delete the Safety Signature, if one exists. See ‘Delete the Safety Signature’ on page 5-19.

Change the SNN of the Controller

1. In the Controller Organizer, right-click on the GuardLogix controller and select *Properties*.
2. On the *General* tab of the *Controller Properties* dialog, press the  button to the right of the *Safety Network Number* to open the *Safety Network Number* dialog.



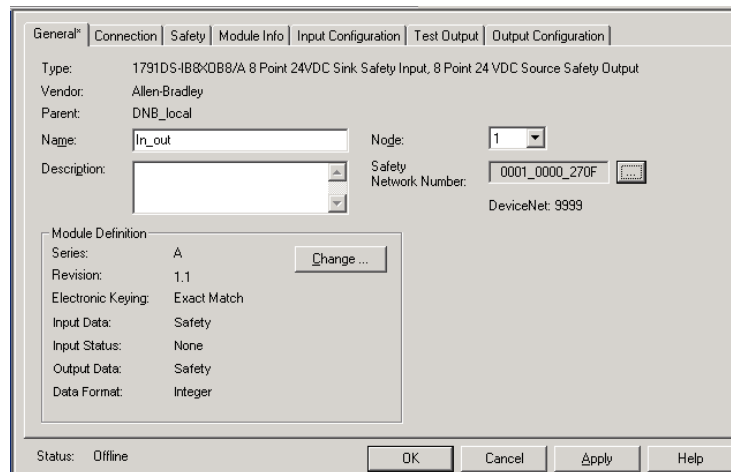
3. Select *Time-based* and press the *Generate* button. Click *OK*.





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

This example uses DeviceNet.

1. Find the first DeviceNet Scanner (1756-DNB) module in the I/O Configuration tree.
2. Expand the I/O modules available through the 1756-DNB.
3. Double-click on the first safety I/O module to view the *General* tab.

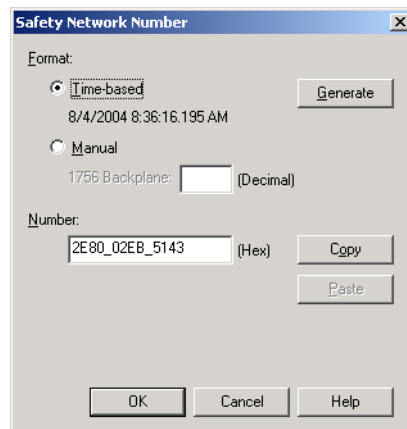



4. Press the  button to the right of the *Safety Network Number* to open the *Safety Network Number* dialog.
5. Select *Time-based* and press the *Generate* button to generate a new SNN for that DeviceNet network. Click *OK*.
6. Press the *Copy* button to copy the new SNN to the Windows[®] Clipboard.
7. Open the *General* Tab of the Module Properties dialog of the next safety I/O module under that 1756-DNB.
8. Press the  button to the right of the *Safety Network Number* to open the *Safety Network Number* dialog.
9. Select *Time-based* and press the *Paste* button to paste that DeviceNet network's SNN into that device. Click *OK*.
10. Repeat steps 7 through 9 for the remaining safety I/O modules under that 1756-DNB.
11. Repeat steps 2 through 9 for any remaining 1756-DNB modules under the I/O Configuration tree.

Copy and Paste an SNN

If the module's configuration is owned by a different 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 for the module.



2. Press the *Copy* button.
3. Go to the *General* tab on the *Module Properties* dialog 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. Press the  button to the right of the Safety Network Number to open the *Safety Network Number* dialog.
5. Press the *Paste* button. Click *OK*.

EtherNet/IP Communications

Produce and Consume Data via EtherNet/IP

The GuardLogix controller supports the ability to produce (broadcast) and consume (receive) system-shared tags over the 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.

For more information...

- See Chapter 5 of this manual for information on configuring produced and consumed safety tags.
- Refer to the *EtherNet/IP Modules in Logix5000 Control Systems User Manual*, publication number ENET-UM001, for guidelines and specific details on interlocking and data transfer between controllers on the EtherNet/IP network.
- Refer to the *Logix5000™ Controllers Common Procedures Programming Manual*, publication number 1756-PM001, for more information on how to produce and consume tags between controllers.

EtherNet/IP in a GuardLogix System

The 1756-ENBT module provides safety interlocking between GuardLogix controllers on an EtherNet/IP network. It interfaces via RJ45, category 5, unshielded, twisted-pair cable and supports half/full duplex 10 Mbps or 100 Mbps operation. The 1756-ENBT supports up to 32 produced/consumed connections.

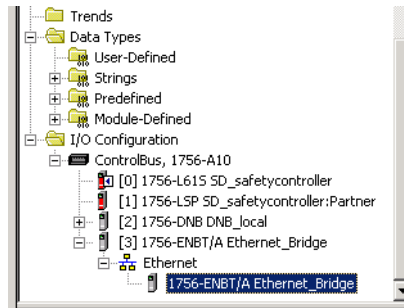
Configure the 1756-ENBT

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

EtherNet/IP Parameter	Description
IP address	<p>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. The following reserved values cannot be used:</p> <ul style="list-style-type: none"> • 127.0.0.1 • 0.0.0.0 • 255.255.255.255
subnet mask	<p>Subnet addressing is an extension of the IP address scheme that allows a site to use a single 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.</p> <p>If you change the subnet mask of an already-configured module, you must cycle power for the change to take effect.</p>
gateway	<p>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.</p>

Add the Module to the Project

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



Download the Project

Use RSLogix 5000 to download the project. When the controller begins operation, it establishes connections with the EtherNet/IP modules.

For more information...

- The *EtherNet/IP Bridge Module Installation Instructions*, publication number 1756-IN019, provides information on how to install 1756-ENBT modules.
- The *EtherNet/IP Modules in Logix5000 Control Systems User Manual*, publication number ENET-UM001, provides specific information on configuring and using the 1756-ENBT in a Logix5000 control system.

DeviceNet Communications

To communicate and exchange data with DeviceNet Safety I/O modules, you need a 1756-DNB module in the local chassis.

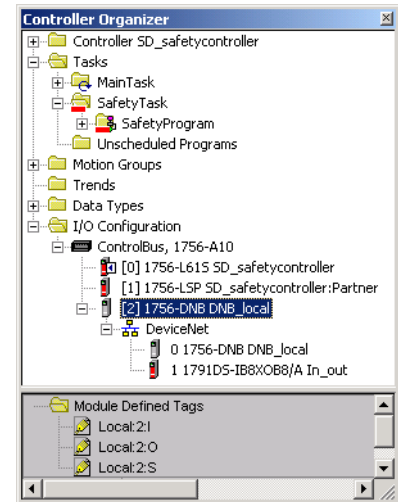
For information on how to install your 1756-DNB module, refer to the *ControlLogix DeviceNet Scanner Module Installation Instructions*, publication number 1756-IN566.

The 1756-DNB supports communication with DeviceNet Safety devices and standard DeviceNet connections. You can use both types, but you must not use standard data in the safety program.

DeviceNet Safety Connections

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

DeviceNet Safety I/O modules are added to the project under the 1756-DNB, as described in Chapter 4, 'Add, Configure, Monitor, and Replace DeviceNet Safety I/O'. When you add a DeviceNet Safety I/O module, RSLogix 5000 automatically creates controller-scoped safety data tags for that module.



For more information... See Chapter 4 for more information on DeviceNet Safety I/O and addressing Safety I/O data.

Standard DeviceNet Connections

If you use standard DeviceNet I/O with your GuardLogix controller, you will 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 to access standard data via DeviceNet, you must use RSNetWorx for DeviceNet to:

- 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 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.

For more information... Refer to the *DeviceNet Modules in Logix5000 Control Systems User Manual*, publication number DNET-UM004, for detailed information on configuring and using the 1756-DNB in a Logix5000 control system.

Serial Communications

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

- 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:

1. Configure the serial communication driver for the workstation.
2. Configure the serial port of the controller. You can select from:

Use this mode:	For:
DF1 point-to-point	<p>communication between the controller and one other DF1-protocol-compatible device.</p> <p>This is the default system mode. This mode is typically used to program the controller through its serial port.</p>
DF1 master mode	<p>control of polling and message transmission between the master and slave nodes.</p> <p>The master/slave network includes one controller configured as the master node and as many as 254 slave nodes. Link slave nodes using modems or line drivers. A master/slave network can have node numbers from 0 to 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).</p>
DF1 slave mode	<p>using a controller as a slave station in a master/slave serial communication network.</p> <p>When there are multiple slave stations on the network, link slave stations 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 to 255 nodes to a single link. In DF1 slave mode, a controller uses DF1 half-duplex protocol.</p> <p>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.</p>
DH-485	<p>communicating with other DH-485 devices multi-master, token passing network allowing programming and peer-to-peer messaging.</p>

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

This chapter provides information on using DeviceNet Safety I/O in a GuardLogix controller system.

For information on how to	See page
Add DeviceNet Safety I/O	4-1
Configure DeviceNet Safety I/O Modules via RSLogix 5000	4-2
Set the Safety Network Number	4-3
Set the Connection Reaction Time Limit	4-4
Understand the Configuration Signature	4-8
Reset Safety I/O Module Ownership	4-8
Address Safety I/O Data	4-9
Monitor Safety I/O Module Status	4-9
Replace a DeviceNet Safety I/O Module	4-11

For more information on installation, configuration, and operation of DeviceNet Safety I/O, refer to the *DeviceNet Safety I/O User Manual*, publication number 1791DS-UM001.

Add DeviceNet Safety I/O

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

- **Node Address**
Set the rotary switches on the module to a value between 0 and 63 or set them from 64 to 99, which allows the node address to be set via an alternate configuration software. You cannot set the node address of an I/O module via RSLogix 5000.
- **Safety Network Number**
See page 4-3 for information on setting the SNN.
- **Configuration Signature**
See page 4-8 for information on when the Configuration Signature is set automatically and when you need to set it.

- Reaction Time Limit

See page 4-4 or refer to the *DeviceNet Safety I/O User Manual*, publication number 1791DS-UM001, for information on setting the reaction time limit.

- Safety Input, Output, and Test Parameters

Refer to the *DeviceNet Safety I/O User Manual*, publication number 1791DS-UM001, and to RSLogix 5000 online help for more information on configuring these parameters.

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

TIP

Safety I/O modules support standard as well as safety data. For standard data configuration, you must use RSNetWorx for DeviceNet software. Refer to the *DeviceNet Safety I/O User Manual*, publication number 1791DS-UM001, for details.

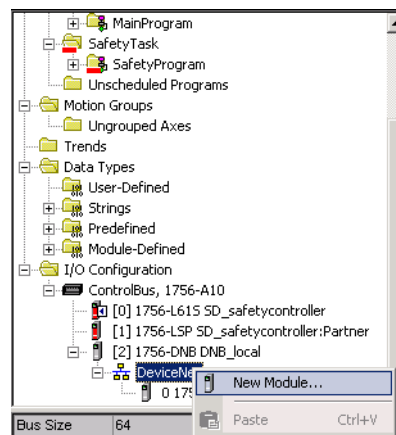
Configure DeviceNet Safety I/O Modules via RSLogix 5000

To communicate with a DeviceNet safety I/O module in your system, you add the module to the 1756-DNB under the I/O Configuration folder of the RSLogix 5000 project.

TIP

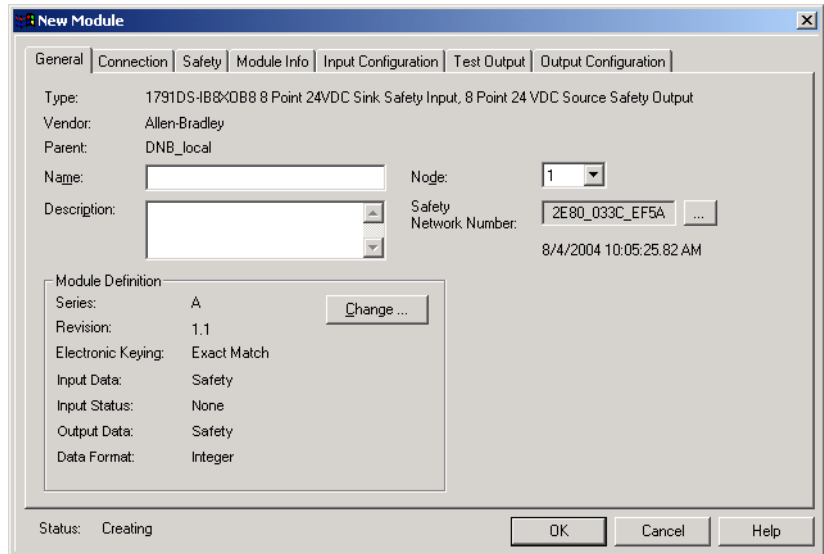
You cannot add or delete a DeviceNet Safety I/O module while online.


1. Right-click on the DeviceNet network and select *New Module....*



2. Expand the *Safety* category and select a DeviceNet Safety I/O module.

3. Specify the module properties.



- Modify the Module Definition settings, if required, by clicking on the *Change...* button.
- Type a name for the new module.
- Enter the node address of the module on its connecting network. Only unused node numbers are included in the dropdown list.
- Modify the Safety Network Number (SNN), if required, by clicking on the  button. See page 4-3 for details.
- Set module configuration parameters using the *Input Configuration*, *Test Output*, and *Output Configuration* tabs.
Refer to RSLogix 5000 online help for more information on DeviceNet Safety I/O module configuration.
- Set the Connection Reaction Time Limit using the *Safety* tab. See page 4-4 for details.

Set the Safety Network Number

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

The DeviceNet Safety I/O module SNN is set in the module the first time that an out-of-box module is connected to the system and prior to the Safety Signature being applied to the controller project.

For most applications, the automatic, time-based SNN is sufficient. However, there are cases in which manipulation of SNNs is required. See 'Assign the SNN' on page 3-3.

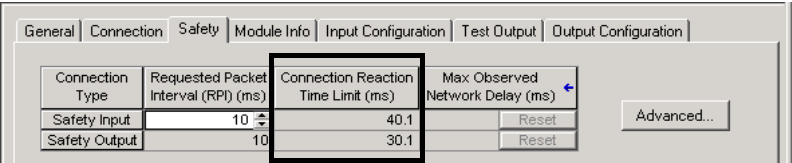
Set the Connection Reaction Time Limit

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

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

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

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



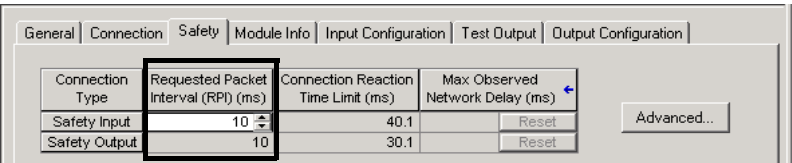
Specify the Requested Packet Interval

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. The RPI is entered in 1 millisecond increments, with a valid range of 1 to 500 ms and a default of 10 ms.

TIP The DeviceNet Safety I/O modules listed on page 1-6 support RPI settings of 6 ms or greater.

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



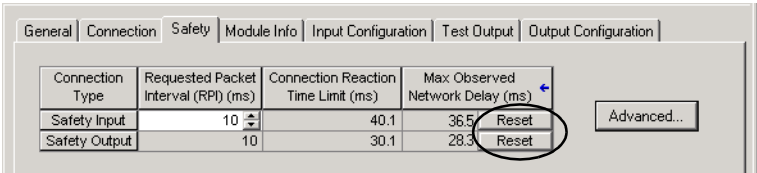
For safety output connections, the RPI is fixed at the GuardLogix Safety Task Period. If the corresponding Connection Time Reaction Limit is not satisfactory, you can adjust the Safety Task Period via the

Safety Task Properties dialog. See ‘Safety Task Period Specification’ on page 5-2 for more information on the Safety Task Period.

For simple timing constraints, setting the RPI is usually sufficient. However, for more complex requirements, use the *Advanced...* button to set the Connection Reaction Time Limit parameters, as described on page 4-6.

Understand the Maximum Observed Network Delay

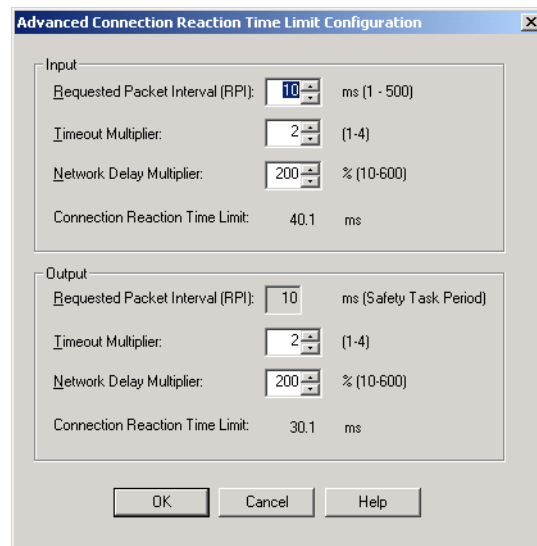
When the GuardLogix controller receives a safety packet, the software records the maximum observed transport delay. The Maximum Observed Network Delay specifies the round trip delay from the producer to the consumer and the acknowledge back to the producer. This Maximum Observed Network Delay value is the result of capturing the age of the data upon the arrival of the message. The Maximum Observed Network Delay is shown on the *Safety* tab of the *Module Properties* dialog. When online, you can reset the Maximum Observed Network Delay by pressing the *Reset* button.



IMPORTANT

The actual Maximum Network Delay time from the producer to the consumer will always be less than the value displayed in the Maximum Network Delay field on the *Safety* tab. Since the CIP safety time coordination is based on a message from the producer to the consumer and all calculations are done in a conservative manner, the actual message delay will be less than the Maximum Network Delay. In general, the actual maximum message delay will be approximately one-half the Maximum Network Delay observed.

Set the Advanced Connection Reaction Time Limit Parameters



The dialog box is titled "Advanced Connection Reaction Time Limit Configuration". It contains two sections: "Input" and "Output". Each section has four parameters with spin buttons and ranges.

Section	Parameter	Value	Range
Input	Requested Packet Interval (RPI)	10	ms (1 - 500)
	Timeout Multiplier	2	(1-4)
	Network Delay Multiplier	200	% (10-600)
	Connection Reaction Time Limit	40.1	ms
Output	Requested Packet Interval (RPI)	10	ms (Safety Task Period)
	Timeout Multiplier	2	(1-4)
	Network Delay Multiplier	200	% (10-600)
	Connection Reaction Time Limit	30.1	ms

Buttons: OK, Cancel, Help

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 using one of the two methods described on page 4-7.

1. Use the ratio between the input RPI and the Safety Task Period. Use this method only under the following conditions:
 - a. If the path or delay is approximately equal to the output path or delay, and
 - b. The input RPI has been configured so that the actual input message transport time is less than the input RPI, and
 - c. 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
Calculating Approximate Output Network Delay Multiplier

If:

Input RPI = 10 ms

Input Network Delay Multiplier = 200%

Safety Task Period = 20 ms

Then the Output Network Delay Multiplier equals:

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

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

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

EXAMPLE
Calculating Network Delay Multiplier from Maximum Observed Network Delay

If:

RPI = 50 ms

Maximum Observed Network Delay = 20 ms

Margin_Factor = 10

Then the Network Delay Multiplier equals:

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

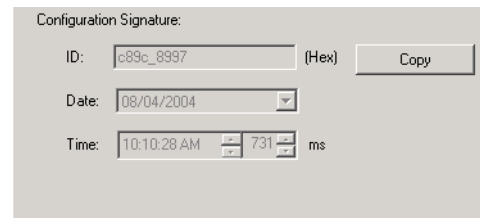
For more information... The *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093, and the *DeviceNet Safety I/O Users Manual*, publication number 1791DS-UM001, also provide information on calculating reaction times.

Understand the Configuration Signature

Each safety device has a unique Configuration Signature, which identifies the module configuration to ensure the integrity of configuration data during downloads, connection establishment, and module replacement. The Configuration Signature is composed of an ID number, a Date and a Time.

Configured Via RSLogix 5000

When the I/O module is configured using RSLogix 5000, the Configuration Signature is generated automatically. You can view and copy the Configuration Signature via the *Safety* tab on the *Module Properties* dialog.



Different Configuration Owner

When the I/O module configuration is owned by a different controller, you must enter the components of the Configuration Signature on the *Safety* tab of the *Module Properties* dialog.

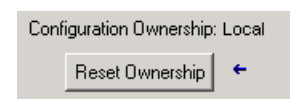
TIP

If the module does not have outputs, you can use the *Paste* button to enter the Configuration Signature.

Reset Safety I/O Module Ownership

When RSLogix 5000 is online, the *Safety* tab of the *Module Properties* dialog 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 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 pressing the *Reset Ownership* button.



TIP

You cannot reset ownership when there are pending edits to the module properties.

Address Safety I/O Data

When you add a module to the I/O configuration folder, RSLogix 5000 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 its name in the system.

A DeviceNet Safety I/O device follows this format:

Modulename:Type.Member

Where	Is	
Modulename	the name of the DeviceNet Safety I/O module	
Type	Type of data	
	Input Module: I	
	Output Module: 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

See Chapter 7 for information on monitoring safety tag data.

For more information... The *Logix5000™ Controllers Common Procedures Programming Manual*, publication number 1756-PM001, provides information on addressing standard I/O modules.

Monitor Safety I/O Module Status

You can monitor system status via the LEDs on the I/O modules and via input and output status codes.

Via LEDs

LEDs on the safety I/O modules indicate system status, as shown below.

LED	Color/State	Description
Module Status (MS)	Off	No power.
	Green, On	Operating under normal conditions.
	Green, Flashing	Device is Idle.
	Red, Flashing	A recoverable fault exists.
	Red, On	An unrecoverable fault exists.
	Red/Green, Flashing	Self-tests in progress.
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.
	Red, On	Communication failure. The device has detected an error which has prevented network communication.
	Red/Green, Flashing	Device is in Communication Faulted state or SNN is being set.
Input Points (INx)	Off	Safety input is OFF.
	Yellow, On	Safety input is ON.
	Red, On	An error has occurred in the input circuit.
	Red, Flashing	When dual channel operation is selected, an error has occurred in the input circuit.
Output Points (Ox)	Yellow, Off	Safety output is OFF.
	Yellow, On	Safety output is ON.
	Red, Flashing	When dual channel operation is selected, an error has occurred in the output circuit.
	Red, On	An error has occurred in the output circuit.
LOCK	Yellow, On	Device configuration is locked.
	Yellow, Flashing	Device configuration is valid, but device is not locked. ⁽¹⁾
	Yellow, Off	Invalid or no configuration data.
IN PWR	Green, On	Input power normal.
	Green, Off	No input power.
OUT PWR	Green, On	Output power normal.
	Green, Off	No output power or output power exceeds the upper/lower limit of the power range.

(1) The device configuration is locked in the controller is the controller is locked or a Safety Signature exists.

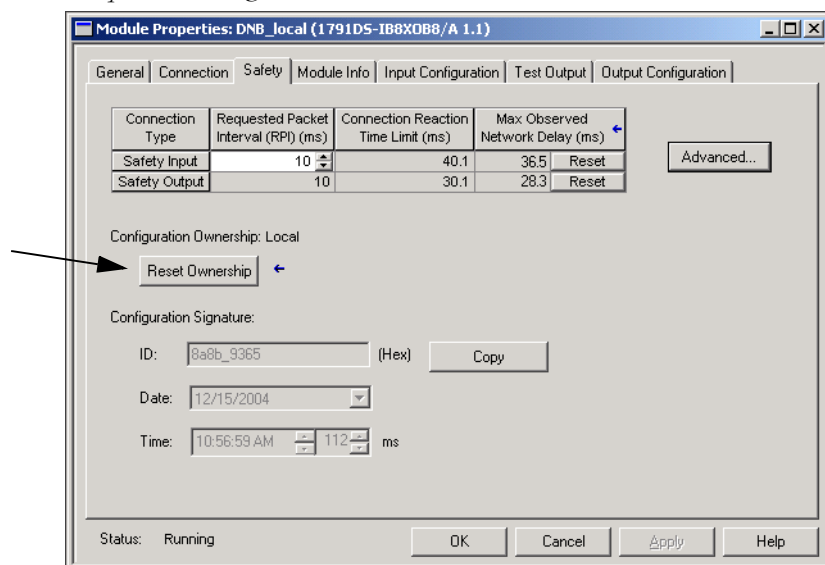
Monitor Input and Output Status Data

You can monitor Safety I/O module status data via explicit messaging. The *DeviceNet Safety I/O User Manual*, publication number 1791DS-UM001, provides information on explicit messaging and I/O module troubleshooting.

Replace a DeviceNet Safety I/O Module

Prepare the I/O Module

1. Set the Node Address of the replacement module.
2. Ensure that the replacement module is of the correct type and in out-of-box condition.
3. You can return the module to the out-of-box condition by selecting the *Reset Ownership* button from the *Safety* tab of the *Module Properties* dialog.



IMPORTANT

You must clear any pre-existing configuration from a safety device prior to installing it on a safety network.

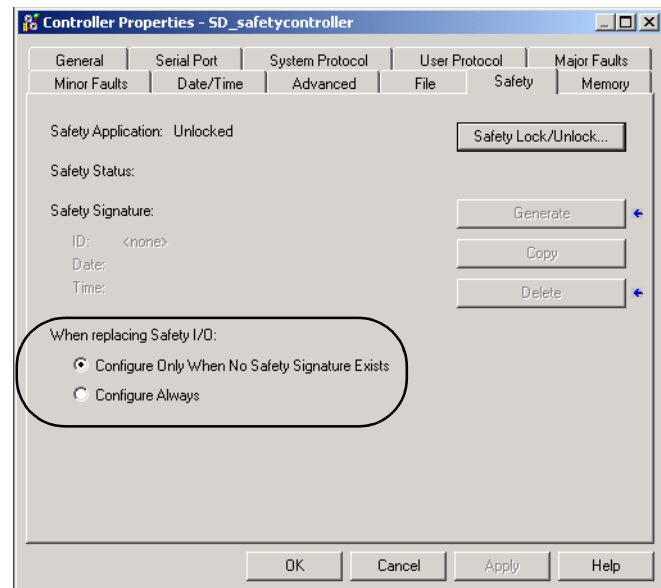
4. If you are relying on a portion of the CIP Safety system to maintain SIL 3 behavior during module replacement and functional testing, follow the 'I/O Replacement with Configure Always Disabled' procedure on page 4-12.

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, the *Configure Always* feature may be

used. Follow the 'I/O Replacement Using Configure Always Feature' procedure on page 4-14.

TIP

The *Configure Always* option is located on the *Safety* tab of the *Controller Properties* dialog.



The default is 'Configure Only When No Safety Signature Exists'.


I/O Replacement with *Configure Always* Disabled

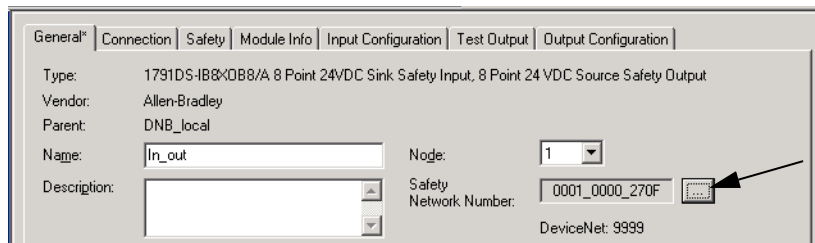
ATTENTION

If other parts of the CIP Safety Control Systems are being relied upon to maintain SIL 3 behavior during the replacement and functional testing of a module, ensure that the *Configure Always* feature is disabled.

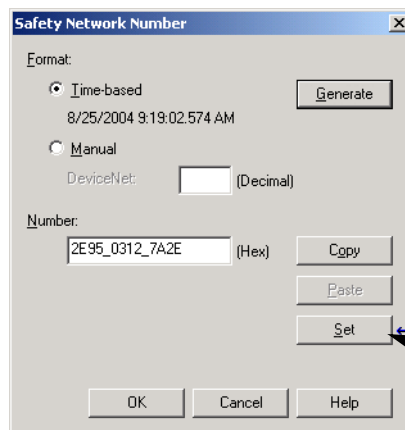
If the project has a Safety Signature and the *Configure Always* feature is disabled, follow the procedure below to replace a module.

1. Remove the old I/O module and install the new module.
2. Restore power to the system if it was removed during replacement.
3. The controller will recognize the replacement module, and announce an 'out-of-box' error.

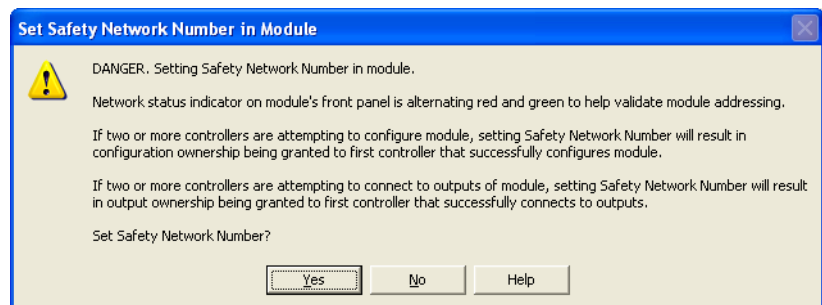
4. Go online to the controller using RSLogix 5000 to set the SNN.
5. Go to the *General* tab of the *Module Properties* dialog for the replaced module.
6. Press the  button to the right of the *Safety Network Number* to open the *Safety Network Number* dialog.



7. Press the *Set* button.



8. The *Set Safety Network Number in Module* confirmation dialog appears. Verify that the Network Status (NS) LED is alternating red/green on the correct module before clicking *Yes* to set the SNN and accept the replacement module.



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

I/O Replacement Using *Configure Always* Feature

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 any modules in the out-of-box condition on any CIP Safety Network when the *Configure Always* feature is enabled, except while following the module replacement procedure below.

When the *Configure Always* feature is enabled in RSLogix 5000, the controller automatically accepts 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.

When a Safety Signature exists and the *Configure Always* feature is enabled, follow the procedure below to replace an I/O module.

1. Remove the old I/O module and install the new module.
2. The controller will recognize, accept, and configure the replacement module.
3. 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

This chapter explains the components that make up a safety project, including the Safety Task, safety programs, safety routines, and safety tags. It also provides information on using features that help protect safety application integrity, such as the Safety Signature and Safety-Locking.

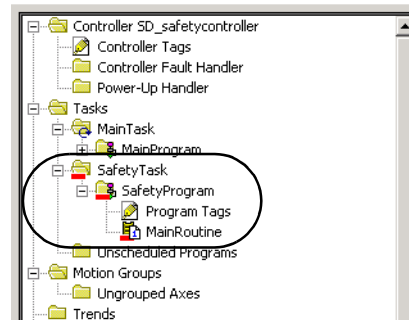
For information about	See page
The Safety Task	5-2
Safety Programs	5-4
Safety Routines	5-4
Safety Tags	5-5
Produced/Consumed Safety Tags	5-9
Safety Tag Mapping	5-14
Safety Application Protection	5-16
Software Restrictions	5-20

For guidelines and requirements for developing and commissioning SIL 3 and CAT 4 safety applications, refer to the *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093. The Safety Reference Manual addresses:

- creating a detailed project specification
- writing, documenting, and testing the application
- generating the Safety 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

The Safety Task

When you create a new safety controller project, RSLogix 5000 automatically creates a single Safety Task with a safety program and a main (safety) routine.

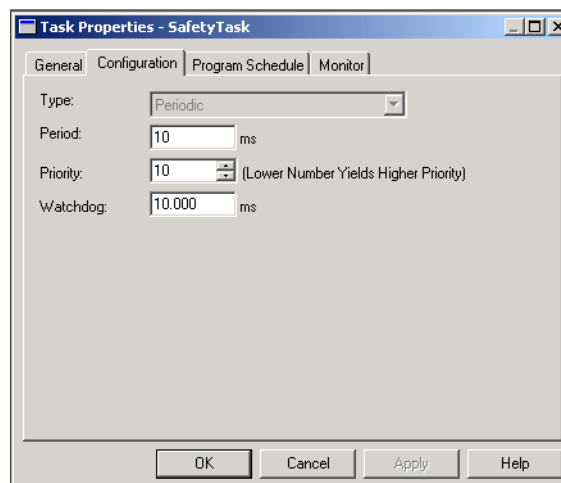


Within the Safety Task, you can schedule multiple safety programs, composed of multiple safety routines. However, the GuardLogix controller supports only a single Safety Task. The Safety Task cannot be deleted or inhibited via programming.

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. Open the dialog by right-clicking on the Safety Task and selecting *Properties*.



The Safety Task should be the controller's top priority. You specify both 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. Ensure that the Safety Task has enough time to finish before it is triggered again. Safety Task Watchdog Timeout, a non-recoverable safety fault in the GuardLogix controller, occurs if the Safety Task is triggered while it is still executing from the previous trigger.

The Safety Task Period and Safety Task Watchdog affect the system reaction time. The *GuardLogix Controller Systems Safety Reference Manual*, publication number 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 have established their control partnership and the Coordinated System Time (CST) is synchronized. However, standard tasks begin executing as soon as the controller transitions to RUN mode.
- Safety input tags and safety-consumed tags are updated at the beginning of Safety Task execution.
- Safety input values are frozen at the start of Safety Task execution. As a result, timer-related instructions (e.g. TON, TOF, etc.) will not include time elapsed during a single Safety Task execution. They will keep accurate time from one task execution to another, but the elapsed time value will not change during the Safety Task execution.
- For standard tags that are mapped to safety tags, the standard tag values are copied into Safety Task memory at the start of Safety Task execution. See page 5-14 for information on safety tag mapping.
- Safety-produced tags are produced at the conclusion of Safety Task execution.
- Safety output tag values are sent to safety outputs 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 may 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 may also define program-scoped safety tags.

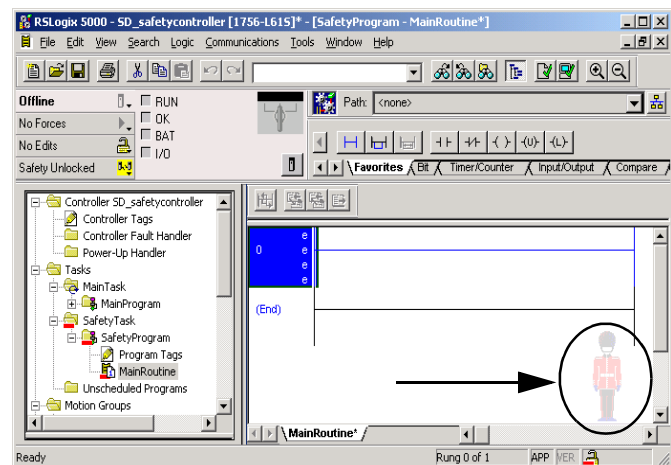
Safety programs cannot contain standard routines or standard tags.

Safety Routines

Safety routines have all the attributes of standard routines, except that they can exist only in a safety program. Only relay ladder logic is supported for safety routines. In addition, safety routines must not attempt to read or write standard tags.

TIP

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



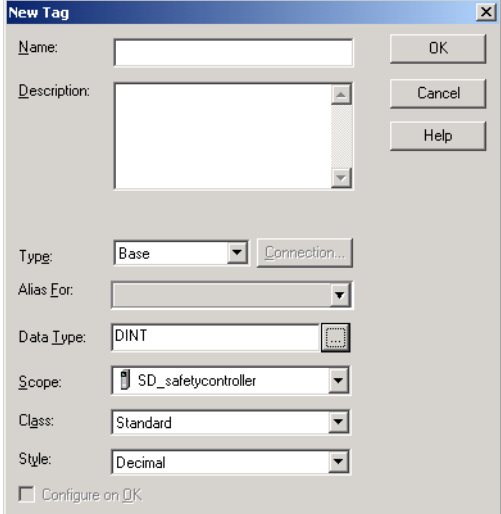
Safety Tags

A tag is a text-based name for 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 to it:

- name
- description (optional)
- tag type
- data type
- scope
- class
- style

Open the *New Tag* dialog by right-clicking on *Controller Tags* or *Program Tags* and selecting *New Tag*.



Tag Type

There are four different types of tags: Base, Alias, Produced, and Consumed.

Tag Type	Description
Base	These tags store value(s) for use by logic within the project.
Alias	<p>A tag that references another tag. An alias tag can refer to another alias tag or a base tag. An alias tag can also refer to a component of another tag by referencing a member of a structure, an array element, or a bit within a tag or member.</p> <p>IMPORTANT: Aliasing between standard and safety tags is prohibited in safety applications.</p>
Produced	A tag that a controller makes available for use by other controllers. A maximum of 15 controllers can simultaneously consume (receive) the data. A produced tag sends its data to one or more consuming tags without using logic. Produced tag data is sent at the RPI of the consuming tag.
Consumed	A tag that receives the data of a produced tag. The data type of the consumed tag must match the data type of the produced tag. The Requested Packet Interval (RPI) of the consumed tag determines the period at which the data updates.

Data Type

The data type defines the type of data that the tag stores, such as bit, integer, floating-point value, string, etc.

Data types can be combined into a structure. A structure is formatted to create 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.

IMPORTANT

You cannot create or delete a user-defined data type while online.

All Logix controllers contain pre-defined data types for use with specific instructions. You can create safety tags of any valid data type. Tags that cannot be used as safety tags are those with the following data types:

- AXIS_CONSUMED
- AXIS_GENERIC
- AXIS_SERVO
- AXIS_SERVO_DRIVE
- AXIS_VIRTUAL
- MOTION_GROUP
- MESSAGE
- COORDINATE_SYSTEM
- REAL

IMPORTANT

This restriction includes user-defined data types that contain any of the above data types.

Scope

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

Controller-Scoped Tags

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

- used in more than one program in the project
 - used in a MSG instruction
 - used to produce or consume data
 - used to communicate with a PanelView terminal
 - used in safety tag mapping
- See 'Safety Tag Mapping' on page 5-14 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, but the safety tag's update rate is based on the execution of the Safety Task.

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

For more information...

- See 'Safety Connections' on page 7-4 for more information on the CONNECTION_STATUS member.
- The *Logix5000 Controllers Common Procedures Programming Manual*, publication number 1756-PM001, provides instructions for creating user-defined data types.

Program-Scoped Tags

When tags are program-scoped, the data is isolated from the other programs. Re-use 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 either standard or safety. Tags classified as safety tags must have a valid data type and must be either controller-scoped or safety-program-scoped.

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.

Produced/Consumed Safety Tags

To transfer safety data between GuardLogix controllers, you use produced and consumed safety tags. Produced and consumed tags require connections which must be configured.

Tag	Connection Description
produced	<p>A produced tag allows other GuardLogix controllers to consume a tag, which means that a controller can receive the tag data from another controller.</p> <p>The local controller (producing) uses one connection for the produced tag and one connection for each consumer. The controller's communication device (i.e. 1756-ENBT) also uses one connection for each consumer.</p>
consumed	<p>A tag that receives the data of a produced tag.</p> <p>Each consumed tag requires one connection for the controller that is consuming the tag. The controller's communication device (i.e. 1756-ENBT) also uses one connection for each consumer.</p>

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

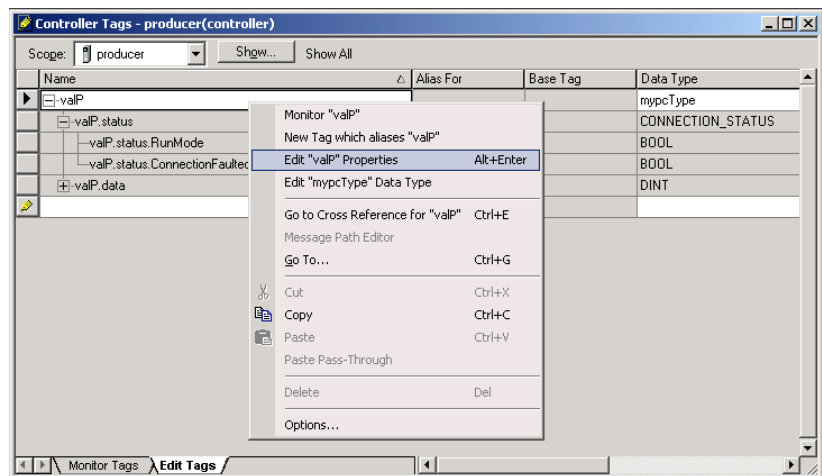
- Only controller-scoped tags can be shared.
- Produced and consumed safety tags are limited to 128 bytes.
- Produced/consumed tag pairs must be of the same user-defined data type.
- The first member of that user-defined data type must be the pre-defined CONNECTION_STATUS data type.
- The RPI of the consumed safety tag must match the Safety Task Period of the producing safety project.

Produce a Safety Tag

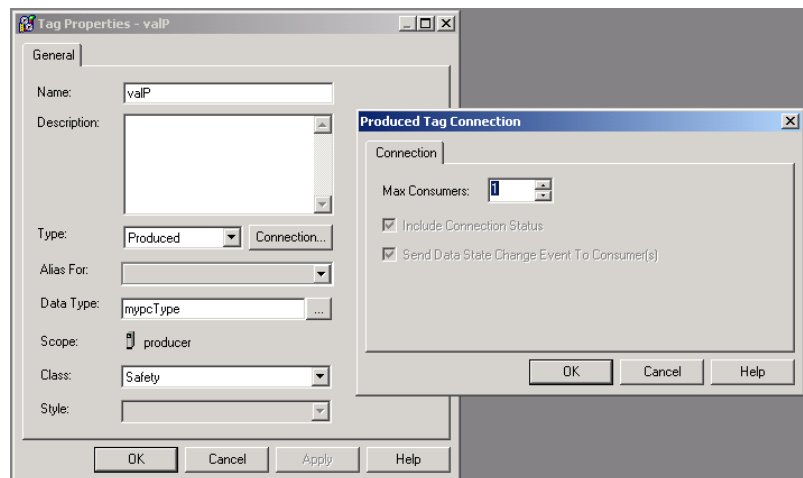
To produce a safety tag:

1. Open the GuardLogix controller project that contains the tag you want to produce.
2. In the Controller Organizer, right-click the *Controller Tags* folder and choose *Edit Tags*.

3. In the *Controller Tags* dialog, right-click on the tag you want to produce and select *Edit Tag Properties*.



4. In the *Tag Properties* dialog, click on the *Connection...* button to open the *Produced Tag Connection* dialog. Enter the number of controllers that will consume (receive) the data.



5. Choose OK.

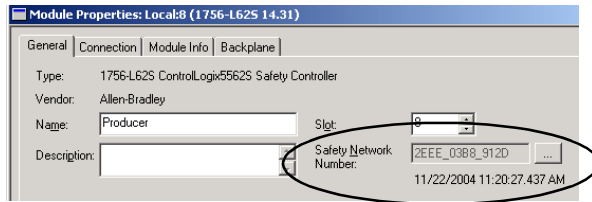
Consume Safety Tag Data

To consume data produced by another controller:

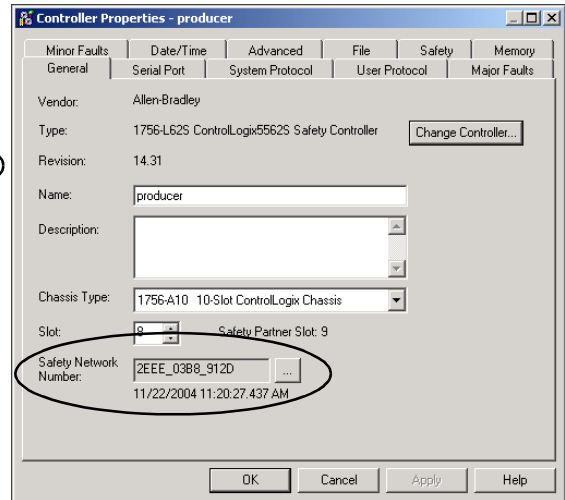
1. Open the GuardLogix project that will consume the data.
2. Add the controller producing the data to the *I/O Configuration* folder.

3. Verify that the SNN shown on the producer controller's *Module Properties* dialog in the consumer's safety project matches the SNN that is configured in the producer controller's project, as shown on the producer controller's *Controller Properties* dialog.

Producer Module Properties Dialog in Consumer Project

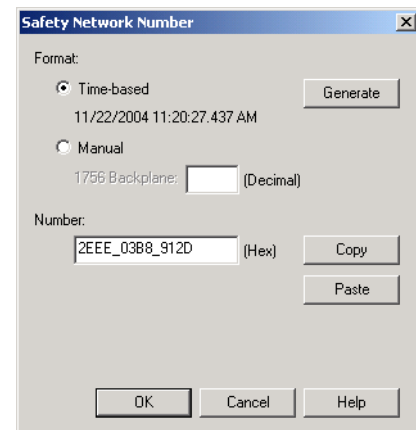


Producer Controller Properties in Producer Project



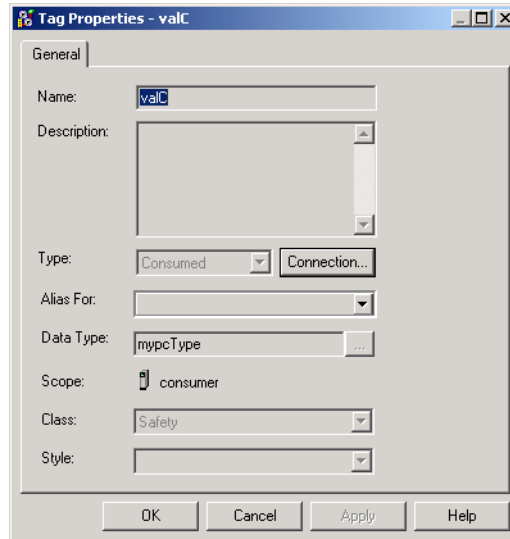
TIP

SNNs can be copied and pasted using buttons on the *Safety Network Number* dialog.

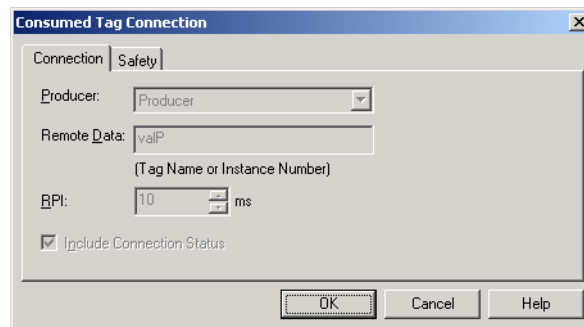


4. In the Controller Organizer, right-click on the *Controller Tags* folder and choose *Edit Tags*.

5. In the *Controller Tags* dialog, right-click on the tag that will consume the data and choose *Edit Tag Properties*. In the *Tag Properties* dialog, click on the *Connection...* button to open the *Consumed Tag Connection* dialog

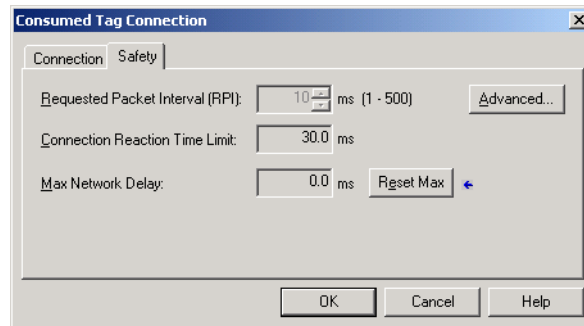


6. Configure the consumed tag connection properties on the *Connection* tab.

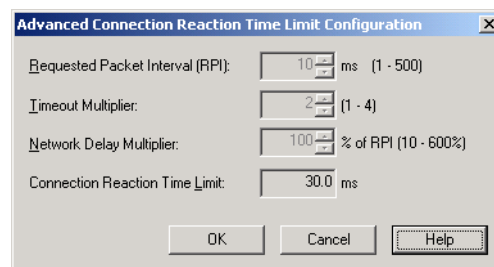


- a. Select the controller that produces the data.
- b. Enter the name of the produced tag.
- c. The RPI specifies the period at which data updates over a connection. The RPI of the consumed safety tag must match the Safety Task Period of the producing safety project. Enter the RPI for the connection in 1 ms increments. The default is 10 ms.

7. Select the *Safety* tab to further refine the timing parameters.



- a. 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. For more complex requirements, set the Advanced Connection Reaction Time Limit parameters as described in step 8.
 - b. 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 using the *Reset Max* button.
8. If the Connection Reaction time limit is acceptable, click *OK*. To set the Advanced Connection Reaction Time Limit parameters, click on the *Advanced...* button.



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

For more information...

- See pages 4-4 through 4-7 for more information on setting the RPI and understanding how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time.
- See Chapter 7 for more information on the CONNECTION_STATUS pre-defined data type.
- The *Logix5000 Controllers Common Procedures Programming Manual*, publication number 1756-PM001, provides instructions for creating user-defined data types.

Safety Tag Mapping

Controller-scoped standard tags cannot be accessed by a safety routine, because the data is not high integrity. To allow standard tag data to be used within the Safety Task's routines, the GuardLogix controller provides a safety tag mapping feature that allows a standard tag value to be copied into the Safety Task's memory at the start of the task's execution.

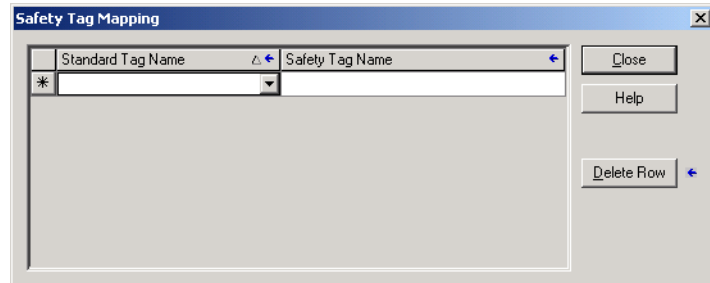
Restrictions

Safety tag mapping is subject to the following 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.
- One safety tag may be mapped to one standard tag.
- Tag mapping cannot be modified when:
 - the project is Safety-Locked.
 - a Safety Signature exists.
 - the keyswitch is in RUN position.
 - a non-recoverable safety fault exists.
 - an invalid partnership exists between the Primary Controller and Safety Partner.

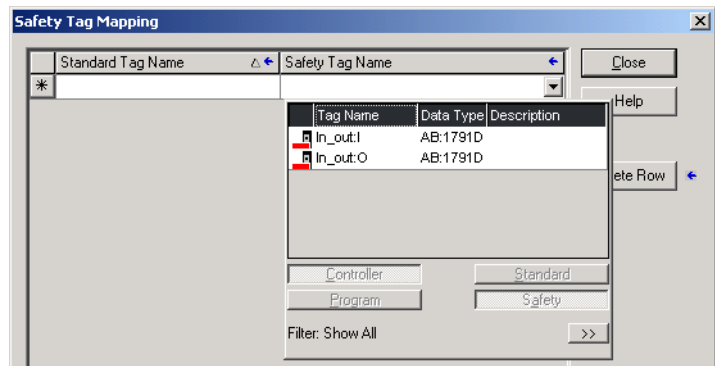
Create Tag Mapping Pairs

1. Select *Map Safety Tags...* from the *Logic* menu to open the *Safety Tag Mapping* dialog.



2. Add an existing tag to either the *Standard Tag Name* or *Safety Tag Name* column by:
 - typing the tag name into the cell, or
 - selecting a tag from the drop-down list.





Clicking on the drop-down arrow displays a filtered tag browser window. 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 either the *Standard Tag Name* or *Safety Tag Name* column by:
 - right-clicking in the empty cell and selecting *New Tag*, or
 - typing the tag name into the cell. Right-click in the cell and select *New 'tagname'*, where 'tagname' is the text you entered in the cell.

Monitor Tag Mapping Status

The left-most column of the *Safety Tag Mapping* dialog indicates the status of the mapped pair, as described below.

Cell Contents	Description
empty	tag mapping is valid
	<p>When offline, the 'X' icon indicates that tag mapping is invalid. You can move to another row or close the Safety Tag Mapping dialog.⁽¹⁾</p> <p>When online, an invalid tag map results in an error message explaining why the mapping is invalid. You cannot move to a different row or close the Safety Tag Mapping dialog if a tag mapping error exists.</p> <p>See the tag mapping restrictions on page 5-14.</p>
	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.

Safety Application Protection

Safety-Lock the Controller

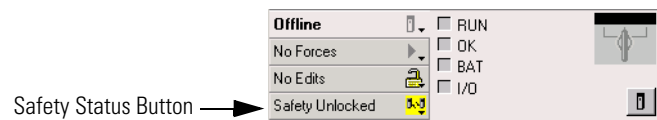
The GuardLogix controller system can be Safety-Locked to protect safety-related control components from modification. The Safety-Lock feature applies only to safety components, such as the Safety Task, safety programs, safety routines, safety tags, Safety I/O, Safety Signature, etc.

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



- Online/offline programming or editing
- Forcing Safety I/O
- Changing the inhibit state of safety I/O or producer controllers
- Data manipulation (except by safety routine logic)
- Generating or deleting the Safety Signature

TIP

The text of the online bar's safety status button indicates the Safety-Lock status:



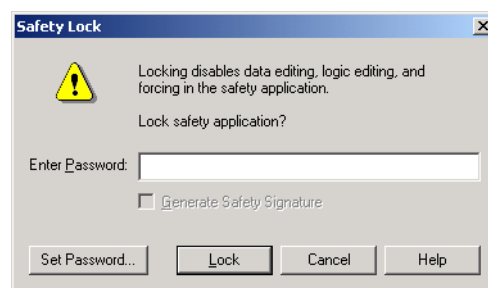
The application tray also displays the following icons to indicate the safety controller's Safety-Lock status:

-  = controller Safety-Locked
-  = controller Safety-Unlocked

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

Safety-Locked or -Unlocked status cannot be changed when the keyswitch is in the RUN position.

You can Safety-Lock and -Unlock the controller from the *Safety* tab of the *Controller Properties* dialog or by selecting *Safety > Safety Lock/Unlock...* from the *Tools > Safety* menu.



If you set a password for the Safety-Lock feature, you must enter it. Otherwise, select *Lock*.

You can also set or change the password from the *Safety Lock* dialog. See page 2-4.

In addition to the Safety-Lock feature described in this section, the standard RSLogix Security measures are also applicable to GuardLogix controller applications. Refer to the *Logix5000 Controllers Common Procedures Programming Manual*, publication number 1756-PM001, for information on RSLogix 5000 Security features.

Generate a Safety Signature

Before verification testing, you must generate the Safety Signature. You can generate the Safety Signature only when the GuardLogix controller is online, in program mode, Safety-Unlocked, and has no safety forces, pending online safety edits, or safety faults. The safety status must equal *Safety Task OK*.

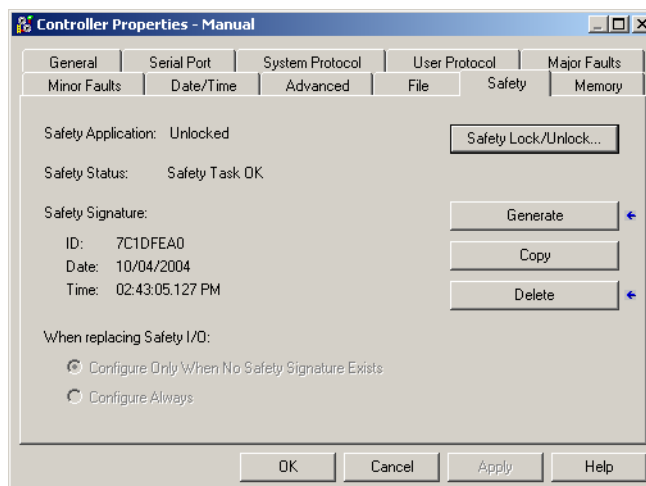
TIP

You can view the safety status via the safety status button on the online bar (see page 7-3) or on the *Safety* tab of the *Controller Properties* dialog, as shown on page 5-18.

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

- Online/offline programming or editing
- Forcing Safety I/O
- Changing the inhibit state of safety I/O or producer controllers
- Data manipulation (except by safety routine logic)

You can generate the Safety Signature from the *Safety* tab of the *Controller Properties* dialog by clicking the *Generate* button. You can also select *Safety > Generate Signature* from the *Tools* menu.



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

Copy the Safety Signature

You can use the *Copy* button to create a record of the Safety Signature for use in safety project documentation, comparison, and validation. When you click on *Copy*, the ID, Date, and Time components are copied to the Windows[®] clipboard.

Delete the Safety Signature

You can use the *Delete* button to delete the Safety Signature only when the controller is Safety-Unlocked. The Safety Signature cannot be deleted when the controller is in Run mode with the keyswitch in RUN.

ATTENTION

If you delete the Safety Signature, you must re-test and re-validate your system to meet SIL 3. Refer to the *GuardLogix Controller Systems Safety Reference Manual*, publication number 1756-RM093, for more information on SIL 3 requirements.

Software Restrictions

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

- the controller is Safety-Locked
- a Safety Signature exists
- safety faults are present
- safety status is:
 - Partner missing
 - Partner unavailable
 - Hardware incompatible
 - Firmware incompatible

If any of the above conditions apply, you may not:

- create new safety objects, including safety programs, safety routines, safety tags, and Safety I/O modules.
- modify existing safety objects, including safety programs, safety routines, safety tags, and Safety I/O modules.

IMPORTANT

The scan times of the Safety Task and any safety programs can be reset when online.

- edit safety routines while online.
- modify safety tag values using the tag monitor.
- apply forces to safety tags.
- create new safety tag mappings.
- modify or delete existing tag mappings.
- modify or delete user-defined data types that are utilized by safety tags.
- modify the controller name, description, chassis type, slot, and Safety Network Number.
- modify or delete the Safety Signature, when Safety-Locked.

Go Online with the Controller

This chapter outlines the process for connecting to the GuardLogix controller and explains the controller features that affect whether or not you can go online.

For information about	see page
Connect the Controller to the Network	6-1
Configure the Network Driver	6-3
Understand the Factors that Affect Going Online	6-4
Download	6-8
Upload	6-10
Go Online	6-11

Connect the Controller to the Network

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

For this network:	Connect the controller via a:
serial	1756-CP3 or 1747-CP3 cable
EtherNet/IP	1756-ENBT module in an open slot in the same chassis as the controller
DeviceNet	1756-DNB module in an open slot in the same chassis as the controller
ControlNet	1756-CNB module in an open slot in the same chassis as the controller

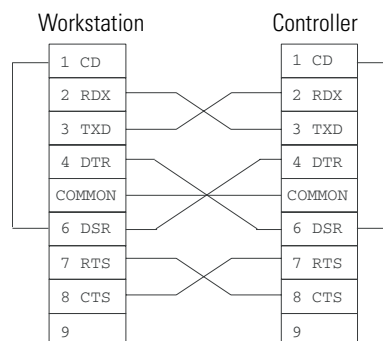
Connect the Controller via a Serial Network

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

TIP

If you make your own cable:

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



You can also use a 1747-CP3 cable from the SLC product family, but once the cable is connected, you cannot close the controller door.

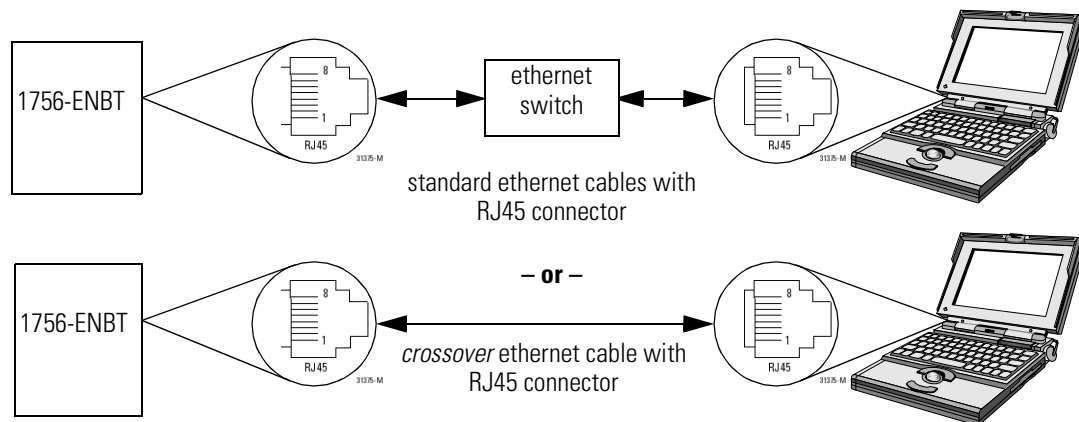
Connect Your EtherNet/IP Device and Computer

WARNING



If you connect or disconnect the communications 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.

Connect your EtherNet/IP device and computer using ethernet cable.



Connect Your DeviceNet Scanner or ControlNet Communication Module and Your Computer

To access either the DeviceNet network or the ControlNet network, you can:

- connect directly to the network,
- or
- connect to a serial or EtherNet/IP network and browse (bridge) to the desired network. This requires no additional programming.

Configure the Network Driver

RSLinx[®] software handles communication between GuardLogix controllers and RSLogix 5000 software. To communicate with the controller (e.g. download, monitor data), configure RSLinx software for the required communication.

For this network:	Configure this driver:
serial	RS-232 DF1 Devices
EtherNet/IP	EtherNet/IP Driver or Ethernet Devices
DeviceNet	DeviceNet Drivers...
ControlNet	ControlNet Drivers

Configure a Serial Communications Driver

1. Start RSLinx software.
2. From the *Communications* menu, select *Configure Drivers*.
3. From the *Available Driver Types* list, select the driver.
4. Click *Add New*.
5. Click *OK* to accept the default name for the driver.
6. From the *Comm Port* drop-down list, select the serial port (on the workstation) to which the cable is connected.
7. From the *Device* dropdown list, select *Logix5550 Serial Port*.
8. Click *Auto-Configure*.

9. Does the dialog box display the following message?

“Auto Configuration Successful!”

If:	Then:
Yes	Click <i>OK</i> .
No	Go to step 6 and verify that you selected the correct Comm Port.

10. Click *Close*.

Configure an EtherNet/IP, DeviceNet, or ControlNet Driver

For information on configuring an EtherNet/IP or DeviceNet driver, refer to the appropriate publication:

- *EtherNet/IP Modules in Logix5000 Control Systems*, publication number ENET-UM001.
- *DeviceNet Modules in Logix5000 Control Systems*, publication number DNET-UM004.
- The *ControlNet Modules in Logix5000 Control Systems User Manual*, publication number CNET-UM001.

Understand the Factors that Affect Going Online

RSLogix 5000 determines whether you can go online with a target controller based on whether the offline project is new or whether changes have occurred in the offline project. If the project is new, you must first download the project to the controller. If changes have occurred to the existing project, you will be prompted to upload or download. If no changes have 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 between the Primary Controller and Safety Partner, the existence of a Safety 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 all projects, both standard and safety.

If the Project to Controller Match feature is enabled in the offline project, RSLogix 5000 compares the serial number of the controller in the offline project to that of the connected controller. If they do not match, you must either:

- cancel the download/upload,
- connect to the correct controller,
or
- confirm that you are connected to the correct controller, which will update 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

Firmware upgrades can also be performed via the *Tools > ControlFlash* menu in RSLogix 5000.

Safety Partner Status/Faults

Upload of program logic and going online is allowed regardless of safety status. Safety status affects the download process only, as described in the table below.

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

Safety Status/Fault Condition	Action Required
Safety partner is missing or unavailable.	Install a compatible Safety Partner.
Safety partner hardware is incompatible with Primary Controller.	Install a compatible Safety Partner.
Safety partner firmware is incompatible with the Primary Controller.	Update the Safety Partner with the correct firmware revision. The Safety Partner's firmware revision must be an exact match to the Primary Controller's.
Safety Status OK.	None. The software proceeds to check for the existence of a Safety Signature in the offline project. See 'Safety Signature and Safety-Locked/-Unlocked Status' below.
Safety Task Inoperable.	

Safety Signature and Safety-Locked/-Unlocked Status

On Upload

If the controller contains a Safety Signature, it is uploaded with the project. The Safety Lock status of the uploaded project is set to that of the online project. For example, if the online project was Safety-Unlocked, it remains Safety-Unlocked following the upload, even if the offline project was locked prior to the upload.

Following an upload, the Safety Signature also matches the status of the uploaded project. If a Safety Signature existed in the offline project, but there is no Safety Signature in the controller, the offline Safety Signature is deleted during the upload.

On Download

For safety projects, the existence of a Safety Signature in the controller, as well as the controller's Safety-Lock status, determines whether or not a download can proceed. Following a successful download, the controller's Safety-Lock status is set to the original value of the offline project.

The possible combinations of Safety Signature and controller Safety-Locked status are described, along with the resulting download functionality, in the table below.

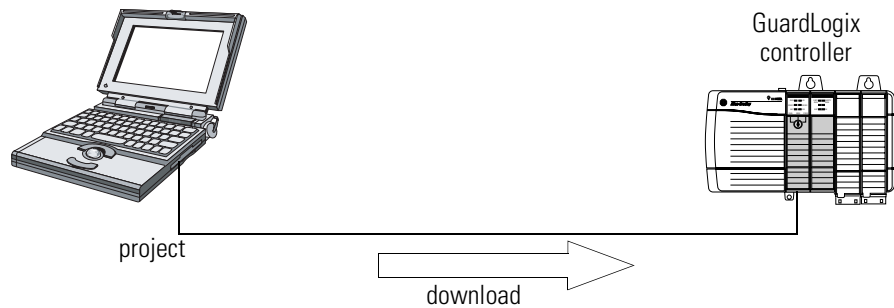
Safety-Lock Status	Safety Signature Status	Download Functionality
Controller Safety-Unlocked	Safety Signature in the offline project matches the Safety Signature in the controller.	The standard application is downloaded and the Safety application is re-initialized via the Safety Signature. Safety tags are re-initialized to the values they had when the Safety Signature was created.
	Safety Signatures <i>do not</i> match, or either the controller or the offline project do not have a Safety Signature.	If the controller had a Safety Signature, it is deleted. Safety and standard applications are downloaded. If an offline Safety Signature exists, it is downloaded to the controller. Safety tags are re-initialized to the values they had when the Safety Signature was created.
	The firmware revision of the offline project is incompatible with the controller.	You must either: <ul style="list-style-type: none"> • proceed with the download. IMPORTANT: Downloading in this condition will clear the Safety Signature and the system will require re-validation. or • install a controller whose firmware major and minor revisions exactly match the offline project and then download the offline project. This will preserve the Safety Signature.
Controller Safety-Locked	Safety Signature in the offline project matches the Safety Signature in the controller.	Download is allowed. However, if the offline project is Safety-UnLocked, you must first Safety-Unlock the controller. Locked status and safety passwords are set to the offline values. The safety application is re-initialized via the Safety Signature.
	Safety Signatures <i>do not</i> match or either the controller or the offline project does not have a Safety Signature.	You must first Safety-Unlock the controller to allow the download to proceed. Refer to the Controller Safety-Unlocked portion of this table for download functionality.
	The firmware revision of the offline project is incompatible with the controller.	

IMPORTANT

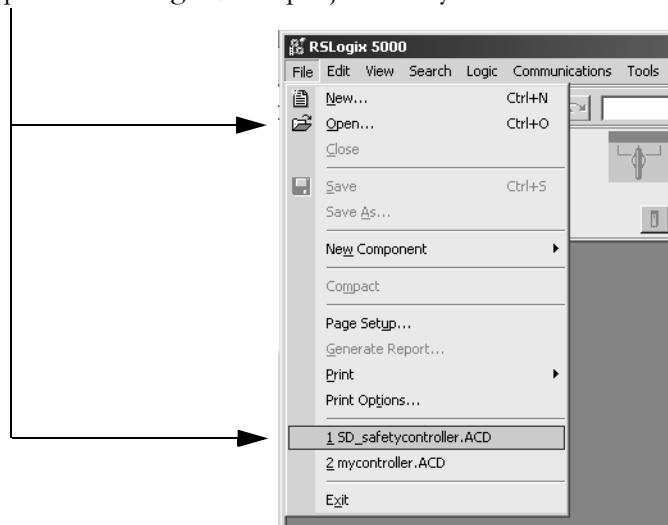
During a download to a controller that is Safety-Unlocked, the controller's status will be set to the Safety-Locked or -Unlocked value of the offline project.


Download

download – transfer a project from your computer to your controller so you can execute its logic.



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 the *Who Active* button .
 - 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 on the *Download* button.
5. 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 between the Primary Controller and Safety Partner
 - Safety Signature (if one exists)
 - Safety-Lock status

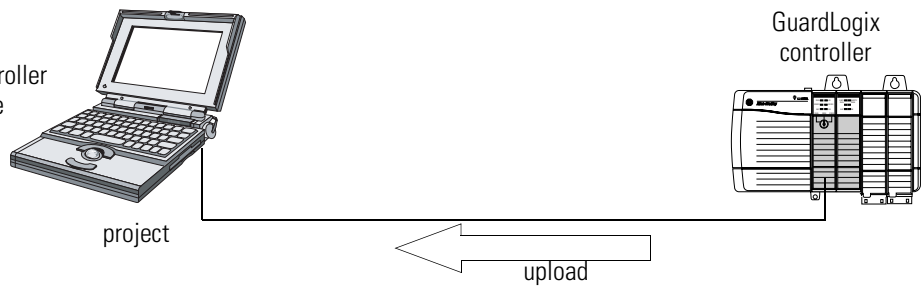
6. Follow the directions in the table below to complete the download based on the software's response to the comparisons listed in step 5.


If the software indicates	Then
Download to the controller.	Choose <i>Download</i> . The project downloads to the controller and RSLogix 5000 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 by selecting the <i>Update project serial number</i> ... checkbox to allow the download to proceed. The project serial number will be 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.	Select <i>Update Firmware</i> . Select the required revision and click on <i>Update</i> . Confirm your selection by clicking <i>Yes</i> .
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. Select <i>Update Firmware</i> . Select the required revision and click on <i>Update</i> . Confirm your selection by clicking <i>Yes</i> .
Unable to download to controller. Incompatible Safety Signature cannot be deleted while the project is safety-locked.	Cancel the download. To download the project, you must either: <ul style="list-style-type: none"> • Download to a controller with firmware revisions that match the Safety Signature, or • Safety-Unlock the offline project, delete the Safety Signature, and then download the project. <p>IMPORTANT: The safety system will require re-validation.</p>
Cannot download in a manner that preserves safety signature. Controller's firmware minor revision is not compatible with Safety Signature in offline project.	<ul style="list-style-type: none"> • If the firmware minor revision is incompatible, to preserve the safety signature, update the firmware revision in the controller to exactly match the offline project. Then download the offline project. • To proceed with the download despite the Safety Signature incompatibility, click <i>Download</i>. The Safety Signature will be deleted. <p>IMPORTANT: The safety system will require re-validation.</p>
Unable to download to controller. Controller is locked. Controller and offline project Safety Signatures do not match.	Select <i>Unlock</i> . The <i>Safety Unlock for Download</i> dialog appears. If the <i>Delete Signature</i> checkbox is selected and you choose <i>Unlock</i> , you must confirm the deletion by selecting <i>Yes</i> .

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

Upload

upload – transfer a project from a controller to your computer so you can monitor the project.



1. Define the path to the controller:
 - a. Click the *Who Active* button .
 - 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 on the *Upload* button.
3. If the project file does not already exist, create the project file on your computer by choosing *Select File....*, then *Select* and *Yes*. If the project file exists, select it.
4. If the project to controller match is enabled, RSLogix 5000 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:

- Cancel the upload and connect to a matching controller. Then, start the upload procedure again.
 - Select a new project to upload into or select a different project by choosing *Select File....*
 - Update the project serial number to match the controller by checking the *Update Project Serial Number* checkbox and selecting *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. If there are no changes in the offline project, you can go online without uploading. Select *Go Online*.

If there are changes in the open project that are not present in the controller, you can choose to upload the project, cancel the upload, or select a different file.

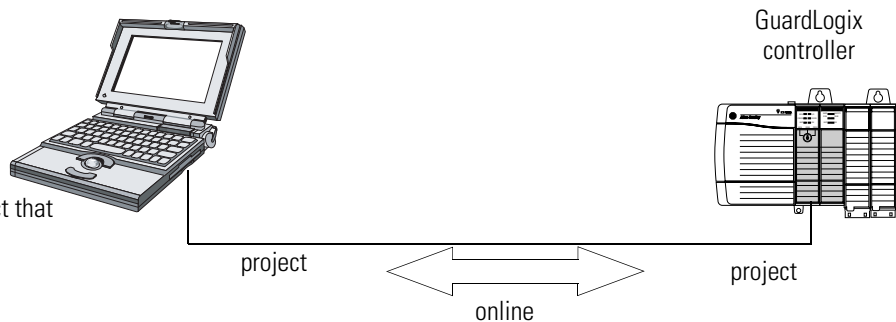
7. If you select *Upload*, the standard and Safety applications are uploaded. If a Safety Signature exists, it is also uploaded. The Safety-Lock status of the project reflects the original status of the online (controller) project.

TIP

Prior to the upload, if an offline Safety Signature exists, or the offline project is Safety-Locked but the controller is Safety-Unlocked or has no Safety Signature, the offline Safety Signature and Safety-Locked state will be replaced by the online values (Safety-Unlocked with no Safety Signature). If you do not want to make these changes permanent, do not save the offline project following the upload.

Go Online

online – monitor a project that a controller is executing.



1. Define the path to the controller:

- a. Click the *Who Active* button .
- 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 on the *Go Online* button.

3. The software checks:

- whether the offline project and controller serial numbers match (if Project to Controller Match is selected).
- whether the offline project contains changes that are not in the controller project.
- whether the revisions of the offline project and controller firmware match.
- whether the offline project or the controller are Safety-Locked.
- whether the offline project or the controller have compatible Safety Signatures.

4. Follow the directions in the table below to connect to the controller based on the software's response to the checks listed in step 3.

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 a different project file, or select the <i>Update project serial number ...</i> checkbox and choose <i>Go Online...</i> to connect to the controller and update the offline project serial number to match the controller.
Unable to connect to controller. The revision of the offline project and the controller's firmware are not compatible.	Choose one of the following options: <ul style="list-style-type: none"> • Select <i>Update Firmware</i>. Select the required revision and click on <i>Update</i>. Confirm your selection by clicking <i>Yes</i>. IMPORTANT: The online project will be deleted. • To preserve the online project, cancel the online process and install a version of RSLogix 5000 that is compatible with the firmware revision of your controller.
You need to upload or download in order to go online using the open project.	Choose one of the following options: <ul style="list-style-type: none"> • <i>Upload</i> to update the offline project (see page 6-10), • <i>Download</i> to update the controller project (see page 6-9), or • <i>Select File</i> to choose a different offline project.
Unable to connect in a manner that preserves safety signature. Controller's firmware minor revision is not compatible with Safety Signature in offline project.	<ul style="list-style-type: none"> • To preserve the safety signature when the firmware minor revision is incompatible, update the firmware revision in the controller to exactly match the offline project. Then go online to the controller. • To proceed with the download despite the Safety Signature incompatibility, click <i>Download</i>. The Safety Signature will be deleted. IMPORTANT: The safety system will require re-validation.
Unable to connect to controller. Incompatible Safety Signature cannot be deleted while project is Safety-Locked.	Cancel the online process. You must Safety-Unlock the offline project before attempting to go online.

5. When the controller and RSLogix 5000 are online, the Safety-Locked status and Safety Signature of the controller match the controller's project. The Safety-Lock status and Safety Signature of the offline project are overwritten by the controller. If you do not want the changes to the offline project to be permanent, do not save the project file following the go online process.

Monitor Status and Handle Faults

This chapter covers options for monitoring controller, connection, and system status, and provides guidelines for developing fault routines.

For information about	see page
Monitor Controller Status	7-1
Monitor Connections	7-4
Monitoring Safety Status	7-5
GuardLogix Controller Faults	7-6
Developing a Fault Routine	7-8

Monitor Controller Status Controller LEDs

Primary controller and Safety Partner status is indicated via LEDs, as described below.

LED	Color/Status	Primary Controller Description	Safety Partner Description
RUN	Off	No user tasks running. Controller is in PROGram mode.	Not applicable.
	Green	Controller is in RUN mode.	Not applicable.
SAFE RUN	Off	Not applicable.	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	Not applicable.	The user Safety Task and safety outputs are enabled. The safety application is executing at its periodic rate.
FORCE	Off	No forces, standard or Safety, are enabled on the controller.	Not applicable.
	Amber	Standard and/or Safety forces have been enabled.	Not applicable.
	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.	Not applicable.
BAT	Off	Battery is able to support memory.	Battery is able to support memory.
	Red	Battery is not able to support memory.	Battery is not able to support memory.

LED	Color/Status	Primary Controller Description	Safety Partner Description
OK	Off	No power is applied.	No power is applied.
	Green	Controller is powered-up with no faults.	Safety partner is powered-up with no faults.
	Red, Flashing	Non-recoverable fault or recoverable fault not handled in the fault handler. All user tasks, both standard and Safety, are stopped.	Not applicable.
	Red	Powering up or non-recoverable controller fault.	Powering up or non-recoverable controller fault.
I/O ⁽¹⁾	Off	No activity. No I/O is configured.	Not applicable.
	Green	Controller is communicating to all configured I/O devices, both standard and Safety.	Not applicable.
	Green, Flashing	One or more I/O devices is not responding.	Not applicable.
	Red, Flashing	Controller is not communicating to any configured I/O.	Not applicable.
RS232	Off	There is no activity.	Not applicable.
	Green	Data is being received or transmitted.	Not applicable.
SAFETY TASK	Off	Not applicable.	No partnership established. Primary controller is missing, is not functioning properly, or its firmware revision is incompatible with that of the Safety Partner.
	Green	Not applicable.	Safety controller status is 'OK'. The Coordinated System Time (CST) is synchronized and I/O connections are established.
	Green, Flashing	Not applicable.	Safety controller status is 'OK'. The Coordinated System Time (CST) is not synchronized on either the Primary Controller or the Safety Partner.
	Red	Not applicable.	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	Not applicable.	Safety controller status is 'Inoperable'.

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

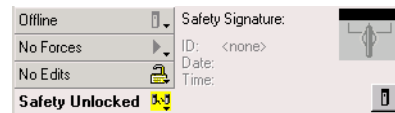
Online Bar

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



When the *Controller Status* button is selected as shown above, the online bar shows the controller's mode (RUN) and status (OK). The BAT LED indicator combines the status of both the Primary Controller and the Safety Partner. If either or both have a battery fault, the LED illuminates. The I/O LED combines the status of both standard and Safety I/O and behaves just like the LED on the controller. The I/O with the most significant error status is displayed next to the LED.

When the *Safety Status* button is selected as shown below, the online bar displays the Safety Signature.



The *Safety Status* button itself indicates whether the controller is Safety-Locked or -Unlocked, or faulted. It also displays an icon that shows the safety status as described below.

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 Signature exists, the icon includes a small check mark.



Monitor Connections

All Connections

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

- The I/O LED 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 for the module
 - the GSV instruction

ATTENTION

Safety I/O and produce/consume connections cannot be configured to fault the controller when a connection is lost. Therefore, if you need to detect a system fault to ensure that the safety system maintains SIL 3, you must monitor the CONNECTION_STATUS bits. See 'Safety Connections' on page 7-4.

Safety Connections

For tags associated with produced or consumed safety data, you can monitor the status of safety connections 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 7.1 Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation is
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.

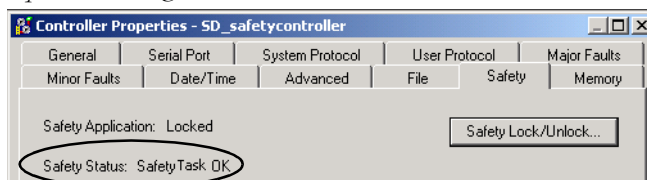
If a module is inhibited, the ConnectionFaulted bit is set to Faulted (1) and the RunMode bit is set to Idle (0) for each connection associated with the module. As a result, safety consumed data is reset to zero.

Monitor Status Flags

All Logix controllers, including GuardLogix, support status keywords that you can use in your logic to monitor specific events. For more information on how to use these keywords, refer to the *Logix5000 Controllers Common Procedures Programming Manual*, publication number 1756-PM001.

Monitoring Safety Status

In addition to viewing controller safety status information on the safety status button on the online bar, as explained on page 7-3, you can also find controller safety status information on the *Safety* tab of the *Controller Properties* dialog.

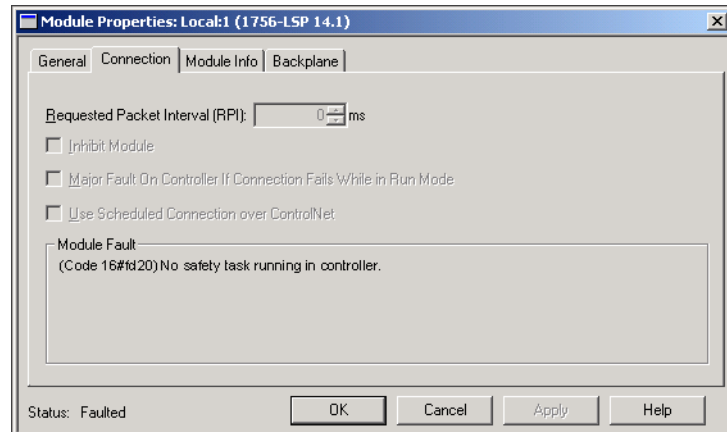


The possible values for safety status are:

- 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 above indicate that non-recoverable safety faults exist. See Table 7.2 on page 7-8 for fault codes and corrective actions.

The status of the Safety Partner can be viewed on the *Connections* tab of its *Module Properties* dialog.



GuardLogix Controller Faults

Non-Recoverable Controller Faults

These occur when the controller’s internal diagnostics fail. When a non-recoverable controller fault occurs, Safety Task execution stops and Safety I/O is placed in the safe state. Recovery requires re-download of the application program.

Non-Recoverable Safety Faults in the Safety Application

When a non-recoverable safety fault occurs in the safety application, both safety logic and the safety protocol are terminated. Safety Task Watchdog and control partnership faults fall into this category.

If the Safety Task encounters a non-recoverable 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 Signature exists, you only need to clear the fault to enable the Safety Task to run. If no Safety Signature exists, the Safety Task cannot run again until the entire application is re-downloaded.

Recoverable Faults in the Safety Application

When 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.

If a recoverable fault is cleared programmatically, the Safety Task is allowed to continue without interruption.

If 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 re-opened 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 allow you to edit the standard and/or safety application as required to correct the cause of the fault. However, if a Safety Signature exists or the controller is Safety-Locked, you must first unlock the controller and delete the Safety Signature before you can edit the safety application.

View Faults

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

Fault Codes

Table 7.1 shows the major and minor fault codes specific to GuardLogix controllers. The type and code correspond to the type and code displayed on the *Major Faults* tab (or *Minor Faults* tab) of the *Controller Properties* dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

Table 7.2 Safety Faults

Type	Code	Cause	Status	Corrective Action
Major (14)	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.	Non-recoverable	Clear the fault. If a Safety Signature exists, safety memory is re-initialized via the Safety Signature and the Safety Task will begin executing. If a Safety Signature does not exist, you must re-download the program to allow the Safety Task to run. Re-insert 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.	Non-recoverable	Install a compatible Safety Partner.
	04	Safety Partner is unavailable.	Non-recoverable	Install a compatible Safety Partner.
	05	Safety Partner hardware is incompatible.	Non-recoverable	Replace the existing Safety Partner with a compatible Safety Partner.
	06	Safety Partner firmware is incompatible.	Non-recoverable	Update the Safety Partner so that the firmware major and minor revision matches the Primary Controller.
	07	Safety task is inoperable.	Non-recoverable	Clear the fault. If a Safety Signature exists, safety memory is re-initialized via the Safety Signature and the Safety Task will begin executing. If a Safety Signature does not exist, you must re-download the program to allow the Safety Task to run.
	08	Coordinated system time (CST) not found.	Non-recoverable	Clear the fault. Configure a device to be the CST master.
	09	Safety Partner non-recoverable controller fault.	Non-recoverable	Clear the fault and re-download the program. If the problem persists, replace the Safety Partner.
Minor (10)	11	The Safety Partner's battery is missing or requires replacement.	Recoverable	Install or replace the battery on the Safety Partner. See Appendix B.

For more information... The *Logix5000™ Controllers Common Procedures Programming Manual*, publication 1756-PM001, contains descriptions of the fault codes common to all 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 (i.e. turning all outputs to their user-configured states).

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 7-10.

Program Fault Routine

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

Controller Fault Handler

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

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

For more information... The *Logix5000™ Controllers Common Procedures Programming Manual*, publication 1756-PM001, provides details on creating and testing a fault routine.

Using 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 get 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 valid object classes, object names, and attribute names for each instruction.

For standard tasks, you can use the GSV instruction to get values for all 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.

The table below shows which attributes you can get values for using the GSV instruction and which attributes you are allowed to set using the SSV instruction in both 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 7.3 GSV/SSV Accessibility

Safety Object	Attribute Name	Attribute Description	Accessible from the Safety Task		Accessible from Standard Tasks	
			GSV	SSV	GSV ⁽¹⁾	SSV
Safety Task	Instance	Provides instance number of this task object. Valid values are 0 to 31.	✓		✓	
	MaximumInterval	The maximum time interval between successive executions of this task.			✓	✓
	MaximumScanTime	Maximum recorded execution time (ms) for this task.			✓	✓
	MinimumInterval	The minimum time interval between successive executions of this task.			✓	✓
	Priority	Relative priority of this task as compared to other tasks. Valid values are 0 to 15.	✓		✓	
	Rate	Period for the task (in ms), or timeout value for the task (in ms).	✓		✓	
	Watchdog	Time limit (in ms) for execution of all programs associated with this task.	✓		✓	
Safety Program	Instance	Provides the instance number of the program object.	✓		✓	
	MajorFaultRecord	Records major faults for this program.	✓	✓	✓	
	MaximumScanTime	Maximum recorded execution time (ms) for this program.			✓	✓
Safety Routine	Instance	Provides the instance number for this routine object. Valid values are 0 to 65,535.	✓			
Safety Controller	SafetyLocked	Indicates whether the controller is Safety-Locked or -Unlocked.			✓	
	SafetyStatus	Specifies the safety status as: <ul style="list-style-type: none"> • Safety Task OK • Safety Task inoperable • Partner missing • Partner unavailable • Hardware incompatible • Firmware incompatible 			✓	
	SafetySignatureExists	Indicates whether the Safety Signature is present.	✓		✓	
	SafetyTaskFaultRecord	Records Safety Task faults.			✓	

(1) From the standard task, GSV accessibility of safety object attributes is the same as for standard object attributes.

Controller Specifications

Certifications

When marked, the components have the following certifications. For UL, CE, C-Tick, and EEX, see the Product Certification link at www.ab.com for Declarations of Conformity, Certificates, and other certification details.

Certification	Description
UL	UL Listed Industrial Control Equipment
CSA	CSA Certified Process Control Equipment
CSA	CSA Certified Process Control Equipment for Class I, Division 2 Group A,B,C,D Hazardous Locations
FM	FM Approved Equipment for use in Class I Division 2 Group A,B,C,D Hazardous Locations
CE	European Union 89/336/EEC EMC Directive, compliant with: <ul style="list-style-type: none"> • EN 61000-6-4; Industrial Emissions • EN 50082-2; Industrial Immunity • EN 61326; Meas./Control/Lab., Industrial Requirements • EN 61000-6-2; Industrial Immunity
C-Tick	Australian Radiocommunications Act, compliant with: AS/NZS CISPR 11; Industrial Emissions
EEx	European Union 94/9/EEC ATEX Directive, compliant with: EN 50021; Potentially Explosive Atmospheres, Protection "n"
TÜV	Functional Safety: SIL 1 to 3, according to IEC 61508; Category 1 to 4, according to EN954-1.

General Specifications

Catalog Number	1756-L61S	1756-L62S	1756-LSP
Memory - Standard Task	2 MB	4 MB	N/A
Memory - Safety Task	1 MB	1 MB	1 MB
Backplane Current at 5V dc	1.20 A	1.20 A	1.20 A
Backplane Current at 24V dc	14 mA	14 mA	14 mA
Power Dissipation	3.5 W	3.5 W	3.5 W
Thermal Dissipation	11.9 BTU/hr	11.9 BTU/hr	11.9 BTU/hr
Weight	0.32 kg (11.3 oz)	0.32 kg (11.3 oz)	0.32 kg (11.3 oz)

Environmental Specifications

Description	Value
Operating Temperature	IEC 60068-2-1 (Test Ad, Operating Cold), IEC 60068-2-2 (Test Bd, Operating Dry Heat), IEC 60068-2-14 (Test Nb, Operating Thermal Shock): <ul style="list-style-type: none"> 0 to 60° C (32 to 140° F)
Storage Temperature	IEC 60068-2-1 (Test Ab, Un-packaged Non-operating Cold), IEC 60068-2-2 (Test Bb, Un-packaged Non-operating Dry Heat), IEC 60068-2-14 (Test Na, Un-packaged Non-operating Thermal Shock): <ul style="list-style-type: none"> -40 to 85° C (-40 to 185° F)
Relative Humidity	IEC 60068-2-30 (Test Db, Un-packaged Non-operating Damp Heat): 5% to 95% noncondensing
Vibration	IEC60068-2-6 (Test Fc, Operating): 2g at 10 to 500 Hz
Operating Shock	IEC60068-2-27 (Test Ea, Unpackaged Shock): 30g
Non-Operating Shock	IEC60068-2-27 (Test Ea, Unpackaged Shock): 50g
Emissions	CISPR 11: Group 1, Class A
ESD Immunity	IEC 61000-4-2: <ul style="list-style-type: none"> 6 kV contact discharges 8 kV air discharges
Radiated RF Immunity	IEC 61000-4-3: <ul style="list-style-type: none"> AM - 10V/m at 80 to 1000 MHz at 1 kHz AM - 10V/m at 1.- to 2.0 GHz at 1 kHz PM - 10V/m at 900 MHz at 200 Hz
EFT/B immunity	IEC 61000-4-4: <ul style="list-style-type: none"> ±4 kV at 2.5 kHz on power ports ±4 kV at 2.5 kHz on communications ports
Surge Transient Immunity	IEC 61000-4-5: ±2 kV line-earth (CM) on shielded ports
Conducted RF Immunity	IEC 61000-4-6: 10V at 150 kHz to 80 MHz at 1 kHz
Enclosure Type Rating	none (open-style)
Isolation Voltage	30V Tested to withstand 500V for 60 seconds
Programming Cable	1756-CP3 or 1747-CP3 serial cable category 3 ⁽¹⁾
Replacement Battery	1756-BA2 (0.50g lithium)

(1) See Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1.

Environment and Enclosure Information

ATTENTION**Environment and Enclosure**

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

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

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 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.

See NEMA Standards publication 250 and IEC publication 60529, as applicable, for explanations of the degrees of protection provided by different types of enclosure. Also, see the appropriate sections in this publication, as well as the Allen-Bradley publication 1770-4.1 ("Industrial Automation Wiring and Grounding Guidelines"), for additional installation requirements pertaining to this equipment.

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations:

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.

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 be changed only in an area known to be nonhazardous.
-

Maintain the Battery

This chapter provides information on the 1756-BA2 battery, including how to estimate battery life, when to replace the battery, and how to replace the 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 LED Turns On

Use the following table to estimate the worst case time before the BAT LED turns red.

Max. Temperature 1 Inch Below Chassis	Power Cycles per day	Project Size		
		1 MB	2 MB	4 MB
0 to 40°C (32 to 104°F)	3	3 years	3 years	26 months
	2 or fewer	3 years	3 years	3 years
41 to 45°C (105 to 113°F)	3	2 years	2 years	2 years
	2 or fewer	2 years	2 years	2 years
46 to 50°C (114 to 122°F)	3 or fewer	16 months	16 months	16 months
51 to 55°C (123 to 131°F)	3 or fewer	11 months	11 months	11 months
56 to 60°C (132 to 140°F)	3 or fewer	8 months	8 months	8 months

EXAMPLE

Under the following conditions:

- Maximum temperature 1 in. below the chassis is 45°C
- Power is cycled 3 times per day
- The controller contains a 2 MB project

The battery will last at least 2 years before the BAT LED turns red.

After BAT LED Turns ON

IMPORTANT

If the BAT LED turns on when you apply power to the controller, the battery life may be less than the table below indicates. Some of the battery life may have been used up while the controller was off and unable to turn on the BAT LED.

Use the table below to estimate the worst case battery life after the BAT LED turns red. Battery life estimates are valid whether or not the controller has power.

Max. Temperature 1 Inch Below Chassis	Power Cycles	Project Size		
		1 MB	2 MB	4 MB
0 to 20°C (32 to 68°F)	3 per day	26 weeks	18 weeks	12 weeks
	1 per day	26 weeks	26 weeks	26 weeks
	1 per month	26 weeks	26 weeks	26 weeks
21 to 40°C (70 to 104°F)	3 per day	18 weeks	14 weeks	10 weeks
	1 per day	24 weeks	21 weeks	18 weeks
	1 per month	26 weeks	26 weeks	26 weeks
41 to 45°C (105 to 113°F)	3 per day	12 weeks	10 weeks	7 weeks
	1 per day	15 weeks	14 weeks	12 weeks
	1 per month	17 weeks	17 weeks	17 weeks
46 to 50°C (114 to 122°F)	3 per day	10 weeks	8 weeks	6 weeks
	1 per day	12 weeks	11 weeks	10 weeks
	1 per month	12 weeks	12 weeks	12 weeks
51 to 55°C (123 to 131°F)	3 per day	7 weeks	6 weeks	5 weeks
	1 per day	8 weeks	8 weeks	7 weeks
	1 per month	8 weeks	8 weeks	8 weeks
56 to 60°C (132 to 140°F)	3 per day	5 weeks	5 weeks	4 weeks
	1 per day	6 weeks	6 weeks	5 weeks
	1 per month	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 LED on the front of the controller turns on (solid red).
- A minor fault occurs (type 10, code 10 for the Primary Controller and type 10, code 11 for the Safety Partner).

ATTENTION



To prevent possible battery leakage, even if the BAT LED is off, replace the battery according to the following schedule:

If the temperature 2.54 cm (1 in.) below the chassis is:	Replace the battery every:
0 to 35°C (32 to 95°F)	no required replacement
36 to 40°C (96 to 104°F)	3 years
41 to 45°C (105 to 113°F)	2 years
46 to 50°C (114 to 122°F)	16 months
51 to 55°C (123 to 131°F)	11 months
56 to 60°C (132 to 140°F)	8 months

Replace the Battery

Because the controller uses a lithium battery, you must follow specific precautions when handling or disposing of a battery.

WARNING



The controller uses a lithium battery, which contains potentially dangerous chemicals. Before handling or disposing of a battery, review *Guidelines for Handling Lithium Batteries*, publication number 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

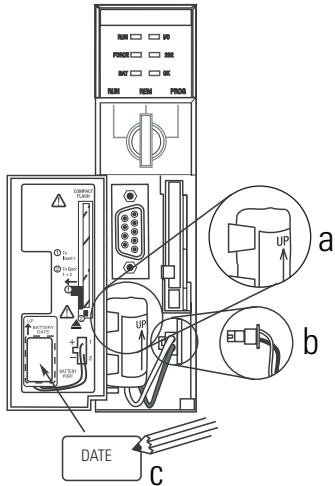
If you remove the battery before power-cycling, the project in the controller will be lost.


To replace the battery:

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

If:	Then:
Yes	Before handling the battery, review <i>Guidelines for Handling Lithium Batteries</i> , publication number 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.



<div style="background-color: black; color: white; padding: 2px 5px; display: inline-block;">ATTENTION</div> <div style="text-align: center; margin-top: 10px;"></div>	Install only a 1756-BA2 battery. If you install a different battery, you may damage the controller.
--	---

- 5. Is the BAT LED on the front of the controller off?

If:	Then:
Yes	Go to the next step.
No	<ul style="list-style-type: none">1. Check that the battery is correctly connected to the controller.2. If the BAT LED remains on, install another 1756-BA2 battery.3. If the BAT LED remains on after installing the alternate battery in step 2, contact your Rockwell Automation representative or local distributor.

4. Dispose of the old battery in accordance with all local regulations.

ATTENTION

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.

Storing Replacement Batteries

Because a battery may leak potentially dangerous chemicals if stored improperly, store batteries as follows:

ATTENTION

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

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

Change Controllers

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

- supported features
- physical configuration of the project (i.e. Safety Partner and Safety I/O)
- controller properties
- project components (e.g. tasks, programs, routines, and tags)

From Standard to Safety

In order to successfully change from a standard controller to a safety controller, the chassis slot immediately to the right of the safety controller must be available for the Safety Partner.

Upon confirmation of a change from a standard controller to a safety controller, 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.
- A safety program and safety routine are created.
- A time-based SNN is generated.
- The controller is Safety-Unlocked.
- Safety-Lock and -Unlock passwords are *not* set.
- A Safety Signature is *not* created.
- Any standard controller features not supported by the safety controller are removed from the *Controller Properties* dialog (i.e. Redundancy).

TIP

Routines with Function Block Diagrams or Sequential Function Charts are not deleted. However, the programs that contain those routines will not verify.

From Safety to Standard

Upon confirmation of a change from a safety controller 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 is changed to a true periodic task.
- Safety programs are changed to standard programs.
- Routines within safety programs are changed to standard 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 is deleted.
- Lock and Unlock passwords are deleted.
- If the standard controller supports features that were not available to the safety controller, those new features will be visible in the *Controller Properties* dialog (i.e. Non-volatile storage).

TIP

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

As a result of the above changes to the system, safety-specific instructions or safety I/O tags will not verify. Instructions may still reference modules that have been deleted. In addition, consumed tags are deleted when the producing module is deleted.

Numerics

- 1747-CP3 cable** 6-1
- 1756-Axx** 1-5
- 1756-CP3 cable** 6-1
- 1756-DNB**
 - connections 3-9
- 1756-ENBT**
 - configuration parameters 3-7
 - in a GuardLogix system 3-7
- 1756-PA72** 1-5
- 1756-PA75** 1-5
- 1756-PA75R** 1-5
- 1756-PB72** 1-5
- 1756-PB75** 1-5
- 1756-PB75R** 1-5
- 1791DS-IB12**
 - hardware overview 1-6
- 1791DS-IB4X0W4**
 - hardware overview 1-6
- 1791DS-IB8X0B8**
 - hardware overview 1-6

A

- advanced connection reaction time** 4-6
- alias tags** 5-6

B

- base tags** 5-6
- battery**
 - disposal B-5
 - installation B-4
 - replacement procedure B-3
 - replacement schedule B-3
 - storage B-5

C

- CE** A-1
- certifications** A-1
- Change Controller button** 2-3
- changing controllers** C-1–C-2
- chassis**
 - hardware overview 1-5
- CIP Safety protocol**
 - definition 3-1
- class** 5-8
- CompactFlash** 1-4
- configuration ownership**
 - identifying 4-8

resetting 4-8

configuration signature

- components 4-8
- copy 4-8
- definition 4-8

configure always checkbox 2-5, 4-12, 4-14

connection status 7-5

consumed tag

- description 5-9

consumed tags 5-6

control and information protocol

- Definition P-3

controller

- configuration 2-1

controller fault handler 7-9

controller match 6-5

controller properties dialog

- date/time tab 2-6
- general tab 2-3
- major faults tab 6-6, 7-7
- safety tab 5-17, 5-18, 6-6

controller-scoped tags 5-7

coordinated system time 2-5

create a new project 2-1

CSA A-1

CST

See Coordinated System Time.

C-Tick A-1

D

Date/Time tab 2-6

DeviceNet network

- configure driver 6-3, 6-4
- connections 3-9, 6-3

DeviceNet Safety I/O

- adding 4-1
- address 4-9
- configuration signature 4-8
- LEDs 4-10
- monitor system status 4-9
- node address 4-1
- replacing 4-11–4-14
- reset ownership 4-8
- status data 4-11

DF1 3-10

DH-485 3-10

diagnostic coverage

- Definition P-3

download

- effect of controller match 6-5
- effect of firmware revision match 6-5
- effect of safety signature 6-6-6-7
- effect of safety status 6-6
- effect of safety-lock 6-6-6-7
- process 6-8-6-9

E**EEx** A-1**enclosure** A-3**environment** A-3**EtherNet/IP network**

- configure driver 6-3, 6-4
- connections 6-2
- parameters 3-7

European norm.

- Definition P-3

F**fault**

- codes 7-7
- non-recoverable safety 7-6
- recoverable fault 7-7
- routines 7-8-7-11

faults

- non-recoverable controller faults 7-6

firmware revision match 6-5**FM** A-1**G****gateway** 3-7**get system value (GSV)**

- accessibility 7-11
- definition P-3

go online

- process 6-11

H**hazardous location approval**

- North America A-4

HMI devices 1-3**I****IP address** 3-7**K****keyswitch** 1-4**L****LEDs**

- DeviceNet Safety I/O 4-10

- GuardLogix controller 7-1

lock/unlock button 2-4**M****major faults tab** 7-7

- view controller faults 7-7

- view safety status 6-6

minor faults tab 7-7**module properties dialog**

- connection tab 4-8

- safety tab 4-4, 4-8

morphing

- See changing controllers.

N**network delay multiplier** 4-6**new controller dialog** 2-1**non-recoverable safety faults**

- re-starting the safety task 7-7

O**online bar** 7-3**ownership**

- configuration 4-8

- resetting 4-8

P**password**

- set 2-4

- valid characters 2-4

peer safety controller

- configuration 2-7

- SNN 2-7

power supplies

- catalog numbers 1-5

primary controller

- description 1-3

- hardware overview 1-3

- memory 1-4

- modes 1-4

probability of failure on demand (PFD)

- definition P-3

probability of failure per hour (PFH)

definition P-3

produce and consume tags 3-6**produced tag**

description 5-6, 5-9

program fault routine 7-9**program-scoped tags** 5-8**protecting the safety application** 5-16–5-19

RSLogix Security 5-18

safety signature 5-18

safety-lock 5-16

R**RAM capacity** 1-4**reaction time limit**

DeviceNet Safety I/O 4-4

requested packet interval

consumed tags 5-6

DeviceNet Safety I/O 4-4

reset ownership 4-8, 4-11**restrictions**

software 5-20

when safety signature exists 5-18

when safety-locked 5-17

RPI

see requested packet interval

RSLogix 5000

description 1-7

restrictions 5-20

RSLogix Security 5-18**S****safe state** 1-1**Safety Lock dialog** 2-4**safety network number** 3-2

assignment 3-1

automatic assignment 3-3

changing controller SNN 3-4

changing I/O SNN 3-5

copy and paste 3-6

copying and pasting 3-6

description 1-2

formats 3-2

managing 3-1

manual 3-2

manual assignment 3-3

modification 3-3

time-based 3-2

safety partner

configuration 1-4

LEDs 7-1

safety projects

features not supported 1-7

safety signature

copy 5-19

delete 5-19

description 1-2

effect on download 6-6

effect on upload 6-6

generate 5-18

restricted operations 5-18

viewing 7-3

safety status

effect on download 6-6

viewing 6-6, 7-3

safety tab

generate safety signature 5-18

safety-lock controller 5-17

view safety status 6-6

safety tag mapping dialog 5-15, 5-16**safety tags**

controller-scoped 5-8

description 5-5

invalid data types 5-7

mapping 5-14–5-16

safety-program-scoped 5-8

safety task

execution 5-3

safety-lock 5-16

effect on download 6-6

effect on upload 6-6

icon 5-17

safety-unlock

icon 5-17

serial communications 3-10**serial network**

configure driver 6-3

serial port

configuration 3-10

connections 6-2

set system value (SSV)

accessibility 7-11

software restrictions 5-20**specifications**

environmental A-2

general A-1

subnet mask 3-7

T

tags

- alias 5-6
- base 5-6
- class 5-8
- consumed 5-6
- controller-scoped 5-7
- data type 5-6
- overview 5-5
- produced 5-6
- produced/consumed safety data 5-7,
5-8
- program-scoped 5-8

- safety I/O 5-7, 5-8
- scopalso, safety tags.

terminology

- used throughout manual P-3

timeout multiplier 4-6

U

UL A-1

upload

- effect of controller match 6-5
- effect of safety signature 6-6
- effect of safety-lock 6-6
- process 6-10

Rockwell Automation Support

Rockwell Automation provides technical information on the web to assist you in using its products. At <http://support.rockwellautomation.com>, 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 Support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit <http://support.rockwellautomation.com>.

Installation Assistance

If you experience a problem with a hardware module within the first 24 hours of installation, please review the information that's contained in this manual. You can also contact a special Customer Support number for initial help in getting your module up and running:

United States	1.440.646.3223 Monday – Friday, 8am – 5pm EST
Outside United States	Please contact your local Rockwell Automation representative for any technical support issues.

New Product Satisfaction Return

We test all of our 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:

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

www.rockwellautomation.com

Corporate Headquarters

Rockwell Automation, 777 East Wisconsin Avenue, Suite 1400, Milwaukee, WI, 53202-5302 USA, Tel: (1) 414.212.5200, Fax: (1) 414.212.5201

Headquarters for Allen-Bradley Products, Rockwell Software Products and Global Manufacturing Solutions

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

Europe: Rockwell Automation SA/NV, Vorstlaan/Boulevard du Souverain 36-BP 3A/B, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Headquarters for Dodge and Reliance Electric Products

Americas: Rockwell Automation, 6040 Ponders Court, Greenville, SC 29615-4617 USA, Tel: (1) 864.297.4800, Fax: (1) 864.281.2433

Europe: Rockwell Automation, Brühlstraße 22, D-74834 Elztal-Dallau, Germany, Tel: (49) 6261 9410, Fax: (49) 6261 17741

Asia Pacific: Rockwell Automation, 55 Newton Road, #11-01/02 Revenue House, Singapore 307987, Tel: (65) 351 6723, Fax: (65) 355 1733

Publication 1756-UM020B-EN-P - October 2005

Supersedes Publication 1756-UM020A-EN-P - January 2005

Copyright © 2005 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.