GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems

Bulletin 1756 and 5069

Allen-Bradley
by ROCKWELL AUTOMATION

Reference Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 4

CIP Safety Systems and Safety Network Numbers

Chapter 5

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Chapter 6

Safety Applications

Chapter 7

Safety Programming Considerations

Chapter 8

Monitor Status and Handle Faults

Appendix A

Safety Instructions

Appendix B

Create and Use a Safety Add-On Instruction

About This Publication

This manual describes the GuardLogix® 5580 and Compact GuardLogix 5380 controller systems, which are type-approved and certified for use in safety applications as detailed in SIL Certification on page 11.

Use this manual for the development, operation, and maintenance of a GuardLogix 5580 or Compact GuardLogix 5380 controller-based safety system that uses the Studio 5000 Logix Designer® application. Read and understand the safety concepts and the requirements that are presented in this manual and familiarize yourself with applicable standards (for example IEC 61508, IEC 62061, IEC 61511, and ISO 13849-1) before operating a GuardLogix 5580 or Compact GuardLogix 5380 controller-based safety system.

Download Firmware, AOP, EDS, and Other Files

Download firmware and associated files and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Summary of Changes

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

Topic	Page
Added GuardLogix-XT™ catalog numbers	17
Revised Compact GuardLogix 5380 SIL 3 Controllers section in Chapter 2	19
Moved Use of Human Interfaces section from Chapter 5 to Chapter 2	24
Added SIL 2 and SIL 3 Considerations for Safety I/O Modules section to Chapter 3	28
Moved Differentiate Between Standard and Safety section from Chapter 5 to 1756-UM543	–
Added Safety Programs, Safety Routines, and Safety Tags sections to Chapter 5	50, 51
Added safety mapped tags to Table 2	53
Revised safety signature content	54, 58, 66, 90
Revised Generate the Safety Signature section in Chapter 6	58
Revised Lock the Controller section in Chapter 6	63
Added Safety Programming Considerations chapter	71...83
Added First Scan Safety Tag Initialization section to Chapter 7	83
Added Develop a Fault Routine section to Chapter 8	91
Moved safety fault codes from Chapter 8 to 1756-RD001	91
Added Use GSV/SSV Instructions in a Safety Application section to Chapter 8	92
Added ATAN2 safety instruction	101
Added information about connection reaction time limit	111
Added checklist item for GuardLogix system	119

Terminology

In this publication, the terms 'GuardLogix controller' or 'GuardLogix system' apply to both GuardLogix 5580 and Compact GuardLogix 5380 controllers unless otherwise noted.

For common abbreviations and other definitions, see the Glossary on page 131.

Additional Resources

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

Resource		Description
Hardware Installation	ControlLogix Chassis Installation Instructions, publication 1756-IN621	Provides information on how to install various ControlLogix® chassis and power supplies.
	Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014	Provides information on how to install Compact GuardLogix 5380 SIL 2 controllers.
	Compact GuardLogix 5380 SIL 3 Controllers Installation Instructions, publication 5069-IN023	Provides information on how to install Compact GuardLogix 5380 SIL 3 controllers.
	GuardLogix 5580 Controllers Installation Instructions, publication 1756-IN048	Provides information on how to install GuardLogix 5580 controllers.
Technical Data	1756 ControlLogix and GuardLogix Controllers Technical Data, publication 1756-TD001	Lists product specifications and certifications for ControlLogix and GuardLogix controllers.
	CompactLogix 5380 and Compact GuardLogix 5380 Controllers Specifications Technical Data, publication 5069-TD002	Lists product specifications and certifications for CompactLogix™ 5380 controllers and Compact GuardLogix 5380 controllers.
Networks	EtherNet/ Network Devices User Manual, publication ENET-UM006	Describes how to configure and use EtherNet/IP™ devices to communicate on the EtherNet/IP network.
	Ethernet Reference Manual, ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
	DeviceNet Network Configuration User Manual, publication DNET-UM004	Provides information on how to use the 1756-DNB module in a Logix 5000™ control system.
Design considerations	System Security Design Guidelines Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.
Programming tasks and procedures	Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Provides information on programming Logix 5000 controllers, including how to manage project files, organize tags, program and test routines, and handle faults.
	Logix 5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on how to create and use standard and safety Add-On Instructions in Logix applications.
	Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Provides information on the Logix 5000 instruction set that includes general, motion, and process instructions.
	GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety Application instruction set.
Logix 5000 controllers	ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information on how to install, configure, program, and use ControlLogix 5580 controllers and GuardLogix 5580 controllers in Studio 5000 Logix Designer® projects.
	CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001	Provides information on how to install, configure, program, and use CompactLogix 5380 controllers and Compact GuardLogix 5380 controllers.
	Replacement Guidelines: Logix 5000 Controllers Reference Manual, publication 1756-RM100	Provides guidelines on how to replace these controllers: • Replace a ControlLogix 5560 or 5570 controller with a ControlLogix 5580 controller • Replace a CompactLogix 5370 L3 controller with a CompactLogix 5380 controller
I/O	Compact 5000 I/O Digital Modules User Manual, publication 5069-UM004	Describes how to use Compact 5000™ I/O digital modules in Logix 5000 control systems.
	Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Provides information on how to use Guard I/O™ DeviceNet® safety modules.
	Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001	Provides information on how to use Guard I/O™ EtherNet/IP safety modules.
	CompactBlock Guard I/O 2-Channel Incremental Synchronous Serial Interface Encoder Module, publication 1791ES-UM002	Describes the CompactBlock™ Guard I/O 2-Channel incremental encoder serial synchronous interface module in a dual feedback version.
	POINT Guard I/O Safety Modules User Manual, publication 1734-UM013	Provides information on how to install and use POINT Guard I/O™ modules.

Resource		Description
Drives	Kinetix 5700 Safe Monitor Functions Safety Reference Manual, publication 2198-RM001	Describes the integrated stopping functions and safe monitoring functions with a Logix 5000 controller and Kinetix® 5700 servo drives.
	Kinetix 5500 Servo Drives User Manual, publication 2198-UM001	Provides information on how to install and use Kinetix 5500 servo drives.
	Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Provides information on how to install and use Kinetix 5700 servo drives.
	PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002	Provides information on how to install and use PowerFlex® 527 drives.
	PowerFlex 755/755T Integrated Safety - Safe Torque Off Option Module User Manual, publication 750-UM004	Describes how to use PowerFlex® 755 drives and PowerFlex® 755T drive products in safety integrity level (SIL) 3, Performance Level (PL) PLe, Category (CAT) 3 applications.
	PowerFlex 755/755T Integrated Safety Functions Option Module User Manual, publication 750-UM005	Describes how to use PowerFlex 755 drives and PowerFlex 755T drive products in safety applications up to safety integrity level 3 (SIL 3), Performance Level e (PLe), category 4.
	PowerFlex 755 On-Machine Drive User Manual, publication 750-UM006	Provides information on how to install, connect, and maintain the PowerFlex 755 On-Machine™ drives.
Standards and certifications	UL Standards Listing for Industrial Control Products, publication CMPNTS-SR002	Assists original equipment manufacturers (OEMs) with construction of panels, to help make sure that they conform to the requirements of Underwriters Laboratories.
	Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley® industrial automation controls and assemblies.
	Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
	Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
	Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

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

Notes:

Safety Integrity Level (SIL) Concept

SIL Certification

This section provides the SIL certifications and Performance Level for the controllers.

Table 1 - Safety Ratings for Safety Controllers

Controller System	IEC 61508 Type-approved and certified for use in safety applications up to and including:	IEC 62061 Suitable for use in safety applications up to and including:	ISO 13849-1 Suitable for use in safety applications up to and including:
GuardLogix® 5580 Controller Systems			
Primary controller without a safety partner	SIL 2	SIL CL 2	Performance Level PLd (Cat. 3)
Primary controller with a safety partner	SIL 3	SIL CL 3	Performance Level PLe (Cat. 4)
Compact GuardLogix 5380 Controller System with a Safety Partner			
Cat. no. ends with a 2 (5069-L3xxxxxS2)	SIL 2	SIL CL 2	Performance Level PLd (Cat. 3)
Cat. no. ends with a 3 (5069-L3xxxxxS3)	SIL 3	SIL CL 3	Performance Level PLe (Cat. 4)

IMPORTANT In the remainder of this publication:
- SIL 2 represents SIL 2, SIL CL 2, and PLd
- SIL 3 represents SIL 3, SIL CL 3, and PLe

TÜV Rheinland has approved GuardLogix 5580 and Compact GuardLogix 5380 controller systems for use in safety-related applications where the de-energized state is considered to be the safe state.

All I/O examples in this manual are based on achieving de-energization as the safe state for typical machine safety and emergency shutdown (ESD) systems.

IMPORTANT As the system user, you are responsible for these items:
- The setup, SIL rating, and validation of any sensors or actuators that are connected to the GuardLogix system
- Project management and functional test
- Access control to the safety system, including password handling
- Programming the application and the device configurations in accordance with the information in this safety reference manual and these publications:
  - ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
  - CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

When applying Functional Safety, restrict access to qualified, authorized personnel who are trained and experienced.

Use the Studio 5000 Logix Designer® application to create programs for GuardLogix 5580 and Compact GuardLogix 5380 controllers. Only the safety task, not standard tasks, can be used for safety functions.

SIL 2 and SIL 3 Safety Application Differences

A risk assessment determines whether a safety function requires SIL 2 or SIL 3. For example, one machine has multiple safety functions with the maximum risk, which requires only SIL 2. In that case, a SIL 2 capable controller is acceptable. Another machine has multiple safety functions with at least one risk, which requires SIL 3. In that case, a SIL 3 capable controller is required.

A SIL 2 GuardLogix 5580 controller requires only the primary controller, and a SIL 3 GuardLogix 5580 controller requires both the primary controller and the safety partner. See GuardLogix 5580 Controller Hardware on page 17.

Compact GuardLogix 5380 controllers are also capable of SIL 2 and SIL 3 support depending on the catalog number. See Compact GuardLogix 5380 Controller Hardware on page 18.

IMPORTANT If operating above 55 °C (131 °F) in a SIL 2 application, modules greater than 6.2 W must not be installed in slots that are next to a GuardLogix 5580 controller.

ATTENTION: The safety signature is required for the controller to operate at a SIL 2 or SIL 3 rating. Running without a safety signature is only suitable during development. See Generate the Safety Signature on page 58.

IMPORTANT The safety task can contain a number of safety functions. For a particular function to be SIL 3, the entire chain of devices and programming from the sensor to the actuator must be SIL 3. Be careful that you do not use a SIL 2 input signal for a safety function that requires SIL 3.

Proof Tests

IEC 61508 requires you to perform various proof tests of the equipment that is used in the system. Proof tests are performed at user-defined times. For example, proof tests can be once a year, once every 15 years, or whatever time frame is appropriate.

GuardLogix 5580 and Compact GuardLogix 5380 controllers have a useful life of 20 years, no proof test required. Other components of the system, such as safety I/O devices, sensors, and actuators can have different useful life times.

IMPORTANT Your specific applications determine the time frame for the useful life.

GuardLogix Architecture

This section provides examples of SIL 3 and SIL 2 systems, including the following:

- The overall safety function
- The GuardLogix portion of the overall safety function
- How other devices that operate outside the safety function, such as HMI, are connected

Figure 1 - Example SIL 3 System

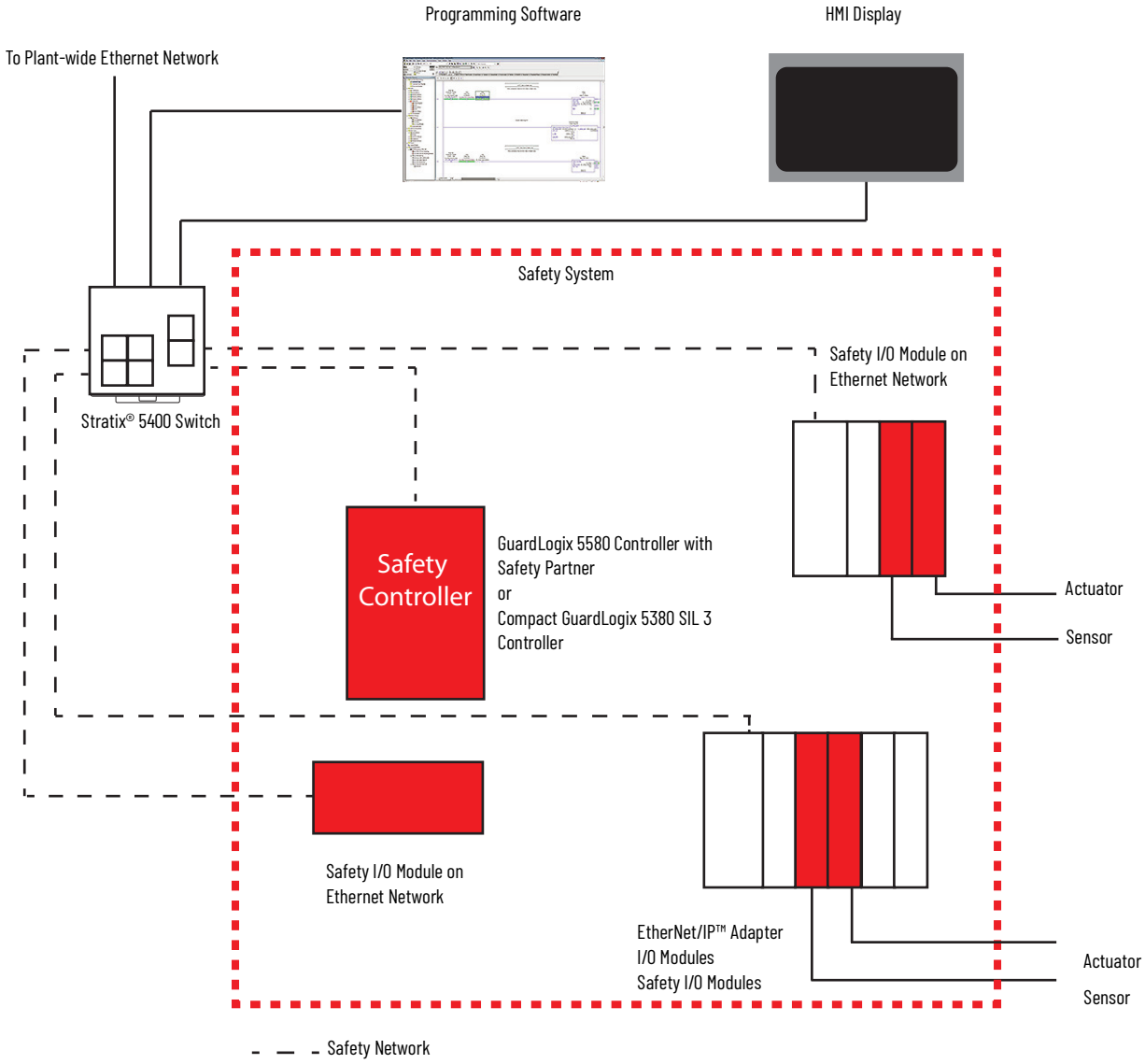
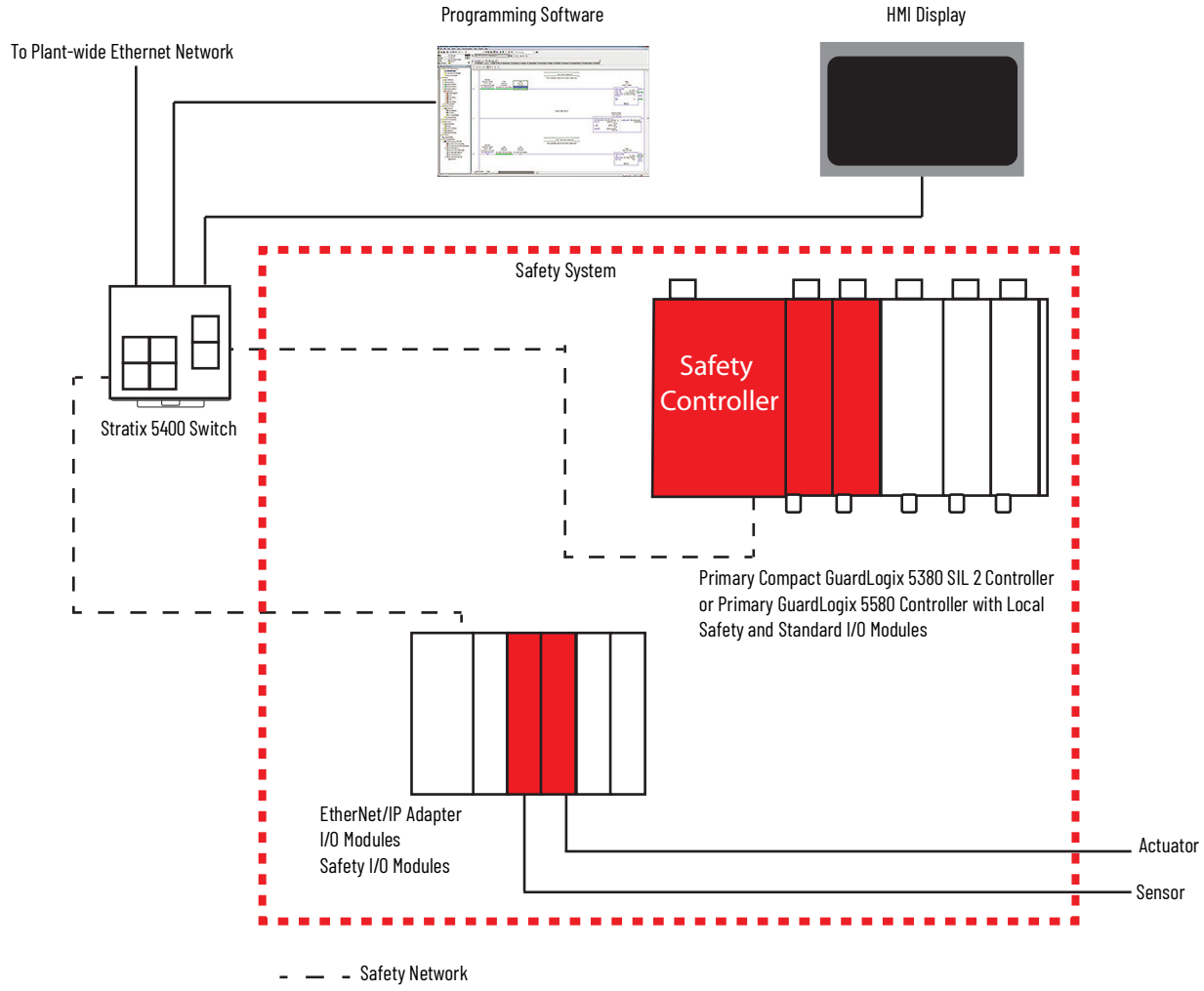


Figure 2 - Example SIL 2 System



Controller Specifications

These publications list the specifications and the agency certifications for the products:

- ControlLogix Controllers Technical Data, publication 1756-TD001
- CompactLogix 5380 Controllers Specifications Technical Data, publication 5069-TD002

Agency certifications are also marked on the product labels.

For Declarations of Conformity, Certificates, and other certification details, see rok.auto/certifications.

System Reaction Time

The system reaction time is the worst-case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safe state.

This worst-case definition includes the effects of asynchronous communications, and multiple potential faults, occurring within the system. Actual reaction times can be faster.

Each of the reaction times is dependent on factors such as the type of I/O device and instructions that are used in the program.

For more information about reaction time calculations, see Appendix on page 109.

Contact Information If Device Failure Occurs

If you experience a failure with any device, contact Rockwell Automation Technical Support: Rok.auto/knowledgebase

Your local Rockwell Automation sales office or Allen-Bradley distributor can also initiate the following actions:

- Return the device to us so the failure is logged for the catalog number that is affected, and a record is made of the failure.
- Request a failure analysis (if necessary) to try to determine the cause of the failure.

Notes:

GuardLogix Controller System

For safety certificate information, see https://rok.auto/certifications. Use the filters to search for your products.

See Additional Resources on page 8 to find installation information for GuardLogix® 5580 and Compact GuardLogix 5380 controllers.

GuardLogix 5580 Controller Hardware

The GuardLogix controller consists of a primary controller (1756-L8*x*ES), which can be used alone in SIL 2 applications, and a safety partner (1756- L8SP), which is added to create the SIL 3-capable controller.

Both the primary controller and safety partner perform power-up and runtime functional-diagnostic tests of all safety-related components in the controller.

- Primary controller that is used without a safety partner is up to SIL 2.
- Primary controller that is used with a safety partner is up to SIL 3.

Controller	Cat. No.
GuardLogix 5580 controller	1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L8SP, 1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8SPK
GuardLogix-XT™ controllers	1756-L81EXTS, 1756-L82EXTS, 1756-L83EXTS, 1756-L84EXTS, 1756-L8XTSP

For the most current list of GuardLogix controller and safety I/O devices certified series and firmware revisions, see the safety certificates at https://rok.auto/certifications.

Firmware revisions are available from the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at https://compatibility.rockwellautomation.com/Pages/home.aspx.

You can fill slots of a SIL 2 or SIL 3 system chassis that are not used by the GuardLogix SIL 2 or SIL 3 system with other ControlLogix® 1756 modules. The module must be certified for low voltage and EMC Directives.

To find certificates for the controllers and I/O modules, see https://rok.auto/certifications.

Primary Controller

The primary controller is the processor that performs standard and safety control functions and communicates with the safety partner for safety-related functions in the GuardLogix control system. The primary controller consists of a central processor, I/O interface, and memory.

Safety Partner

To satisfy SIL 3 requirements, you must install a 1756-L8SP safety partner in the slot immediately to the right of the primary controller. The safety partner is a co-processor that provides 1oo2 architecture for safety-related functions in the system. The 1oo2 system does not run degraded.

Be aware of the following types of fault scenarios:

- If the two processors disagree, the result is a major nonrecoverable fault, which requires you to redownload the application.
- If the two processors cannot communicate, the result is a nonrecoverable safety fault, which may require you to redownload the application.

For information about how to respond to nonrecoverable faults, see the following:

This manual links to Logix 5000 Controller and I/O Fault Codes, publication, 1756-RD001; the file automatically downloads when you click the link.

For SIL 2 requirements, do not install a safety partner.

The primary controller configures the safety partner. Only one download of the user program to the primary controller is required. The primary controller controls the operating mode of the safety partner.

Chassis

The chassis provides the physical connections between modules and the 1756 GuardLogix system. Any failure, though unlikely, would be detected as a failure by one or more of the active components of the system. Therefore, the chassis is not relevant to the safety discussion.

Power Supply

No extra configuration or wiring is required for SIL 2 or SIL 3 operation of the ControlLogix power supplies. Any failure would be detected as a failure by one or more of the active components of the GuardLogix system. Therefore, the power supply is not relevant to the safety discussion.

Compact GuardLogix 5380 Controller Hardware

The Compact GuardLogix 5380 controller is a SIL 2 or SIL 3 capable controller that performs standard and safety control functions for safety-related functions in the Compact GuardLogix control system.

Controller	SIL Rating	Cat. No.
Compact GuardLogix 5380	SIL 2	5069-L306ERMS2, 5069-L306ERS2, 5069-L310ERMS2, 5069-L310ERS2, 5069-L320ERMS2, 5069-L320ERS2, 5069-L320ERS2K, 5069-L320ERMS2K, 5069-L330ERMS2, 5069-L330ERS2, 5069-L330ERS2K, 5069-L330ERMS2K, 5069-L340ERMS2, 5069-L340ERS2, 5069-L350ERMS2, 5069-L350ERS2, 5069-L350ERS2K, 5069-L350ERMS2K, 5069-L380ERMS2, 5069-L380ERS2, 5069-L3100ERMS2, 5069-L3100ERS2
	SIL 3	5069-L306ERMS3, 5069-L310ERMS3, 5069-L320ERMS3, 5069-L330ERMS3, 5069-L340ERMS3, 5069-L350ERMS3, 5069-L380ERMS3, 5069-L3100ERMS3, 5069-L320ERMS3K, 5069-L330ERMS3K, 5069-L350ERMS3K

IMPORTANT This equipment is supplied as open-type equipment for indoor use. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that are present and appropriately designed to help prevent personal injury resulting from accessibility to live parts.

The enclosure must have suitable flame-retardant properties to help prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool.

For more information regarding specific enclosure type ratings that are required to comply with certain product safety certifications, see:

- Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014
- Compact GuardLogix 5380 SIL 3 Controllers Installation Instructions, publication 5069-IN023

For the most current list of GuardLogix controller and safety I/O devices certified series and firmware revisions, see the safety certificates at https://rok.auto/certifications.

Firmware revisions are available from the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at https://compatibility.rockwellautomation.com/Pages/home.aspx.

Expansion slots of the system bus can be populated with Compact 5000™ I/O expansion modules that are certified to the Low Voltage and EMC Directives and populated per the instructions that are listed under Power Supply.

To find certificates for the controllers and I/O modules, see https://rok.auto/certifications.

Compact GuardLogix 5380 SIL 3 Controllers

For SIL 3/PLe safety applications, the Compact GuardLogix 5380 SIL 3 controller system consists of a primary controller and an internal safety partner. The internal safety partner is a co-processor that provides 1oo2 architecture for safety-related functions in the system. The 1oo2 system does not degrade. If the two processors disagree or cannot communicate with each other, the result is a major nonrecoverable controller fault.

For information about how to respond to nonrecoverable faults, see the following:

This manual links to Logix 5000 Controller and I/O Fault Codes, publication, 1756-RD001; the file automatically downloads when you click the link.

The primary controller configures the safety partner. Only one download of the user program to the primary controller is required. The primary controller controls the operating mode of the safety partner.

Power Supply

For Functional Safety applications, SELV/PELV-listed power supplies are required for both module power (MOD) and sensor actuator (SA) power.

Consider the following when you choose a power supply:

- The MOD power of the Compact GuardLogix 5380 controller requires a 24V DC SELV/PELV-listed power supply.
- All local 24V DC safety I/O require a SELV/PELV-listed power supply.
- If the SA power connector of the Compact GuardLogix 5380 controller is used, it requires a 24V DC SELV/PELV-listed power supply.
- If local 120/240V AC I/O are used in the Compact GuardLogix 5380 chassis, their 120/240V AC I/O SA power must be connected to a catalog number 5069-FPD module.
- If any standard I/O are used that are not powered by a SELV/PELV-listed power supply, their I/O power must be connected to a catalog number 5069-FPD module.

IMPORTANT For more information on how to power the 5069 platform when a CompactLogix™ or Compact GuardLogix Controller is present, see the CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001.

Network Communication

This section provides examples of network communication configurations.

EtherNet/IP Network

A GuardLogix 5580 or Compact GuardLogix 5380 controller can connect directly to an EtherNet/IP™ network through the onboard Ethernet port and supports 10/100/1000 Mbps network speeds. A separate Ethernet communication module is not required, but can be used in the local chassis.

Contact your local Rockwell Automation sales office or Allen-Bradley distributor for other communication interface modules available for use in the GuardLogix 5580 or Compact GuardLogix 5380 controller system.

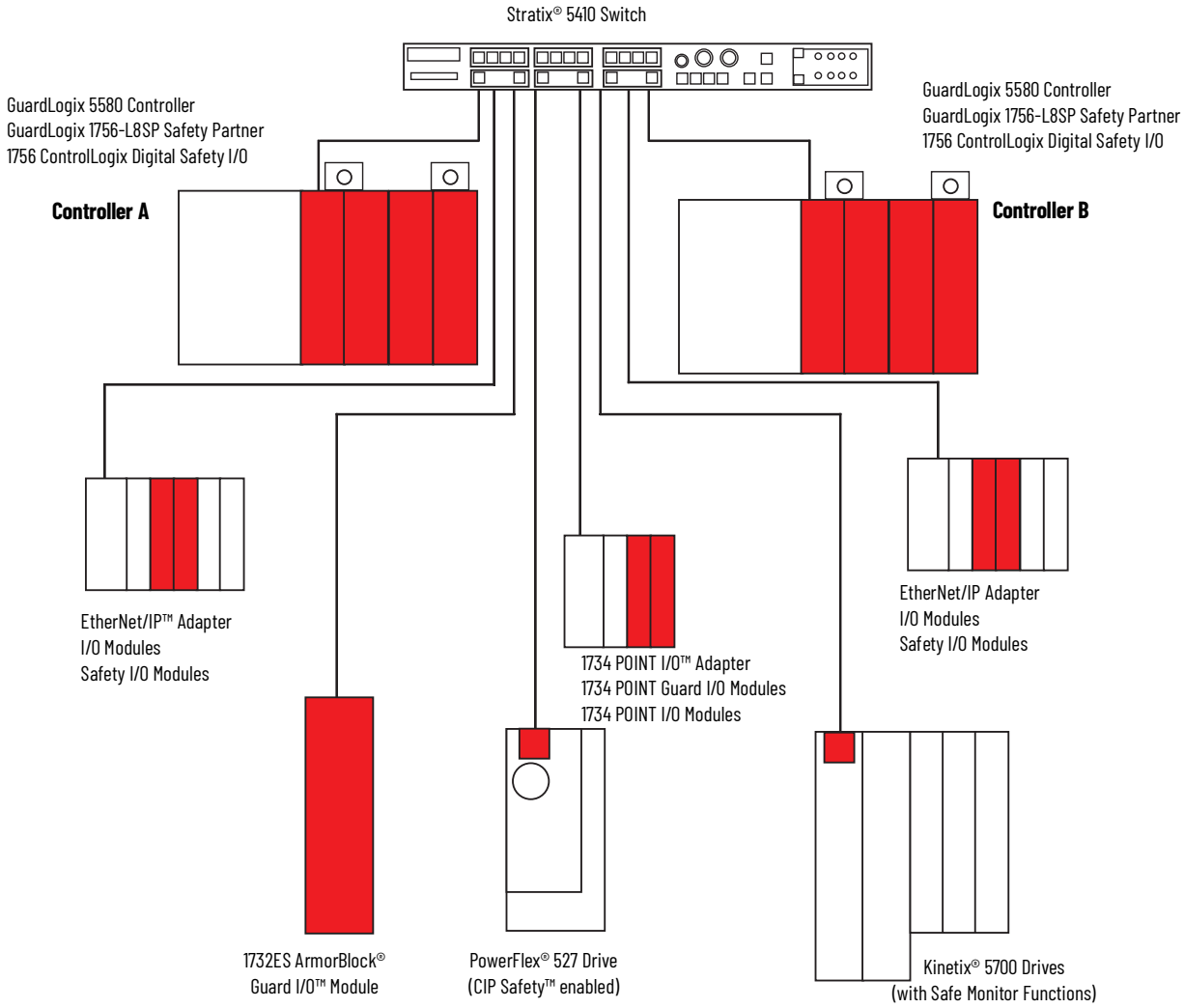
Peer-to-peer safety communication between GuardLogix controllers is possible via the EtherNet/IP network. GuardLogix controllers can control and exchange safety data with safety I/O devices on an EtherNet/IP network, via the onboard Ethernet ports or EtherNet/IP bridges.

IMPORTANT A remote GuardLogix or Compact GuardLogix controller that has firmware earlier that revision 28 cannot consume data from a GuardLogix 5580 or Compact GuardLogix 5380 controller.

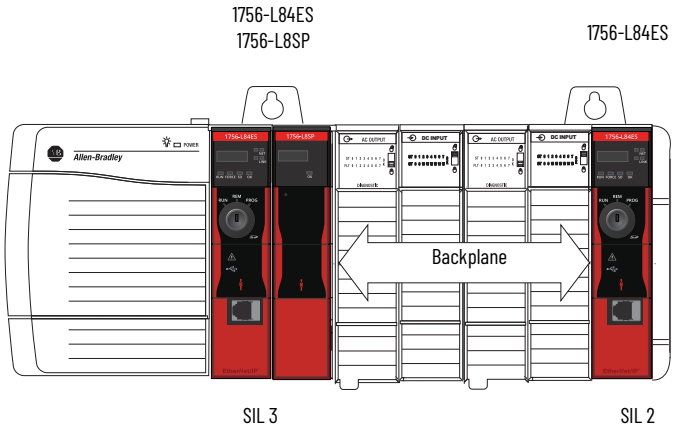
Older consumer controllers must be updated to at least to firmware revision 28, or use a dedicated, separate EtherNet/IP module in the same rack as the 5580 GuardLogix, making a connection for produced/consumed tags that bridges through the Logix backplane.

See Knowledgebase Article *Safety Tags produced by a GuardLogix 5580 controller consumed by an older GuardLogix 5570 controllers*.

Figure 3 - GuardLogix 5580 Peer-to-peer Communication via the EtherNet/IP Network

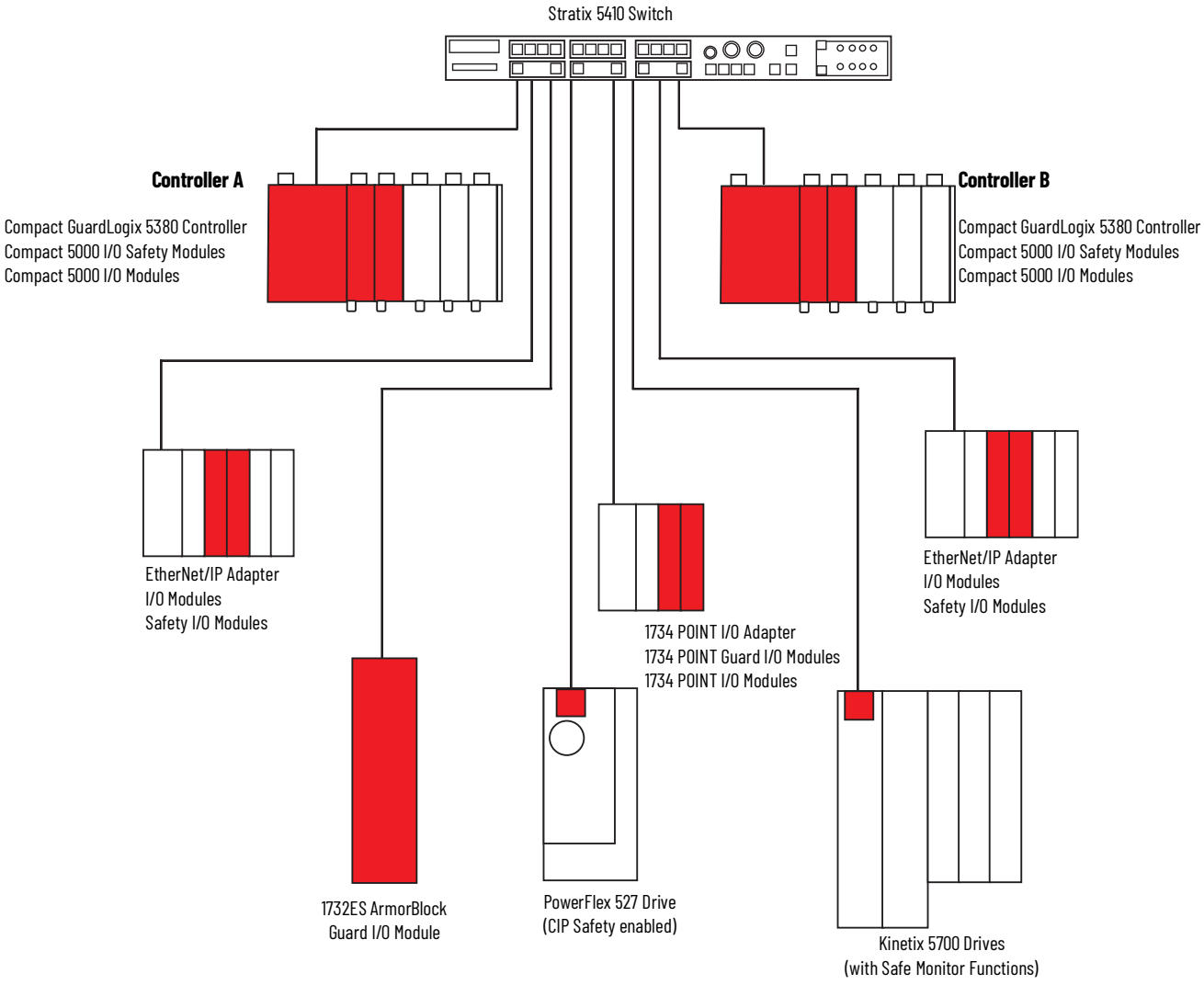


Peer-to-peer safety communication between two GuardLogix 5580 controllers in the same chassis is also possible via the backplane.



Compact GuardLogix 5380 controllers connect directly to the EtherNet/IP network through the onboard Ethernet ports. They also support 10/100/1000 Mbps network speeds. A local Ethernet communication module is not used.

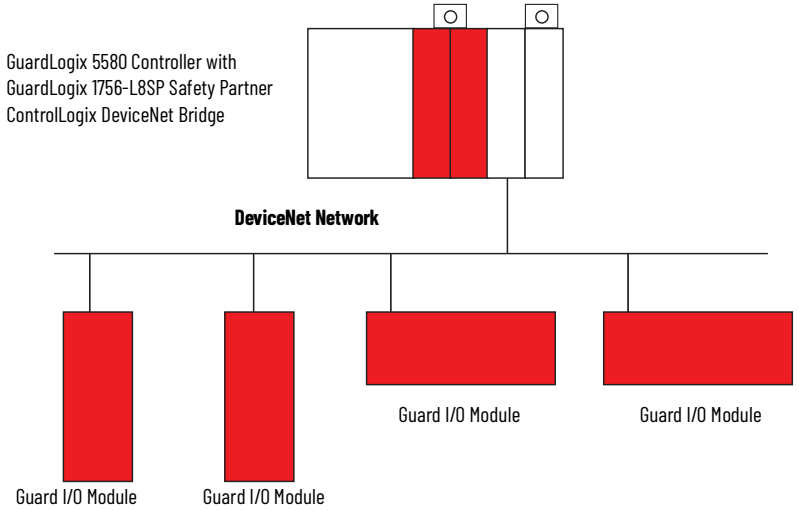
Figure 4 - Compact GuardLogix 5380 Peer-to-peer Communication via the EtherNet/IP Network



DeviceNet Safety Network

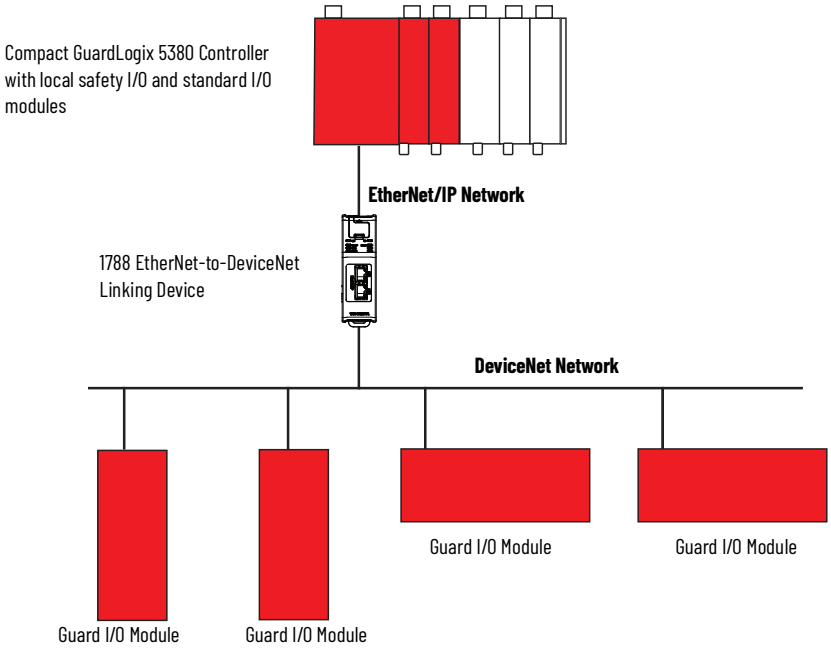
DeviceNet® bridges let the GuardLogix controller control and exchange safety data with safety I/O modules on a DeviceNet network.

Figure 5 - GuardLogix 5580 Communication via a DeviceNet Bridge



Compact GuardLogix 5380 controllers can communicate with safety devices on a DeviceNet network via a 1788-EN2DNR EtherNet/IP to DeviceNet linking device.

Figure 6 - Compact GuardLogix 5380 Controller with a DeviceNet Network



Use of Human Machine Interfaces

Follow these precautions and guidelines for HMI devices in SIL-rated GuardLogix systems.

Precautions

You must exercise precautions and implement specific techniques on HMI devices. These precautions include, but are not restricted to the following:

- Limited access and security
- Specifications, testing, and validation
- Restrictions on data and access
- Limits on data and parameters

For more information on how HMI devices fit into a typical SIL loop, see GuardLogix Architecture on page 12.

Use sound techniques in the application software within the HMI and controller.

Access to Safety-related Systems

HMI-related functions consist of two primary activities: reading and writing data.

Reading Data in Safety-related Systems

Reading data is unrestricted because reading doesn't affect the behavior of the safety system. However, the number, frequency, and size of the data being read can affect controller availability. To avoid safety-related spurious trips, use good communication practices to limit the impact of communication processing on the controller. Do not set read rates to the fastest rate possible.

Writing Data in SIL-rated Systems

Writing data, or changing parameters, in a safety-related loop via a device that operates outside the safety loop, such as HMI, is allowed only with the following restrictions:

- Only authorized, specially trained operators can write data in safety-related systems via an HMI.
- The operator that writes data in a safety-related system via an HMI is responsible for the effect of those changes in the safety loop.
- You must clearly document the variables that are to be written.
- You must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI.
- Writing data can be accepted in a safety-related system only if the following sequence of events occurs:
  a. The new value must be sent twice to two different standard tags. Both values must not be changed with one command.
  b. The two standard tags that receive the value from the HMI must be mapped into two safety tags.
  c. Safety-related code that executes in the controller, must check both safety tags for equivalency and make sure that they are within range (boundary checks).
  d. Both new variables must be read back and displayed on the HMI device. The HMI display reads the safety tags that received the mapped tag values from the standard tags.

e. Trained operators must visually check that both variables are the same and are the correct value.

f. Trained operators must manually acknowledge that the values are correct on the HMI display that sends a command to the safety logic, which allows the new values to be used in the safety function.

In every case, the operator must confirm the validity of the change before they are accepted and applied in the safety loop.

- Test all changes as part of the safety assessment procedure.
- Sufficiently document all safety-related changes that are made via the HMI, including the following:
  - Authorization
  - Impact analysis
  - Execution
  - Test information
  - Revision information
- Process Safety changes to the safety-related system must comply with IEC 61511 requirements.
- Machine safety changes to the safety-related system must comply with IEC 62061 requirements.
- The developer must follow the same sound development techniques and procedures that are used for other application software development, including the verification and test of the operator interface and its access to other parts of the program. In the controller application software, create a table that is accessible by the HMI and limit access to only required data points.
- Similar to the controller program, the HMI software is secured and maintained for SIL-level compliance after the system has been validated and tested.

Notes:

Safety I/O for the GuardLogix Control System

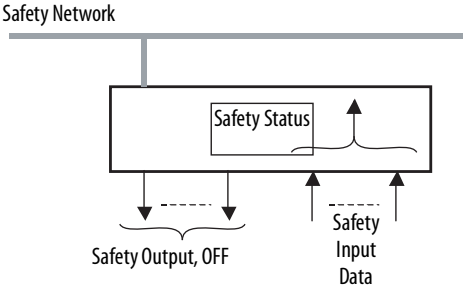
Before you operate a GuardLogix® safety system with safety I/O devices, you must first read, understand, and follow all safety information in the product documentation for those products.

Safety I/O devices can be connected to safety input and output devices, like sensors and actuators. The GuardLogix controller monitors and controls the devices. For safety data, I/O communication is performed through safety connections by using the CIP Safety™ protocol. Safety logic is processed in the GuardLogix controller.

Typical Safety Functions of Safety I/O Devices

The following is treated as the safe state by safety I/O devices:

- Safety outputs: OFF
- Safety input data to controller: OFF



Use safety I/O devices for applications that are in the safe state when the safety output turns OFF.

Diagnostics

Safety I/O devices perform self-diagnostics when the power is turned ON and periodically during operation. If a diagnostic failure is detected, safety input data (to the controller) and local safety outputs are set to their safe state (OFF).

Status Data

In addition to safety input and output data, safety I/O devices support status data to monitor device and I/O circuit health. See the product documentation for your device for specific product capabilities.

Status Indicators

The safety I/O devices include status indicators. For details on status indicator operation, see the product documentation for your specific device.

On-delay or Off-delay Function

Some safety I/O devices support on-delay and off-delay functions for input signals. Consider the following:

- Safety inputs can require an on-to-off delay to filter out the low pulse test in an output signal switching device (OSSD). Though the pulse test duration is measured in microseconds, the safety inputs can detect the low pulse as a transition to the safe state. The smallest configurable millisecond delay can be enough to filter out the pulse test.
- An on-to-off delay filter can help to filter out noise that affects the input logic level.
- Be sure to count any configured delays into the system reaction time.

  For information about system reaction time, see Appendix C.

SIL 2 and SIL 3 Considerations for Safety I/O Modules

A difference between the safety integrity levels is that single-channel I/O devices are possible for SIL 2, and dual-channel I/O devices are typically required for SIL 3.

From a safety architecture perspective, one channel means that the hardware fault tolerance (HFT) is zero. When the HFT is zero, there are guidelines that state that faults must be detected and the safety function must be taken to a safe state within the process safety time. An exception applies if the diagnostic test rate is 100 times the demand rate. If you use safety I/O modules in single channel SIL 2 applications, consider the following:

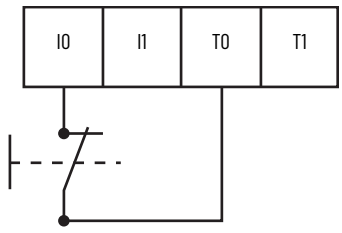
- Input or output channel must be configured for Safety Pulse Test
- Process Safety Time greater than 600 ms (the typical safety I/O pulse test interval) or the demand rate must be less than one demand per minute (for example, one per hour)

ControlLogix® digital safety input modules support single-channel SIL 2 (see preceding considerations) and dual-channel SIL 3 safety input circuits. Because these modules are rated for both SIL 2 and SIL 3 operation, you can mix SIL 2 and SIL 3 circuits on the same module.

Figure 7 shows how to wire SIL 2 safety circuits to Guard I/O™ safety input modules.

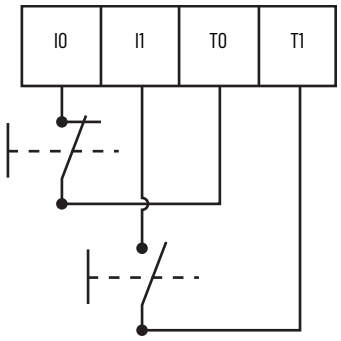
IMPORTANT The test source must be configured for pulse testing.

Figure 7 - Example Input Wiring



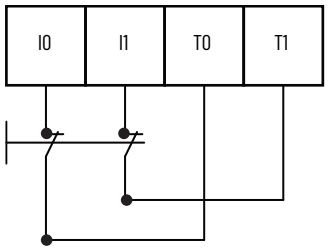
If you have two SIL 2 safety circuits, you can add a second as shown in Figure 8.

Figure 8 - Example Input Wiring in Pairs



A typical SIL 3 wiring diagram is shown in Figure 9.

Figure 9 - SIL 3 Wiring



IMPORTANT These wiring drawings are examples of possible wiring configurations. Depending on your I/O device and system configuration, other wiring configurations can also be used.

IMPORTANT The onboard pulse test outputs (T0...Tx) are typically used with field devices that have mechanical contacts. If a safety device that has electronic outputs is used (to feed safety inputs), they must have the appropriate safety ratings.

Safety Considerations for Safety I/O Devices

You must commission all devices with a node or IP address and communication rate, if necessary, before their installation on a safety network.

Ownership

One GuardLogix controller owns each safety I/O device in a GuardLogix system. Multiple GuardLogix controllers and multiple safety I/O devices can be used without restrictions in chassis or on networks, as needed. When a controller owns an I/O device, it stores the configuration data that you define for that device. This configuration controls how the devices operate in the system.

From a control standpoint, one controller controls safety output devices. One controller also owns each safety input device. However, safety input data can be shared (consumed) by multiple GuardLogix controllers.

Safety I/O Configuration Signature

IMPORTANT The safety I/O configuration signature applies to individual safety modules.
The safety I/O configuration signature is different than the controller safety signature, which applies to the entire safety portion of the controller.

The safety I/O configuration signature verifies that the device is configured as expected by the safety application. The configuration signature consists of an ID, which represents the following:

- The I/O module configuration
- The time and date that the module configuration was last applied

For a GuardLogix controller to establish a connection to a safety I/O module, the configuration signature in the GuardLogix controller must match the configuration signature in the safety I/O module. The process of synchronizing the configuration signatures requires these steps:

1. Create a safety I/O module in a Logix Designer application project.
2. Configure the I/O module in the module profile.
3. Download the project to the GuardLogix controller.

Online changes to the module configuration change the configuration signature. When online changes are applied, the GuardLogix controller downloads the configuration to the I/O module.

Offline changes to the I/O module configuration change the time and date. Once altered, the time and date remain changed even if the configuration is returned to the current running configuration. Offline changes to the time and date require one of these actions:

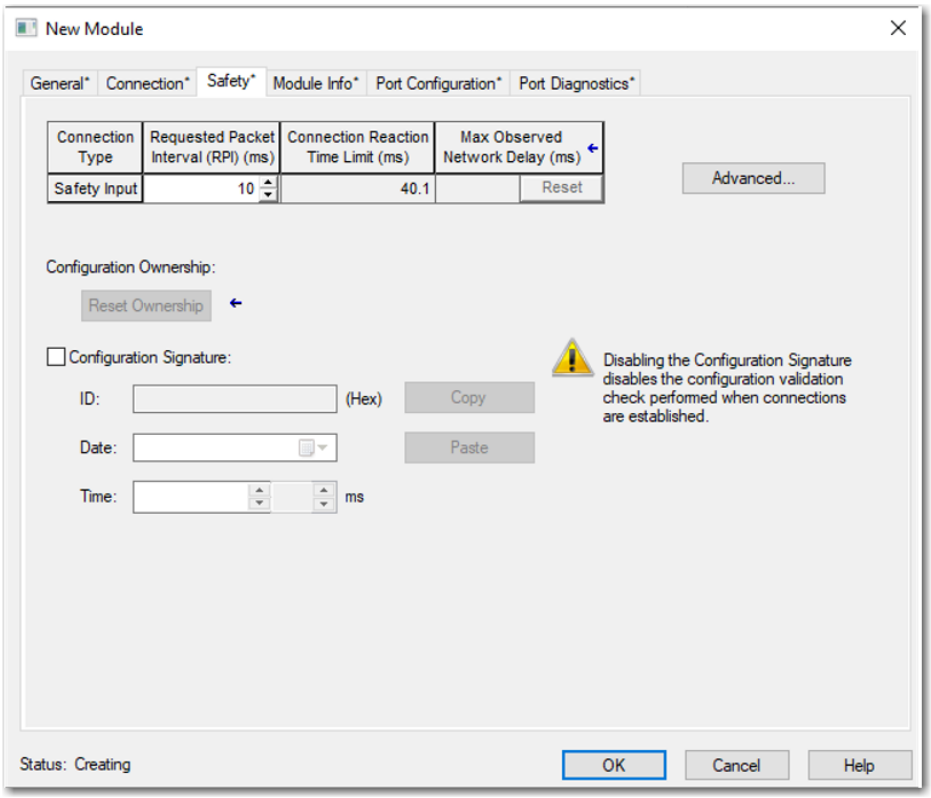
- Upload to keep the existing configuration.
- Download to push the new configuration to the I/O modules.

If a safety I/O module was previously configured in another location, the I/O module retains the configuration signature from the previous location. When a GuardLogix controller and a safety I/O module attempt to establish a safety connection, a mismatch of the configuration signatures can cause the connection to fail. To clear the safety I/O module configuration and enable the GuardLogix controller to download the module configuration to the safety I/O module, you must reset ownership.

The GuardLogix controller verifies that configuration signatures match, so there is no requirement to monitor or document the configuration signature. If the configuration signature changes unexpectedly, the safety connection between the controller and I/O module fails and causes the I/O module to enter its safe state.

When using a third-party module, if you connect to a safety I/O device without a configuration signature, you must verify that a valid configuration exists in the safety I/O device.

IMPORTANT Rockwell Automation safety I/O modules typically default to using a configuration signature and do not allow your system to run without a configuration signature.



Safety I/O Device Replacement

The replacement of safety devices requires that the replacement device is properly configured, and that the operation of the replacement device is verified.

ATTENTION: During replacement or functional testing of a device, the safety of the system must not rely on any portion of the affected device.

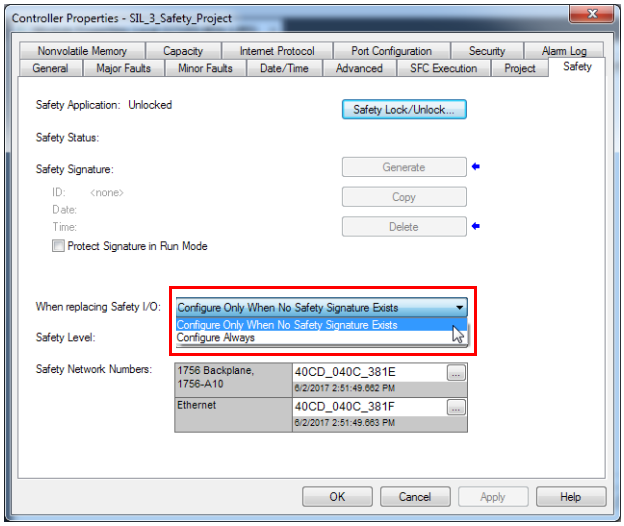
The electronic keying configuration affects the process for replacing safety I/O modules. Carefully consider the implications of each of the following electronic keying options.

Keying Option	Description	I/O Replacement Considerations
Compatible Module	Lets the installed device accept the key of the device that is defined in the project when the installed device can emulate the defined device. With Compatible Module, you can typically replace a device with another device that has the following characteristics: • Same catalog number • Same or higher major revision • Minor revision as follows: – If the major revision is the same, the minor revision must be the same or higher. – If the major revision is higher, the minor revision can be any number.	To maintain the safety signature, the replacement module must meet Compatible Module requirements.
Disable Keying	Indicates that the keying attributes are not considered when attempting to communicate with a device. With Disable Keying, communication can occur with a device other than the type specified in the project. **ATTENTION:** Be cautious when using Disable Keying. If used incorrectly, this option can lead to personal injury or death, property damage, or economic loss. We **strongly recommend** that you **do not use** Disable Keying. If you use Disable Keying, you must take full responsibility for understanding whether the device being used can fulfill the functional requirements of the application.	Many safety devices do not have a Disable Keying option. Disabled Keying is not recommended for safety applications.
Exact Match	Indicates that all keying attributes must match to establish communication. If any attribute does not match precisely, communication with the device does not occur.	• To maintain the safety signature, the replacement module must be Exact Match. • After a firmware change, keying in the safety application must be updated. Updating cannot be done without removing the controller safety signature. See Revalidation Considerations on page 61. • Exact Match is often used to meet specific industry requirements.

Two options for I/O device replacement are available on the Safety tab of the Controller Properties dialog box in the Studio 5000 Logix Designer® application:

- Configure Only When No Safety Signature Exists
- Configure Always

Figure 10 - Safety I/O Replacement Options



Configure Only When No Safety Signature Exists

This setting instructs the GuardLogix controller to configure a safety device when the safety task does not have a safety signature, and the replacement device is in an out-of-box condition with no safety network number.

If the controller has a safety signature, the GuardLogix controller automatically configures the replacement safety I/O device if the following are true:

- The device already has the correct safety network number.
- The device electronic keying is correct.
- The node or IP address is correct.

To set the proper safety network number (SNN) when a controller safety signature exists, a manual action is required to download the proper SNN. Go online to the GuardLogix or CompactGuardLogix controller with the Studio 5000 Logix Designer® application, then open the Module Properties dialog, General tab, and click the "..." button next to the Safety Network Number. Use the Set button to write the SNN to the module manually. After the manual action, the remainder of the configuration is automatically downloaded.

For detailed information, see the Replace a Safety I/O Device procedure in the user manual for the controller:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

Configure Always

The GuardLogix controller attempts to configure a replacement safety I/O device automatically if the device is in an out-of-box condition. (When a safety network number does not exist in the replacement safety device, and the node number and I/O device keying matches the configuration of the controller.)

ATTENTION: Enable the Configure Always feature only if the entire routable Safety control system is not being relied on to maintain SIL 2 or SIL 3 behavior during the replacement and functional testing of a device. See Routable CIP Safety System on page 40.
If other parts of the Safety control system are being relied upon to maintain SIL 2 or SIL 3, make sure that the Configure Always feature of the controller is disabled.

It is your responsibility to implement a process to make sure that proper safety functionality is maintained during device replacement.

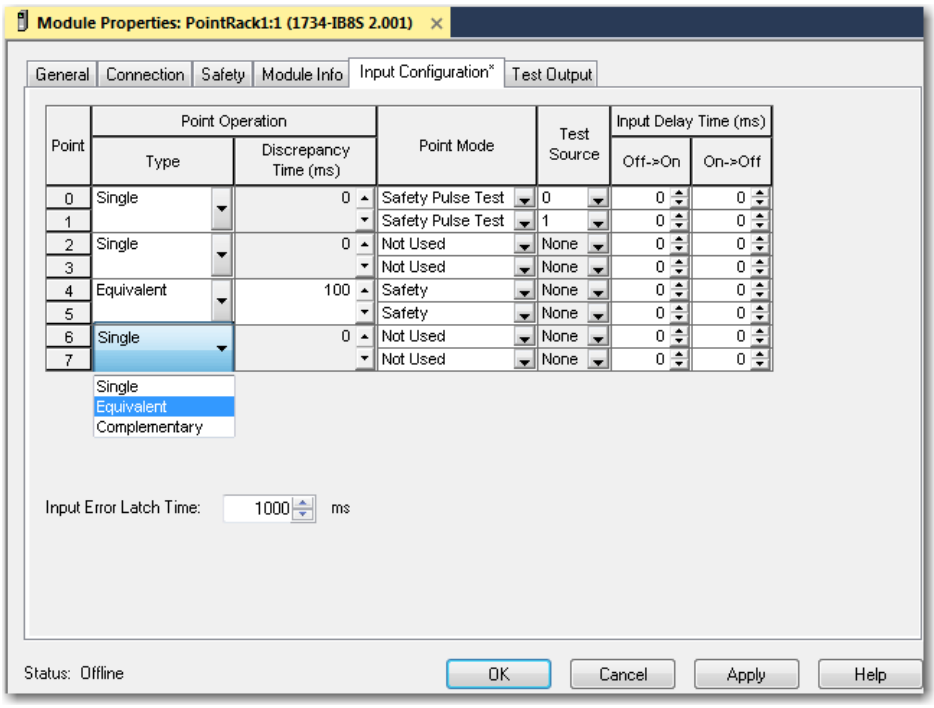
ATTENTION: To place a device in the out-of-box condition on a Safety network when the Configure Always feature is enabled, follow the device replacement procedure in the user manual:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

Input Operation

Some safety input modules, such as Bulletin 1732, 1734, and 1791, have safety inputs that can be configured as single or dual (Equivalent or Complement) point operation types. The selected type configures the safety module to view the inputs individually or as a pair:

- A single configuration is appropriate for single channel inputs or dual channel inputs that are monitored by a dual channel safety instruction like the Dual Channel Stop (DCS).
- A dual configuration configures dual channel discrepancy checking to take place at the module level. The channel data from the input module is sent to the GuardLogix controller as either the safe state or energized state. For example, equivalent inputs are either both low (0) or both high (1).

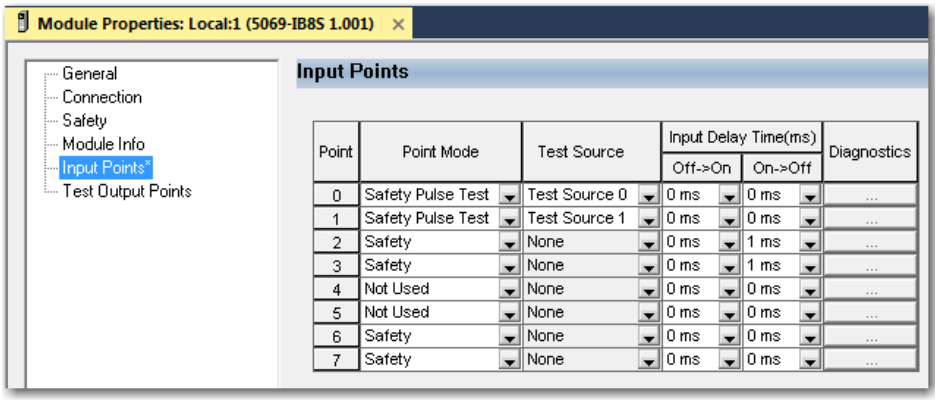


IMPORTANT When inputs are configured for a dual point operation type and monitored by dual channel safety instructions, the instruction is unable to detect discrepancy faults.

The method of monitoring discrepancy has no impact on the safety rating. The main effect is the availability of diagnostic information:

- Module level diagnostics—Status indicators, input status bit, and application code can be written to message the I/O module to monitor 1 bit for a discrepancy fault.
- Dual channel instruction diagnostics—Fault codes include channel-specific discrepancy and whether the cause of a discrepancy is a delay or a change in state to a specific channel.

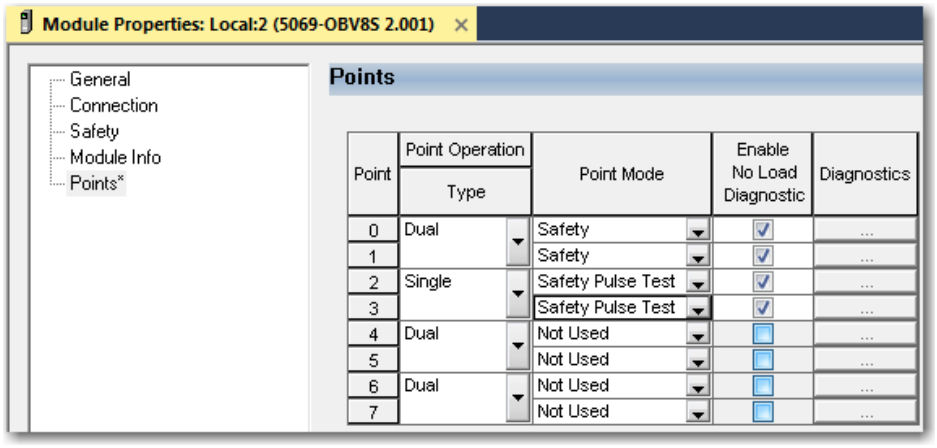
Some safety input modules, such as Bulletin 1756, 5069, and 5094, have no point operation type. All inputs are treated as single.



Output Operation

For output modules, sourcing safety outputs can be configured as point operation type single or dual. The selected type configures the safety module to treat the outputs individually or as a pair:

- A single configuration allows the outputs to turn on and off individually and to fault independently.
- A dual configuration verifies that safety task logic operates both outputs as a pair. If one output has a module fault, the other output goes to the safe state.



Bipolar outputs have no configuration for point operation type and must operate as a sinking sourcing pair.

IMPORTANT The point operation type affects the PFH safety rating of the module.

Safety I/O Configuration Variations

As the range of products using the CIP Safety protocol continues to expand, there are variations to the typical safety I/O configuration steps. Product specific procedures and requirements can include:

- Reset of ownership
- Setting the safety network number (SNN)
- Configuration signature generation
- Request packet interval (RPI) limits
- Device-specific configuration settings

For more information, see the user manual for your I/O device.

Notes:

CIP Safety Systems and Safety Network Numbers

CIP Safety™ control systems are composed of CIP Safety devices that are interconnected via communication networks. These networks consist of devices, such as switches, bridges, and adapters, which may not be SIL 2 or SIL 3 certified. Therefore, the CIP Safety devices must be inherently protected from network delivery errors.

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

For detailed information of CIP Safety functionality, see the ODVA website at https://www.odva.org.

Unique Node Reference

A key element of the CIP Safety protocol is the concept of a Unique Node Reference (also called Unique Node ID or UNID). Every CIP Safety device must have a UNID value that is assigned to each CIP Safety-capable port.

IMPORTANT It is your responsibility to make sure that all UNIDs are unique within the scope of all devices that could possibly communicate with each other.

Safety Network Numbers (SNN)

Communications within a control system travel over subnets that are interconnected with bridging or routing components. Examples of subnets:

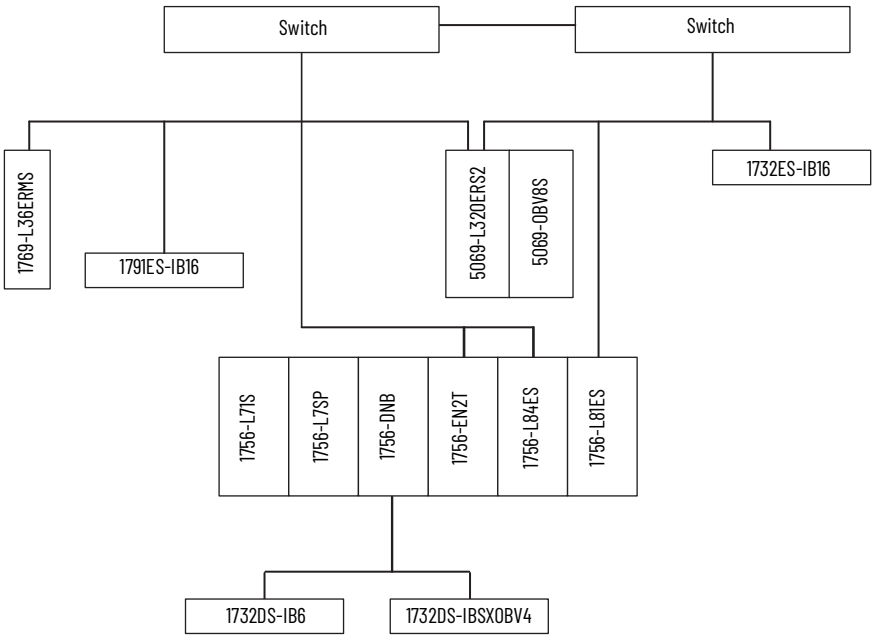
- The backplane of a chassis
- A bank of I/O modules
- An Ethernet subnet within a LAN

Rather than creating a UNID directly for each CIP Safety device, which can be prone to error in a large system, each subnet has a unique SNN, and the UNID is created from the SNN + the Node Address.

Routable CIP Safety System

The example system in Figure 11 is not interconnected to another CIP Safety system through a larger, plant-wide Ethernet backbone. This example system illustrates the extent of a routable CIP Safety system.

Figure 11 - Safety System Example



Note the following:

- For a backplane port, an SNN is assigned to the backplane and the node address is the slot number of the device.
- For an Ethernet port, an SNN is assigned to the EtherNet/IP™ network and the node address is the IP address of the device.
- The 5069-L320ERS2 is in Dual-IP mode and connected to two separate EtherNet/IP networks. They must not share SNN values because the switches can incorrectly route packets between them.

Considerations for Assigning SNNs

When you create a controller project, the Studio 5000 Logix Designer® application generates an SNN value automatically whenever a new subnet contains CIP Safety devices:

- Each CIP Safety-capable port on the controller is assigned an SNN.
- If a bridge or adapter device is in the I/O tree and a child CIP Safety device is added, the subnet that is created by the bridge or adapter is assigned an SNN.

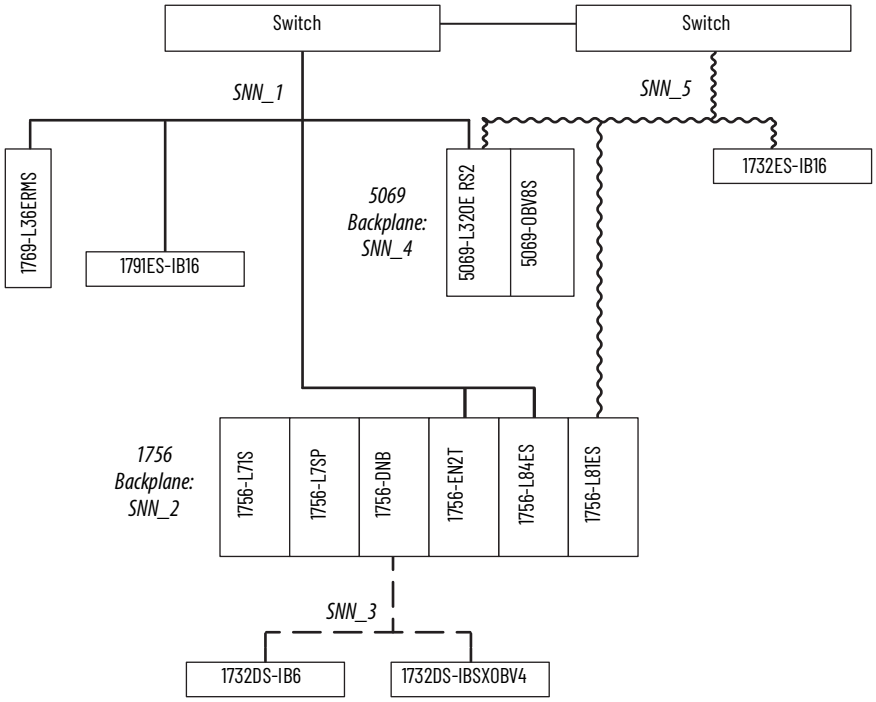
If the entire CIP Safety system consists of one controller project, these automatically generated SNN values are sufficient.

If there are multiple controllers that must interact or access the same safety I/O, the CIP Safety system designer must coordinate the SNN values between the separate project files. The Studio 5000 Logix Designer application provides copy/paste access to the SNN assignments to enable this coordination.

You can also choose to map out the entire routable system (perhaps for the entire plant), and manually assign SNN values to each subnet. The Studio 5000 Logix Designer application provides a manual entry method for assigning SNN values to enable this design methodology.

Figure 12 shows an example of how SNNs can be assigned to subnets.

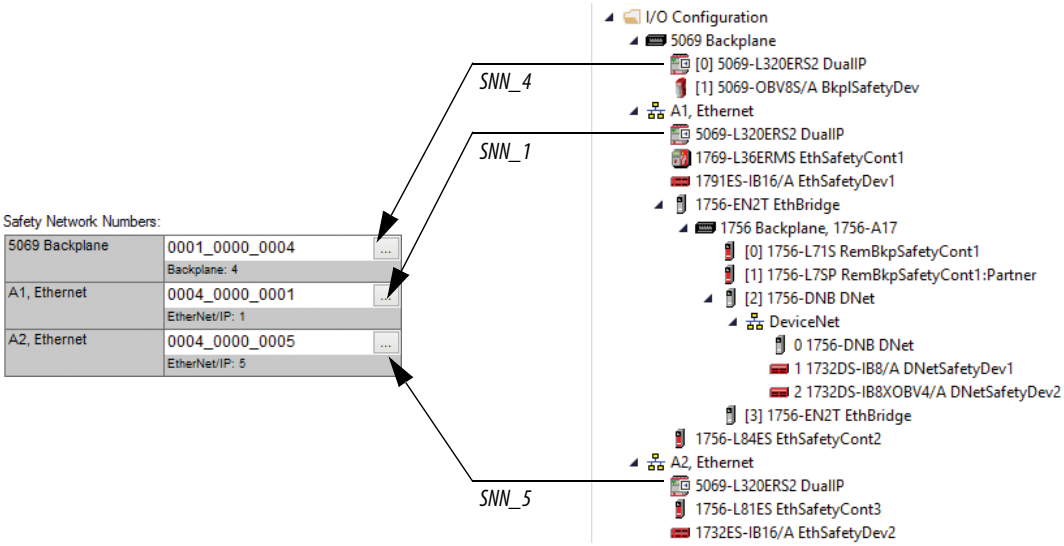
Figure 12 - Example SNN Assignment



Subnet	Type	Line	SNN Assignment
SNN_1	EtherNet/IP	———	1769-L36ERMS Ethernet port, 1791ES-IB16, 5069-L320ERS2 Ethernet port A1 (Figure 13 shows the assignment of SNN 0004_0000_0001 to this port), 1756-EN2T, and 1756-L84ES Ethernet port
SNN_2	Backplane	None	1756-L71S, 1756-L84ES backplane port, and 1756-L81ES backplane port
SNN_3	DeviceNet®	_ __ _	1732DS-IB6, 1732DS-IBSXOBV4
SNN_4	Backplane	None	5069-L320ERS2 backplane (Figure 13 shows the assignment of SNN 0001_0000_0004 to this port) and 5069-OBV8S
SNN_5	EtherNet/IP	~~~~	5069-L320ERS2 Ethernet port A2 (Figure 13 shows the assignment of SNN 0004_0000_0005 to this port) and 1732ES-IB16 and the 1756-L81ES Ethernet port.

Figure 13 shows how the preceding example relates to the Compact GuardLogix® 5380 (catalog number 5069-L320ERS2) Controller Organizer I/O tree.

Figure 13 - Controller Organizer



The configuration profile for each CIP Safety device in the I/O tree includes a parameter for the SNN value that the controller uses when it opens the CIP Safety connection to that device. This parameter automatically adopts the SNN value that is already established by the SNNs known to the project:

- Safety devices (including safety controllers) that are direct children of a GuardLogix controller adopt the SNN that matches the controller for the port that is used to connect to the safety module.
  - Safety devices directly under the backplane port adopt the backplane port SNN of the GuardLogix controller.
  - Safety devices directly under an Ethernet port adopt that Ethernet port SNN of the GuardLogix controller.
- Safety devices (including safety controllers) on a remote subnet adopt the SNN value that is already assigned to that subnet, or a new SNN is generated for the first CIP Safety device on that subnet.

We recommend that you assign each controller SNN to the already established SNN for the subnet. This recommendation enables the Logix Designer application to assign the correct SNN to each safety I/O module and safety controller that are added to the project.

If safety I/O is copied from an existing project during GuardLogix program development, the SNN value from the original location is retained. To create an SNN structure that resembles the newly created I/O, you can manually change the SNN of copied devices to follow the SNN structure of the new project by using copy/paste SNN from other I/O on the subnet or parent device. If you copy safety I/O into a new remote rack, then a new time-based SNN can be established and populated throughout the remote rack. See SNN Formats on page 43.

How SNNs Get to Safety Devices

Most CIP Safety I/O modules in the Factory Default state accept an SNN that is assigned by the controller that owns that module. The SNN value that the Logix Designer application automatically adopts for the connection of that module is accepted when the controller opens the initial connection to the module.

IMPORTANT CIP Safety I/O modules retain their UNID (SNN + Node) once it has been assigned, and must be reset before they can be reused with another value.

Some devices, such as another safety controller in the I/O tree, receive their SNN configuration from a programming workstation. For these devices, you must manually configure the connection to use the same SNN that has been programmed into that device if the Studio 5000 Logix Designer application did not automatically assign the correct SNN.

SNN Formats

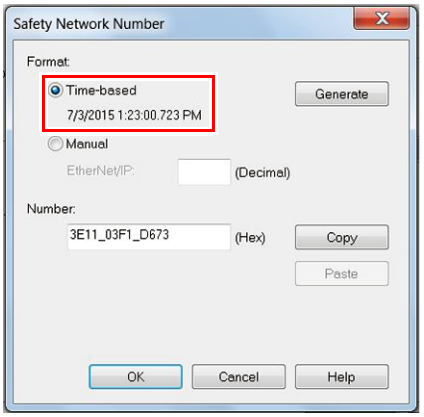
SNNs used by the system are 6-byte hexadecimal numbers. SNNs can be set and viewed in one of two formats:

- Time-based
- Manual

Time-based SNN Format and Assignment

When the time-based format is selected, the SNN represents a localized date and time.

Figure 14 - SNN Formats



The assignment of time-based SNNs is automatic when you create a GuardLogix safety controller project or add EtherNet/IP by changing the IP mode (Compact GuardLogix 5380 only) or controller type. Time-based SNNs generated by the software are always unique to the project, whether generated by project creation or IP mode change. Devices that are created directly under the controller port default to having the same SNN as that port on the controller.

IMPORTANT If you have a network diagram for your application (for example, Figure 12), you must edit the SNNs of the controller to match your network diagram. We recommend that you edit the SNNs before you add devices to the I/O configuration in Controller Organizer.

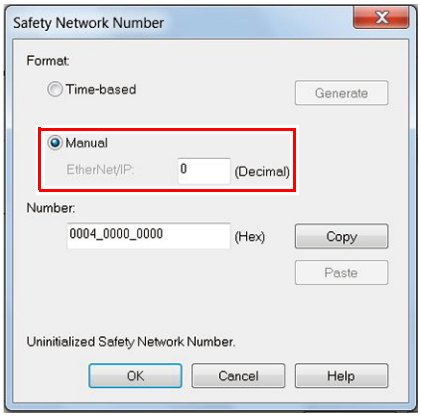
New CIP Safety I/O devices added to ports under an adapter (as opposed to the controller itself) follow similar rules.

- If no other device under the port uses an SNN, a time-based SNN is automatically assigned.
- Otherwise, the device is assigned the same SNN as the first device in address order that has an SNN.

Manual SNN Format and Assignment

When the manual format is selected, the SNN represents a network type and must have a decimal value from 1...9999.

Figure 15 - SNN Formats



Manual manipulation of an SNN is required in the following situations:

- To make sure that each safety controller port on the same subnet has the same SNN in all projects.
- When copying safety projects.

ATTENTION: If a safety project is copied into another project with different hardware or in another physical location, and the new project is within the same routable Safety system, every SNN must be changed in the second system. SNN values cannot be repeated.
See the following user manuals for information on how to change the SNN:
- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

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

A warning appears if your project contains duplicate SNN and unique node reference combinations. You can still verify the project, but we recommend that you resolve the duplicate combinations.

However, there can be safety devices on the routable safety network that have the same SNN and node address and are not in the project. In this case, these safety devices are unknown to the Studio 5000 Logix Designer application, and you may not see a warning.

If there are duplicate unique node references, as the system user, you are responsible for proving that an unsafe condition cannot result.

SNNs for Out-of-box Devices

Out-of-box CIP Safety I/O devices do not have an SNN. The SNN is set when a configuration is sent to the device by the GuardLogix controller that owns the device.

IMPORTANT To add a CIP Safety I/O device to a configured GuardLogix system (the SNN is present in the GuardLogix controller), the replacement CIP Safety I/O device must have the correct SNN applied before it is added to the CIP Safety network.

For detailed information, see the Replace a Safety I/O Device procedure in the user manual for the controller:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

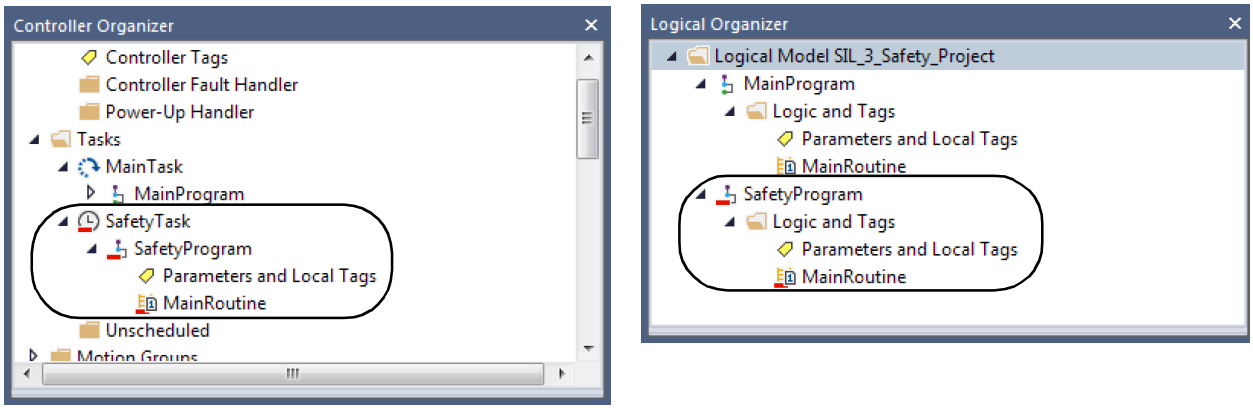
Notes:

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Safety Task

When you create a safety controller project, the Studio 5000 Logix Designer® application automatically creates a safety task with a safety program and a main (safety) routine.

Figure 16 - Safety Task in the Controller Organizer and Logical organizer



IMPORTANT Only the instructions that are listed in Appendix A can be used in the safety task.

Creation of a GuardLogix® project automatically creates one safety task. The safety task has these additional characteristics:

- GuardLogix controllers are the only controllers that support the safety task.
- The safety task cannot be deleted.
- GuardLogix controllers support one safety task.
- Within the safety task, you can use multiple safety programs that are composed of multiple safety routines.
- You cannot execute standard routines from within the safety task.

The safety task is a periodic task, and you must configure the period and the priority of the safety task. The safety task can be interrupted according to the same rules as standard tasks, such as interruptions by the motion task. The motion task is always a higher priority than any user task.

Configure the safety task with a higher priority (lower number) to reduce fluctuations in execution time. A higher priority can allow a lower setting for the safety task watchdog, which improves the reaction time of the safety system.

IMPORTANT Large amounts of mapped safety tags or large amounts of safety produce/consume tag data can cause fluctuations in the safety task scan time of the controller.

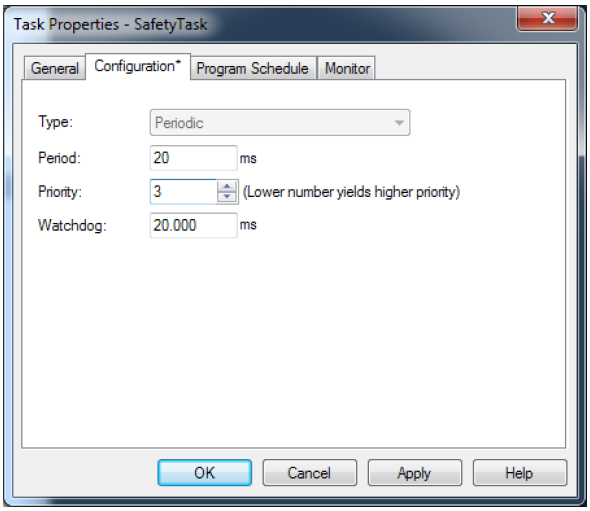
Safety Task Period

The safety task is a periodic timed task. The safety task period is the time interval between successive executions of the safety task. The safety task watchdog is the maximum time that is allowed from the start of safety task scheduled execution to its completion.

For more information on the safety task watchdog, see Appendix C.

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

Figure 17 - Configure the Safety Task Period



IMPORTANT To get the most consistent safety task execution time and to minimize safety task watchdog faults, we recommend running the safety task as the **highest priority** user task.

You specify the safety task period and the safety task watchdog in milliseconds (ms). The safety task period is the elapsed time between successive starting times for the safety task. The safety task watchdog is the maximum time that is allowed from the start of safety task execution to its completion.

The safety task period directly affects system reaction time.

Safety Task Limitations

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

For more information, see Chapter 8.

Safety Task Execution Details

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

- Safety input tags and safety-consumed tags are updated only at the beginning of safety task execution. This process means that even though the I/O RPI can be faster than the safety task period, the data in the Safety Input tag only updates once at the beginning of each safety task execution. Safety input and consumed packets that arrive after the start of the safety task are buffered until the next execution of the safety task.
- Time is frozen at the start of safety task execution. As a result, timer-related instructions, such as TON and TOF, are not updated during a safety-task execution. They keep accurate time from one task execution to another, but the accumulated time is not changed during safety task execution.

ATTENTION: This behavior differs from standard Logix task execution.

- For standard tags that are mapped to safety tags, the standard tag values are copied to the safety tags at the start of the safety task.
  - The standard tag is free to continue changing.

IMPORTANT The addition of more mapped tags can increase the scan time.

  - User code can change the safety tag within the safety task, but the change is not reflected back to the standard tag.
- Safety output tag values can be changed during the safety task scan by the safety application code of the user; the final value is transmitted to safety modules at the end of the safety task scan. Likewise, safety produced values are transmitted to consuming safety controllers at the end of the safety task scan.

IMPORTANT While safety-unlocked and without a safety signature, the controller helps prevent simultaneous write access to safety memory from the safety task and communication commands. As a result, the safety task can be held off until a communication update completes. The time that is required for the update varies by tag size. Therefore, safety connection and safety watchdog timeouts could occur. (For example, if you make online edits when the safety task rate is set to 1 ms, a safety watchdog timeout could occur.)

To compensate for the hold-off time due to a communication update, the safety watchdog time must be lengthened.

Depending on the edit, the safety task may not have enough time to complete the operation and a watchdog timeout occurs.

When the controller is safety-locked or a safety signature exists, the situation that is described in this note cannot occur.

Safety Programs

A safety program has the attributes of a standard program, except that it can be scheduled only in the safety task.

Consider the following characteristics of a safety program:

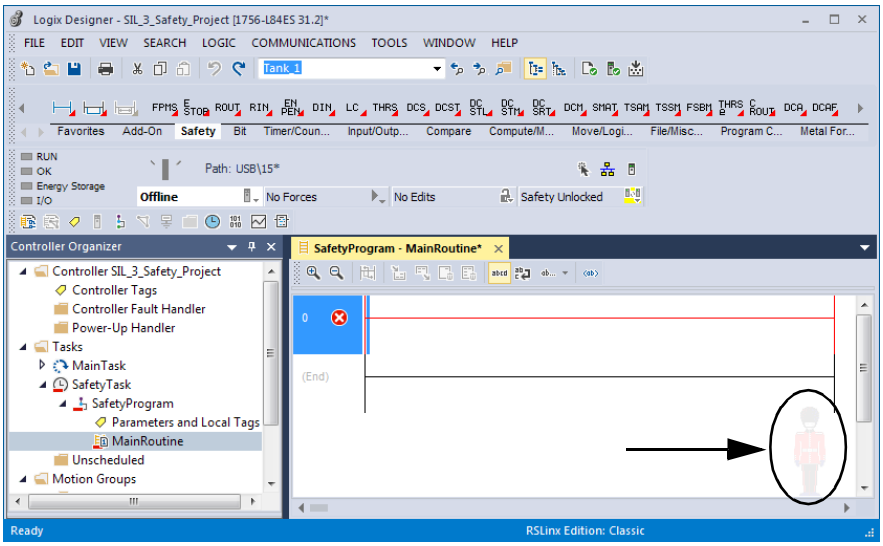
- A safety program can also define program-scoped safety tags.
- A safety program can be scheduled or unscheduled.
- A safety program can contain only safety components.
- All routines in a safety program are safety routines. One safety routine must be designated as the main routine, and another safety routine can be designated as the fault routine.
- A safety program cannot contain standard routines or standard tags.

Safety Routines

Safety routines have the same attributes of standard routines, except for the following:

- Safety routines can exist only in safety programs.
- Safety routines cannot read or write standard tags.
- Safety routines can only be done in Ladder Logic.

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



One safety routine must be designated as the main routine in each safety program. Another safety routine can be designated as the fault routine for that safety program.

Only safety-certified instructions are used in safety routines. For a listing of safety instructions, see Appendix A.

Safety Tags

The GuardLogix control system supports the use of both standard and safety tags in the same project. However, the programming software operationally differentiates standard tags from safety tags.

Safety tags have the same attributes as standard tags with the addition of mechanisms that are certified to provide SIL 2/PLd and SIL 3/PLe data integrity.

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

- Name
- Description (optional)
- Tag type
- Data type
- Scope
- Class
- Style
- External Access
- If the tag value is a constant

The Studio 5000 Logix Designer application helps prevent the direct creation of invalid tags in a safety program. If invalid tags are imported, they cannot be verified.

IMPORTANT You cannot create a standard alias tag of a safety tag. Instead, standard tags can be mapped to safety tags using safety tag mapping. See Safety Tag Mapping on page 79.

The Logix Designer application can write to safety tags directly via the Tag Monitor when the GuardLogix 5580 controller is safety-unlocked, does not have a safety signature, and is operating without safety faults.

The controller does not allow writes to safety tag data from external human machine interface (HMI) devices or via message instructions from peer controllers. HMI devices can have read-only access to safety tags depending on the External Access setting.

Valid Data Types

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

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

Logix controllers contain predefined data types for use with specific instructions. Safety tags can be composed of the following:

- All primitive data types (for example, BOOL, SINT, INT, DINT, LINT, REAL)
- Predefined types used for safety application instructions
- User-defined data types or arrays that are composed of the two preceding types

Scope

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

Controller-scoped safety tags can be read by either standard or safety logic or external communication devices, but can be written by only safety logic or another GuardLogix safety controller.

Program-scoped safety tags can be read by external communication devices, but only local safety routines can write to them. These are routines that reside within the safety program.

When you create program-scoped tags, the class is automatically specified, depending on whether you created the tag in a standard or a safety program. When you create controller-scoped tags, you must manually select the tag class.

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

- Multiple programs in the project
- To produce or consume data
- In safety tag mapping

  See Safety Tag Mapping on page 79 for more information.

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

IMPORTANT Safety input tags and safety consumed tags are readable by any standard routine, but the update rate is based on the execution of the safety task. These tags are updated at the beginning of the safety task execution, which differs from standard tag behavior.

Safety Applications

Safety Concept Assumptions

The safety concept assumes the following requirements:

- If you are responsible to create, operate, and maintain the application, you are fully qualified, specially trained, and experienced in safety systems.
- You apply the logic correctly to detect programming errors through strict adherence to specifications, programming, and naming rules.
- You perform a critical analysis of the application and use all possible measures to detect a failure.
- You confirm all application downloads via a manual check of the safety signature.
- You perform a complete functional test of the entire system before the operational startup of a safety-related system. This test includes, but is not limited to, the following:
  - Validate that the overall functionality of the implemented safety functions, including I/O configuration via Add-On Profiles (AOP), beyond the limits of the individual devices (boundary testing).
  - Verify that the correct versions of software are used.

Table 2 - Effect of Controller Modes on Safety Execution

Controller Mode	Controller Behavior
Program	• Safety input and output connections are established and maintained: – Safety input tags are updated to reflect safety input values. • Safety mapped tags are updated to reflect the standard controller tag values. • Safety Task logic is not being scanned.
Test	• Safety input and output connections are established and maintained: – Safety input tags are updated to reflect safety input values. • Safety mapped tags are updated to reflect the standard controller tag values. • Safety Task logic is being scanned.
Run	• Safety input and output connections are established and maintained: – Safety input tags are updated to reflect safety input values. – The controller sends "run" safety output packets. • Safety mapped tags are updated to reflect the standard controller tag values. • Safety Task logic is being scanned. • All safety task process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.

Table 3 - Safety Application Status

Safety Task Status	Safety[1](Up to and Including)	Controller Behavior
Unlocked No signature	Only for development purposes	• Safety I/O forces can be present. • Safety I/O forces can be modified. • Safety online editing is allowed. • Safety memory is isolated, but is unprotected (read/write). • Download allowed if a major firmware revision of the offline project matches the target GuardLogix© controller.
Locked No signature	Only for development purposes	• Safety I/O forces are not allowed (forces of safety I/O must be removed before locking is possible). • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Download is not allowed.
Unlocked with signature	SIL 3/PLe/Cat. 4 Control reliable	• Safety I/O forces are not allowed. (Forces of safety I/O must be removed before generating a signature is possible.) • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Safety signature is unprotected and anyone who has access to the controller can delete it. • Download allowed if a major firmware revision of the offline project matches the target GuardLogix controller.
Locked with signature	SIL 3/PLe/Cat. 4 Control reliable	• Safety I/O forces are not allowed. • Online editing of the safety task is not allowed. • Safety memory is protected (read-only). • Safety signature is protected. You must enter the unlock password to unlock the controller before you can delete the safety signature. • Download allowed if the major and minor firmware revision and signature of the offline project match the target GuardLogix controller, the project is safety-locked, and the safety task status of the controller is OK. **ATTENTION:** If the controller is safety-locked and the safety-unlock password is lost and a download is needed, you must perform a Stage 1 reset of the controller.

(1) To achieve this level, you must adhere to the safety requirements defined in this safety reference manual.

Basics of Application Development and Testing

We recommend that a system integrator or a user who is trained and experienced in safety applications develop the application program for the intended SIL 2 or SIL 3 system. The developer must follow good design practices:

- Use functional specifications, including flowcharts, timing diagrams, and sequence charts.
- Perform a review of safety task logic.
- Perform application validation.

The Studio 5000® environment is a suite of tools that are certified as an offline tool according to clause 7.4.4 of IEC 61508-3. As you develop your safety application, consider the following:

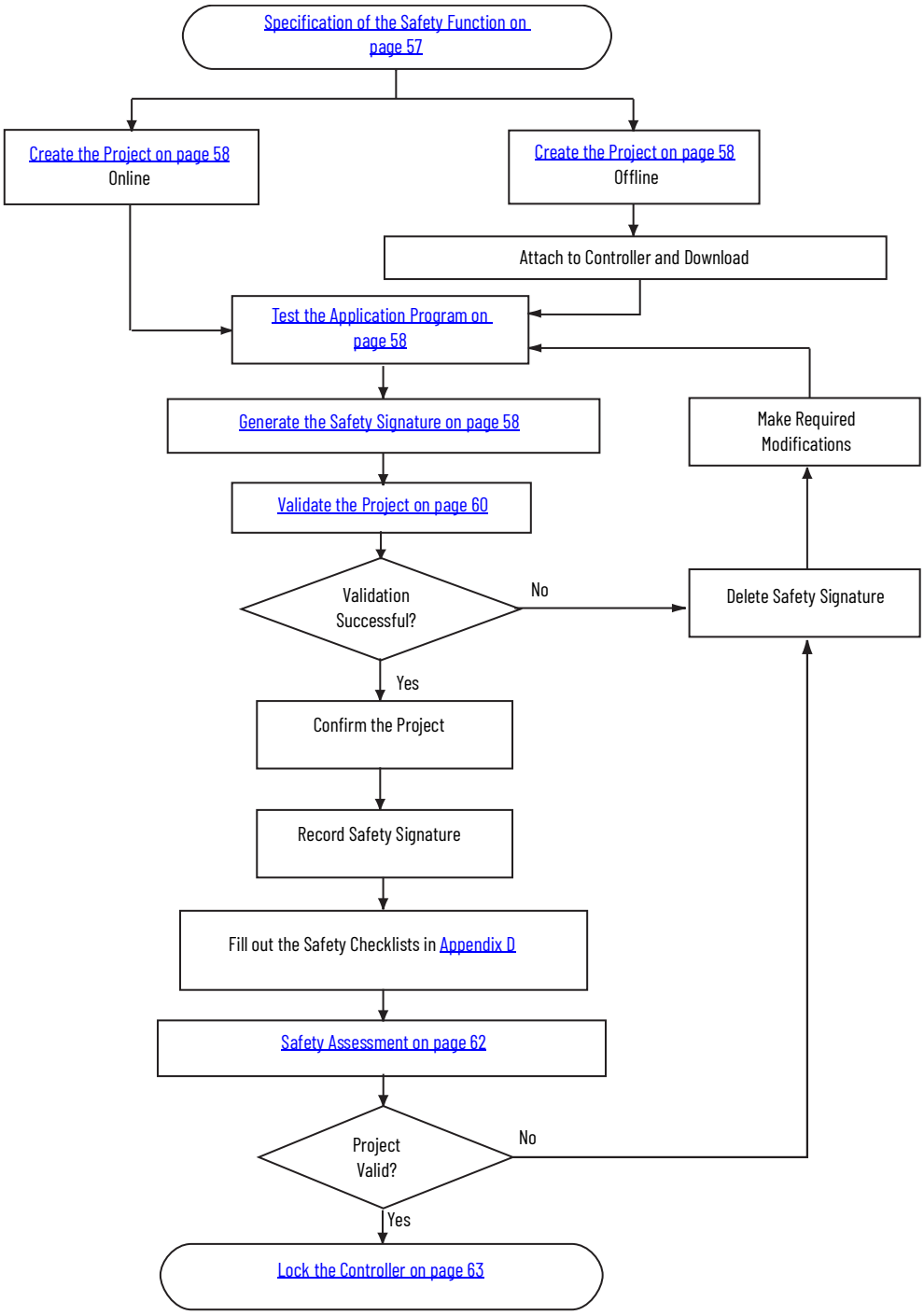
IMPORTANT

- The Studio 5000 Logix Designer® application has been certified to clause 7.4.4 of IEC 61508-3 Edition 2 and can be used during the coding lifecycle of GuardLogix-based applications and also as an aide in the module test, integration test, and validation test lifecycle phases. As a result, no additional justification for its use during those lifecycle phases is required. If, however, other tools are used, either on their own or with the Studio 5000 Logix Designer application, additional justification for those other tools are required. It is your responsibility to verify that other offline tools that are used during all lifecycle phases are selected as a coherent part of the software development activities.
- It is your responsibility to conduct an assessment to determine the level of reliance that is placed on the Studio 5000 Logix Designer application and the potential failure mechanisms that can affect the executable software when the Studio 5000 Logix Designer application is used in a manner other than what is specified in the product documentation.
- You must verify that all programming and configuration information that is entered into the Studio 5000 Logix Designer application, and downloaded to the controller, meets the requirements for your application. See Confirm the Project on page 62 for more information.
- As required by the safety integrity level, the software or design representation must match the characteristics of the application.
- As required by the safety integrity level, the software or design representation must be compatible with the features that are supported in the Studio 5000 Logix Designer application and GuardLogix controllers. It is your responsibility to verify that the desired software and design representation are supported in the Studio 5000 Logix Designer application and GuardLogix controllers. For example, if the design is represented in a flowchart format, it is your responsibility to convert that design to a ladder diagram.
- Use of third-party, or internally developed, tools to generate logic automatically to import into the Studio 5000 Logix Designer application for compilation and download to a GuardLogix controller requires assessment of its suitability at the point in the development cycle where it is selected.

Commissioning Lifecycle

The flowchart shows the steps that are required for commissioning a GuardLogix system. See the links for an explanation of those topics.

Figure 18 - Commission the System



Specification of the Safety Function

You must create a specification for your safety function. Use this specification to verify that program logic correctly and fully addresses the functional and safety control requirements of your application. In some applications, the specification can be presented in various formats. However, the specification must be a detailed description that includes the following (if applicable):

- Sequence of operations
- Flow and timing diagrams
- Sequence charts
- Program description
- Program printout
- Written descriptions of the steps with step conditions and actuators to be controlled, which includes the following:
  - Input definitions
  - Output definitions
  - I/O wiring diagrams and references
  - Theory of operation
- Matrix or table of stepped conditions and the actuators to be controlled, including the sequence and timing diagrams
- Definition of marginal conditions, for example, operating modes and emergency stop

The I/O portion of the specification must contain the analysis of field circuits, that is, the type of sensors and actuators.

- Sensors (Digital or Analog)
  - Signal in standard operation (dormant current principle for digital sensors, sensors OFF means no signal)
  - Determination of redundancies that are required for SIL levels
  - Discrepancy monitoring and visualization, including your diagnostic logic
- Actuators
  - Position and activation in standard operation (normally ON)
  - Safe reaction/positioning when switching OFF or power failure
  - Discrepancy monitoring and visualization, including your diagnostic logic

Create the Project

The logic and instructions that are used in programming the application must be the following:

- Easy to understand
- Easy to trace
- Easy to change
- Easy to test

Review and test all logic. Keep safety-related logic and standard logic separate.

Label the Program

Use these labels to identify the application program clearly:

- Name
- Date
- Revision
- Any other useful identification

Test the Application Program

This step consists of any combination of Run and Program modes, online or offline edits, upload and download, and informal testing that is required to get an application to run properly in preparation for the Project Validation test.

Generate the Safety Signature

ATTENTION: The safety signature is required for the controller to operate at a SIL 2 or SIL 3 rating. Running without a safety signature is only suitable during development.

IMPORTANT One of the following editions of the Studio 5000 Logix Designer application must be present to generate a safety signature: Professional, Full, Lite Edition or a separate 9324-RLDGLXE GuardLogix Editor.

Once the application program tests are complete and before verification testing, you must generate the safety signature. The programming software automatically uploads the safety signature after it is generated.

The safety signature is composed of a safety signature ID (identification number), and a time stamp (date and time). The safety signature ID applies to the entire safety portion of the controller and uniquely identifies each project, including its logic, constant data, and configuration.

You can generate the safety signature if the following conditions are true:

- The Studio 5000 Logix Designer application is online with the controller.
- The controller is in Program mode.
- The controller is safety-unlocked.
- The controller has no safety forces or pending online safety edits.
- The safety task status is OK.

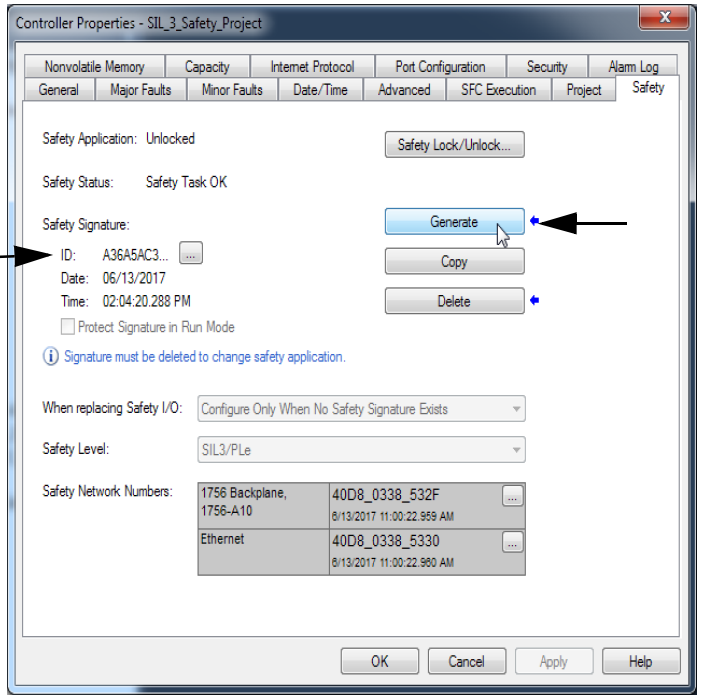
IMPORTANT When the safety application has been validated, there can be occasions that require a redownload (such as editing the Standard application) even though the Safety application has not changed.
To verify that the correct safety application is downloaded, manually record the safety signature after initial creation and check the safety signature after every download to make sure that it matches the original.

To generate the safety signature from the Safety tab of the Controller Properties dialog box, click Generate.

Figure 19 - Generate Safety Signature

For the safety signature, GuardLogix 5580 controllers have a 32 byte ID. Only the first 4 bytes of the ID display on the tab.

To view and copy the entire 32 byte ID, click ... to open the Safety Signature ID dialog box.



In the Logix Designer application, you can also choose Tools > Safety > Generate Signature.

You can view the safety status via the safety status button on the online bar, or on the Safety tab of the Controller Properties dialog box.

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

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

- Online/offline programming or editing (including safety Add-On Instructions)
- Force safety I/O
- Change the inhibit state of safety I/O or producer controllers
- Safety data manipulation (except by safety routine logic)
- Download a new safety application

You cannot update the firmware when a safety signature exists.

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.

Click Copy to copy the ID, Date, and Time components to the Windows® clipboard.

Delete the Safety Signature

ATTENTION: If you delete the safety signature, you must retest and re-validate your system to meet SIL2/PLd or SIL 3/PLe.

To delete the safety signature, click Delete. The safety signature cannot be deleted when the following is true:

- The controller is safety-locked.
- The controller is in Run mode with the keyswitch in RUN.
- The controller is in Run or Remote Run mode with Protect Signature in Run Mode enabled.

Validate the Project

To check your application program for adherence to the specification, you must generate a suitable set of test cases that cover the application. The set of test cases must be filed and retained as the test specification.

You must include a set of tests to prove the validity of the calculations (formulas) used in your application logic. Equivalent range tests are acceptable. These are tests within the defined value ranges, at the limits, or in invalid value ranges. The necessary number of test cases depends on the formulas that are used and must comprise critical value pairs.

Active simulation with sources (field devices) must also be included, as it is the only way to verify that the sensors and actuators in the system are wired correctly. Verify the operation of programmed functions by manipulating sensors and actuators manually.

You must also include tests to verify the reaction to wiring faults and network communication faults.

Project validation includes tests of fault routines, and input and output channels, to be sure that the safety system operates properly.

To perform a project validation test on the GuardLogix controller, you must perform a full test of your application. You must toggle each sensor and actuator that is involved in every safety function. Be sure to test all shutdown functions, because these functions are not typically exercised during normal operation.

Also, know that a project validation test is valid only for the specific application tested. If the safety application is moved to another installation, you must perform startup and project validation on the safety application in the context of the new sensors, actuators, wiring, networks, and control system physical equipment.

Revalidation Considerations

The IEC 61508 functional safety standard requires an impact analysis before you upgrade or modify components in a certified, functional safety system. Reference the standard to make sure that you fulfill all requirements as they relate to your application. Consider the following high-level information for impact analysis of safety controller software, hardware, and firmware modification:

- All major and minor firmware releases for GuardLogix controller systems are certified for use in safety applications. As part of the certification process, Rockwell Automation tests the safety-related firmware functions, such as the CIP Safety™ communication subsystems, embedded safety instruction execution, and safety-related diagnostic functions. The firmware release notes identify changes to safety-related functions.
- Perform an impact analysis of the planned modifications.
  - Review the firmware release notes for changes in safety-related functionality.
  - Review the hardware and firmware compatibility in the Product Compatibility and Download Center (PCDC) to identify potential compatibility conflicts.
  - Plan, analyze, and document the impact of any modification, enhancement, or adaptation of your validated safety system.
  - As part of the upgrade process, remove and regenerate the safety signature.
- Based on the results of the safety impact analysis, choose the appropriate level of hardware and software revalidation.

IMPORTANT The compiler for GuardLogix 5580 and Compact GuardLogix 5380 controllers is different than the compiler for earlier controllers. Be sure that applications for earlier controllers compile correctly on GuardLogix 5580 and Compact GuardLogix 5380 controllers.

Confirm the Project

You must print or view the project, and compare the uploaded safety I/O and controller configurations, safety data, and safety task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

If your application program contains a safety Add-On Instruction that has been sealed with an instruction signature, you must also compare the instruction signature, date/time, and safety instruction signature to the values you recorded when you sealed the Add-On Instruction.

For information about the creation and use of safety Add-On Instructions in SIL 3 applications, see Appendix B.

The following steps illustrate one method for confirming the project.

1. While online with the controller, and with the controller in Program mode, save the project.
2. Answer Yes to the Upload Tag Values prompt.
3. With the Studio 5000 Logix Designer application offline, save the project with a new name, such as Offlineprojectname.ACD, where 'projectname' is the name of your project. This file is the new tested master project file.
4. Close the project.
5. Move the original project archive file out of its current directory. You can delete this file or store it in an archival location. This step is required because if the Studio 5000 Logix Designer application finds the projectname.ACD in this directory, it correlates it with the controller project and does not perform an actual upload.
6. With the controller still in Program mode, upload the project from the controller.
7. Save the uploaded project as Onlineprojectname.ACD, where 'projectname' is the name of your project.
8. Answer Yes to the Upload Tag Values prompt.
9. Use the Studio 5000 Logix Designer Program Compare utility to perform these comparisons:
   - Compare all properties of the GuardLogix controller and CIP Safety™ I/O devices.
   - Compare all properties of the safety task, safety programs, and safety routines.
   - Compare all logic in the safety routines.
10. Verify that all controller and I/O configuration fulfills the requirements of your application specification.

Safety Assessment

An independent, third-party review of the safety system can be required before the system is approved for operation. An independent, third-party certification can be required for IEC 61508 SIL 2 or SIL 3 levels.

Lock the Controller

ATTENTION: Safety-locking alone does not satisfy SIL 2/PLd or SIL 3/PLe requirements.

The default state of the controller is safety-unlocked. We recommend that you safety-lock the GuardLogix controller to help protect safety control components from modification and help prevent the safety signature from being deleted accidentally. However, safety-locking the controller is not a requirement for SIL 2 or SIL 3.

The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety tags, safety Add-On Instructions, safety I/O, and safety signature.

No aspect of safety can be modified while the controller is in the safety-locked state. When the controller is safety-locked, the following actions are not permitted in the safety task:

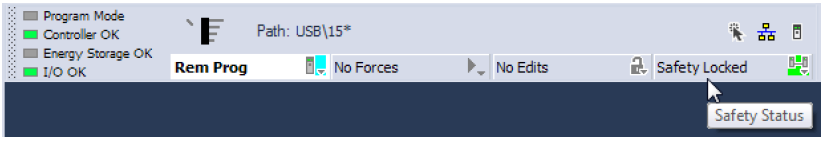
- Update the firmware
- Online or offline programming or editing
- Forcing safety I/O
- Data manipulation of safety components (except through routine logic or another GuardLogix controller)
- Creating or editing safety Add-On Instructions
- Generating or deleting the safety signature

IMPORTANT If a safety signature exists and the controller is safety-locked, only projects with a matching safety signature can be downloaded to the controller.

You can place the safety application in a safety-locked state regardless of whether you are online, offline, or you have the original program source. However, no safety forces or pending safety edits can be present. Safety-locked or -unlocked status cannot be modified when the keyswitch is in the RUN position.

There are multiple ways to view the safety lock status of the controller:

- The 4-character display on the controller indicates lock status.
- In the Logix Designer application, the text of the online bar's safety status button indicates the safety-lock status.



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

 = controller safety-locked

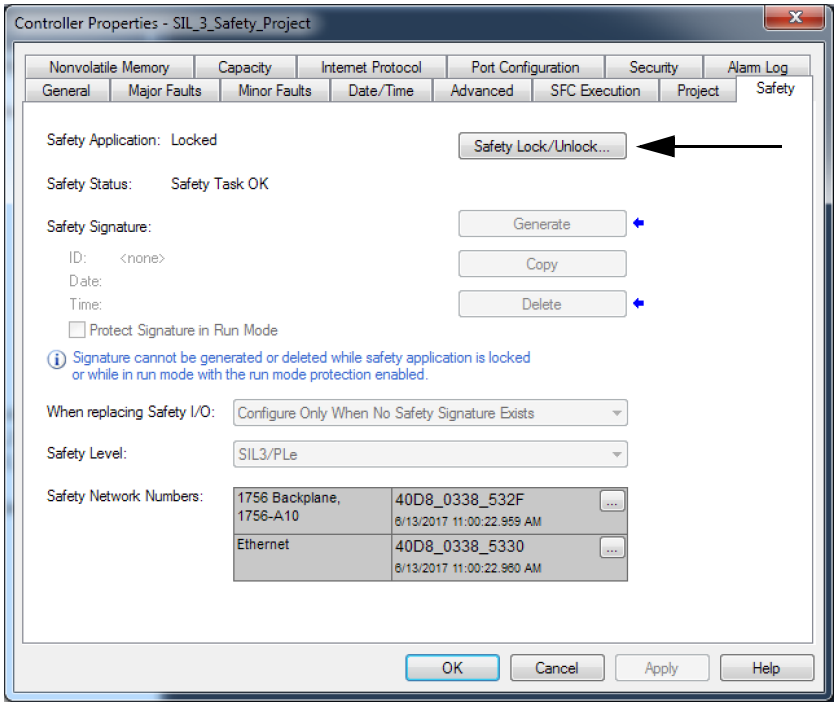
 = controller safety-unlocked

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

For more information on accessing the controller log, refer to the Logix 5000 Controllers Information and Status Programming Manual, publication 1756-PM015.

You can safety-lock and -unlock the controller from the Safety tab of the Controller Properties dialog box.

Figure 20 - Safety-lock the Controller

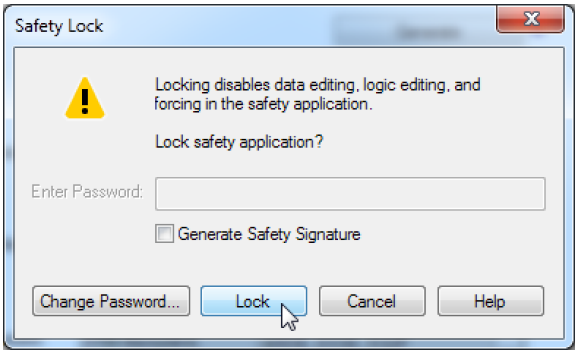


In the Logix Designer application, you can also choose Tools > Safety > Safety Lock/Unlock.

To provide an additional layer of protection, separate passwords can be used to safety-lock or -unlock the controller. Passwords are optional.

If you set a password for the safety-lock feature, you must type it in the Enter Password field. Otherwise, click Lock.

Figure 21 - Safety-locking the Controller

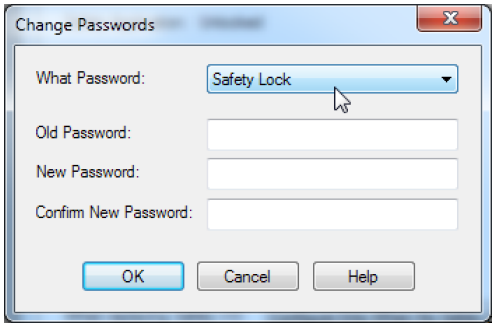


You can also set or change the password from the Safety Lock dialog box.

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

To set passwords, follow these steps.

1. On the Logix Designer menu bar, click Tools > Safety > Change Passwords.
2. From the What Password pull-down menu, choose either Safety Lock or Safety Unlock.



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

Passwords can be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols can be used: ' ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .
To clear an existing password, enter a new password of zero length.

IMPORTANT Rockwell Automation does not provide any form of password or security override services. When products and passwords are configured, Rockwell Automation encourages customers to follow good security practices and to plan accordingly for password management.

Download the Safety Application Program

Upon download, application testing is required unless a safety signature exists.

IMPORTANT To verify that the correct safety application is downloaded or restored from a memory card, you must manually check that the safety signature matches the original signature in your safety documentation.

Downloads to a safety-locked GuardLogix controller are allowed only if the safety signature and the firmware revision of the offline project all match what is contained in the target GuardLogix controller and the safety task status of the controller is OK.

IMPORTANT If the safety signature does not match and the controller is safety-locked, you must unlock the controller to download. In this case, downloading to the controller deletes the safety signature. As a result, you must revalidate the application.

Upload the Safety Application Program

If the GuardLogix controller contains a safety signature, the safety signature is uploaded in an online save of the project. The option to upload tag values includes both standard and safety tag values.

Store and Load a Project from a Memory Card

GuardLogix and Compact GuardLogix controllers support firmware updates, and user program storage and retrieval with a memory card. In a GuardLogix system, only the primary controller uses a memory card.

When you store a safety project on a memory card, we recommend that you select Remote Program as the Load mode, that is, the mode the controller enters following the load. Before actual machine operation, operator intervention is required to start the machine.

You can initiate a load from a memory card only under these conditions:

- If the controller type specified by the project that is stored on the memory card matches your controller type.
- If the major and minor revisions of the project on the memory card match the major and minor revisions of your controller.

  IMPORTANT A revision mismatch helps prevent only user-initiated loads. Controller-initiated loads overwrite the firmware on the controller with the contents of the memory card.

- If your controller is not in Run mode.

Loading a project to a safety-locked controller is allowed only when the safety signature of the project that is stored on the memory card matches the project on the controller. If the signatures do not match or the controller is safety-locked without a safety signature, you must first unlock the controller before attempting to update the controller via a memory card.

IMPORTANT If you unlock the controller and initiate a load from the memory card, the safety-lock status, passwords, and safety signature are then set to the values contained on the memory card once the load is complete.

Force Data

All data that is contained in an I/O, produced, or consumed safety tag, including CONNECTION_STATUS, can be forced while the project is safety-unlocked and no safety signature exists. However, forces must be removed, not just disabled, on all safety tags before the safety project can be safety-locked or a safety signature can be generated. You cannot force safety tags while the project is safety-locked or when a safety signature exists.

You can install and remove forces on standard tags regardless of the safety-locked or unlocked state.

Inhibit a Device

You cannot inhibit or uninhibit safety I/O devices or producer controllers with the Logix Designer application under these conditions:

- The application program is safety-locked
- A safety signature exists

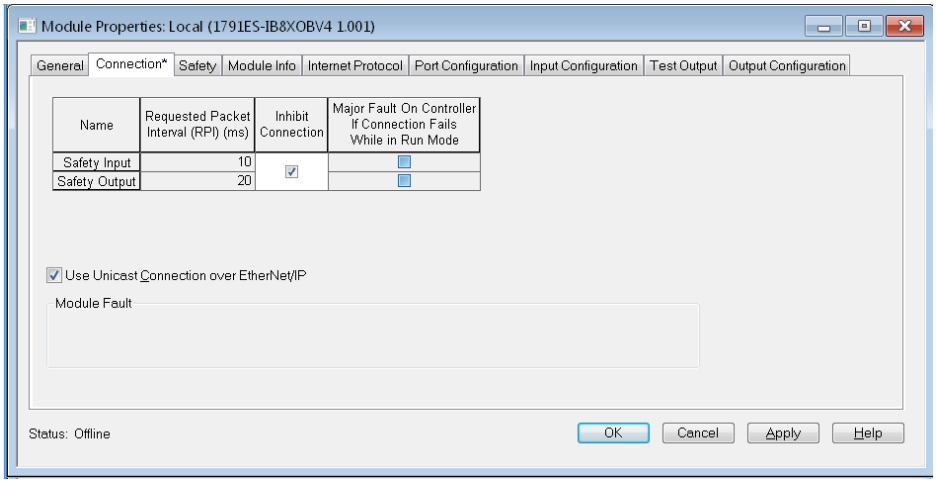
Anytime necessary, you can programmatically inhibit and uninhibit with SSV from the standard task:

- Class Name: Module
- Attribute Name: Mode
- Source: Inhibit = 4; Uninhibit = 0

To inhibit a specific safety I/O device in the Logix Designer application, follow these steps.

1. In the Logix Designer application, right-click the device and choose Properties.
2. On the Module Properties dialog box, click the Connection tab.
3. Check Inhibit Connection and click Apply.

   The device is inhibited whenever the checkbox is checked. If a communication device is inhibited, all downstream devices are also inhibited.



Online Editing

Standard logic online editing is unaffected by the safe state.

Online edits in standard routines are unaffected by the safety-locked or safety-unlocked state.

ATTENTION: Performing an online modification (to logic, data, or configuration) can affect the Safety Function of the system if the modification is performed while the application is running. Online modifications should only be done if necessary. If the modification is not performed correctly, it can stop the application. Therefore, before performing an online modification, alternative safety measures must be used during the update.

Safety logic online editing can only be performed when the controller is safety-unlocked and unsigned. Follow these guidelines for editing safety logic online:

- If the controller is locked with safety edits, you must unlock the controller to assemble or cancel the edits.
- For safety routines, the controller cannot be locked when there is a pending edit, but it can be locked when there is a test edit.

IMPORTANT When changing the instruction configuration parameters of an existing safety instruction, you must transition the controller to Program mode and back to Run mode before the changes take effect.

You cannot edit standard or safety Add-On Instructions while online.

Editing Your Safety Application

The following rules apply to changing your safety application program in the Studio 5000 Logix Designer application:

- Only authorized, specially trained personnel can make program edits. These personnel must use all supervisory methods available, for example, using the controller keyswitch and software password protections.
- When authorized, specially trained personnel make program edits, they assume the central safety responsibility while the changes are in progress. These personnel must also maintain safe application operation.
- When you edit online, you must use an alternate protection mechanism to maintain the safety of the system.
- You must sufficiently document all program edits, which include the following:
  - Authorization
  - Impact analysis
  - Execution
  - Test information
  - Revision information
- If online edits exist only in the standard routines, those edits are not required to be validated before returning to normal operation.
- You must make sure that changes to the standard routine, regarding timing and tag mapping, are acceptable to your safety application.
- You can edit the logic portion of your program while offline or online, as described in the following sections.

Performing Offline Edits

When offline edits are made to only standard program elements, and the safety signature matches following a download, you can resume operation.

When offline edits affect the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before you resume operation.

Figure 22 on page 70 illustrates the process for offline editing.

Performing Online Edits

If online edits affect the safety program, you must revalidate all affected elements of the application, as determined by the impact analysis, before you resume operation. Figure 22 on page 70 shows the process for online editing.

Limit online edits to minor program modifications such as setpoint changes or minor logic additions, deletions, and modifications.

IMPORTANT If you change instruction operands while in Run mode:

- Accept the pending edits.
- Cycle the controller mode from Program to Run for the changes to take effect.

The safety-lock and safety signature features of the GuardLogix controller affect online edits.

See Generate the Safety Signature on page 58 and Lock the Controller on page 63 for more information.

For detailed information on how to edit Ladder Logic in the Studio 5000 Logix Designer application while online, see the Logix 5000 Controllers Quick Start, publication 1756-QS001.

Modification Impact Test

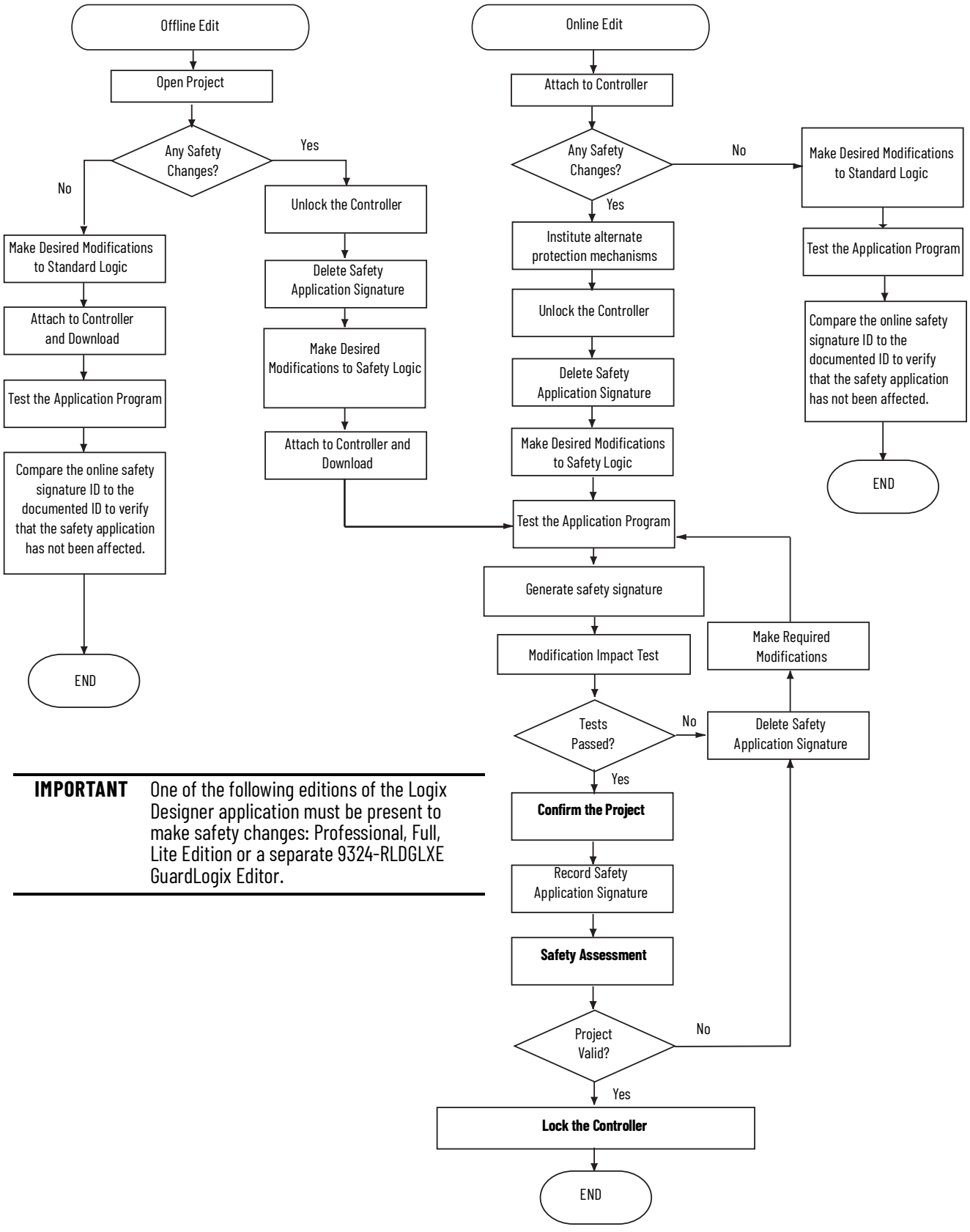
Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system. All appropriate phases of the software safety lifecycle must be conducted as indicated by the impact analysis.

At a minimum, you must perform these actions:

- Functional tests of all impacted software.
- Document all modifications to your software specifications.
- Document all test results.

For detailed information, see IEC 61508-3, Section 7.8 Software Modification

Figure 22 - Online and Offline Edit Process



IMPORTANT One of the following editions of the Logix Designer application must be present to make safety changes: Professional, Full, Lite Edition or a separate 9324-RLDGLXE GuardLogix Editor.

Safety Programming Considerations

Use the Studio 5000 Logix Designer® application to program GuardLogix® safety controllers:

- Define the location, ownership, and configuration of I/O devices and controllers.
- Create, test, and debug program logic. Only ladder diagram is supported in the GuardLogix safety task.

For information on the set of logic instructions available for safety projects, see Appendix A.

IMPORTANT When the GuardLogix controller is in Run or Program mode and you have not validated the application program, you are responsible for maintaining safe conditions.

Programming Restrictions

The Logix Designer application limits the availability of some menu items and features, such as cut, paste, delete, and replace, to protect safety components from being modified whenever any of these are true:

- The controller is safety-locked
- A safety signature exists
- Safety faults are present
- Safety status is in any of these states when online:
  - Partner missing
  - Partner unavailable
  - Hardware incompatible
  - Firmware incompatible

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

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

- Create or modify safety objects, including safety programs, safety routines, safety tags, safety Add-On Instructions, and safety I/O devices
- Apply forces to safety tags
- Create safety tag mappings
- Modify or delete tag mappings
- Modify or delete user-defined data types that are used by safety tags
- Modify the controller name, description, chassis type, slot, and safety network number
- Create, modify, or delete a safety connection

When the controller is safety-locked, you cannot modify or delete the safety signature.

Safety Add-On Instructions

You can create safety Add-On Instructions to be used in Safety applications. Safety Add-On Instructions feature a safety instruction signature for use in safety-related applications up to and including SIL 2-rated applications.

For more information, see the Logix 5000 Controllers Add On Instructions Programming Manual, publication 1756-PM010.

Program Parameters

For program parameters, a safety parameter cannot be connected with or bound to a standard parameter or controller-scoped tag.

For information on program parameters, see Program Parameters on page 137.

Produced/Consumed Safety Tags

To transfer safety data between GuardLogix controllers, you use produced and consumed safety tags.

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

Table 4 - Produced and Consumed Connections

Tag	Connection Description
Produced	GuardLogix 5580 controllers can produce (send) safety tags to other GuardLogix controllers: • GuardLogix 5580 controllers only support unicast produced tags. • GuardLogix 5580 controllers do support producing a tag to up to 15 consumers if all consumers are configured to consume the tag unicast. • The producing controller uses one connection for each consumer. • The consuming controller must be at firmware revision 19 or later. Unicast was not added to safety produced/consumed tags until firmware revision 19.
Consumed	GuardLogix 5580 controllers can consume (receive) safety tags from other GuardLogix controllers in these configurations: • If you have a GuardLogix 5580 controller (the producer) in the I/O tree of another GuardLogix 5580 controller (the consumer), then the consumer can only consume a tag from the producer if the tag is unicast. • If the producer controller is a GuardLogix 5570 controller, then a GuardLogix 5580 consumer controller can consume multicast or unicast tags. • Each consumed tag consumes one connection.

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

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

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

Configure the SNN for a Peer Safety Controller Connection

The peer safety controller is subject to the same configuration requirements as the local safety controller. The peer safety controller must also have a safety network number (SNN).

The safety application that is downloaded into the peer safety controller configures SNN values for each CIP Safety™ port on the controller.

Table 5 - SNN and Controller Placement

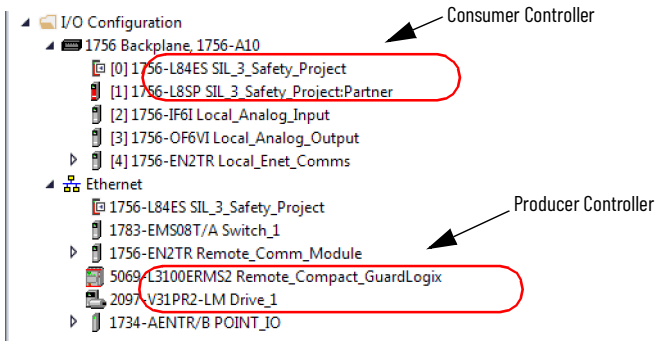
Peer Safety Controller Location	SNN
Placed in the local chassis	The user application on the peer controller generates an SNN value for the local backplane port of the controller.
Placed in another chassis	The controller must have a unique SNN.

For an explanation of the Safety Network Number, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

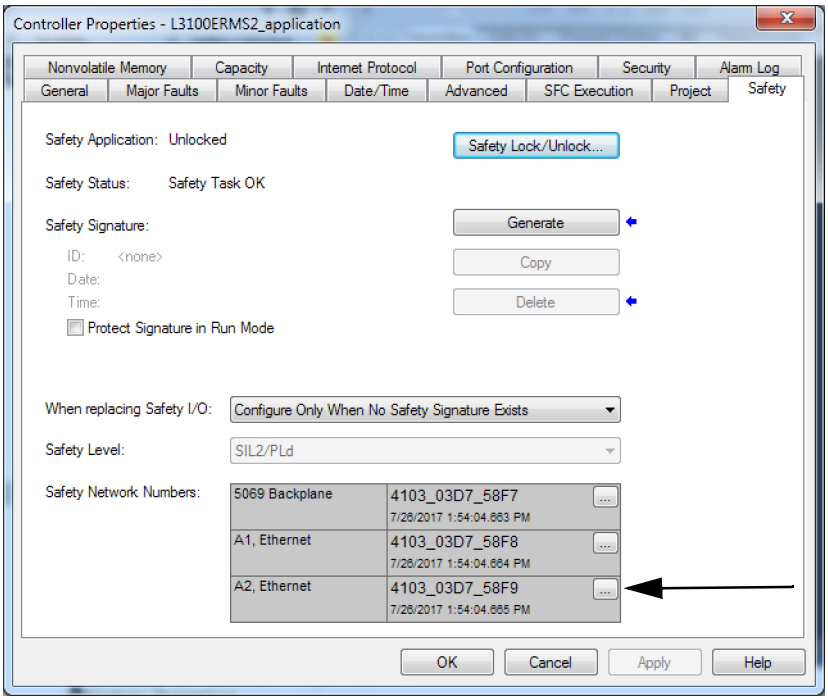
If the automatically assigned SNN of the producer controller does not match the SNN the controller actually uses, you can follow these steps to copy and paste the SNN.

Setting the correct SNNs of the controller as described in Assign the Safety Network Number (SNN) on page 55 usually results in the producer controller being assigned the correct SNN. In these cases you need not perform this procedure.

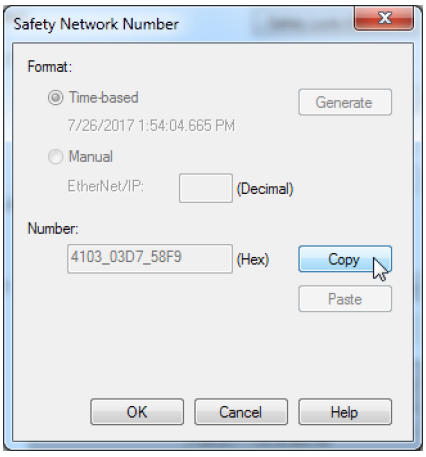
1. Add the producer controller to the consumer controller's I/O tree.



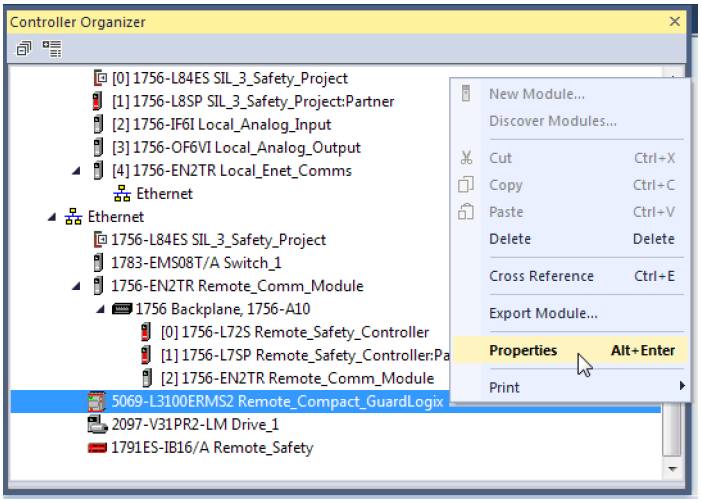
2. In the producer controller's project, right-click the producer controller and choose Controller Properties.
3. On the Safety tab, click the ... next to the port (Ethernet or Backplane) that communicates with the consumer controller. This opens the Safety Network Number dialog box.



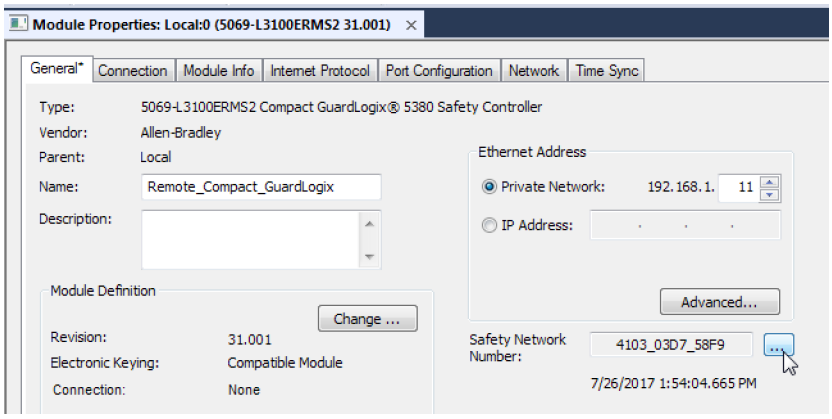
4. Copy the producer controller's SNN.



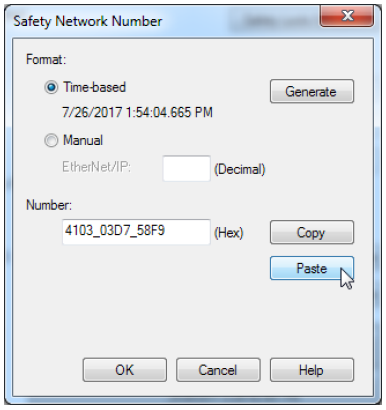
5. In the I/O tree of the consumer controller's project, right-click on the module that represents the producing controller, and choose Module Properties.



6. On the Module Properties General tab, click ... to open the Safety Network Number dialog.

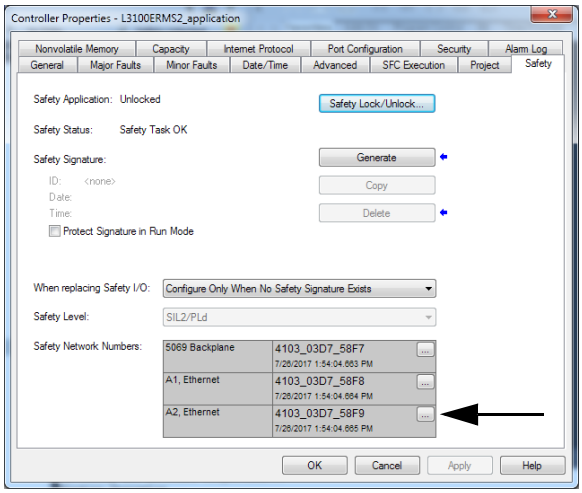


7. Paste the producer controller's SNN into the SNN field and click OK.

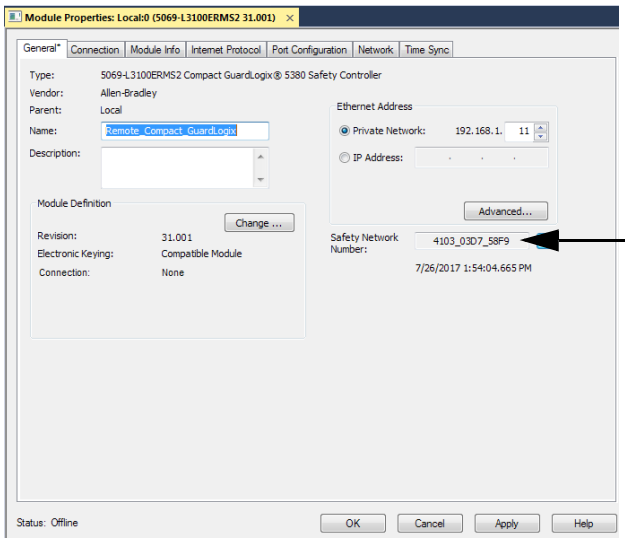


The safety network numbers match.

Producer Controller Properties Dialog Box in Producer Project



Module Properties Dialog Box in Consumer Project

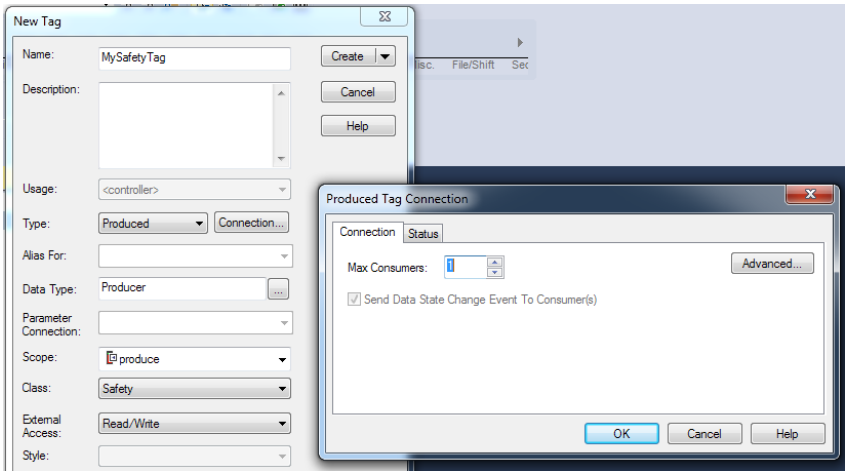


Produce a Safety Tag

Complete these steps to produce a safety tag.

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

   Make sure that the first data member is of the CONNECTION_STATUS data type.
2. Right-click Controller Tags and choose New Tag.
3. Set the type as Produced, the class as Safety, and the Data Type to the user-defined data type you created in step 1.
4. Click Connection and enter the max limit on the number of consumers (1...15).



5. Click OK.
6. Click Create.

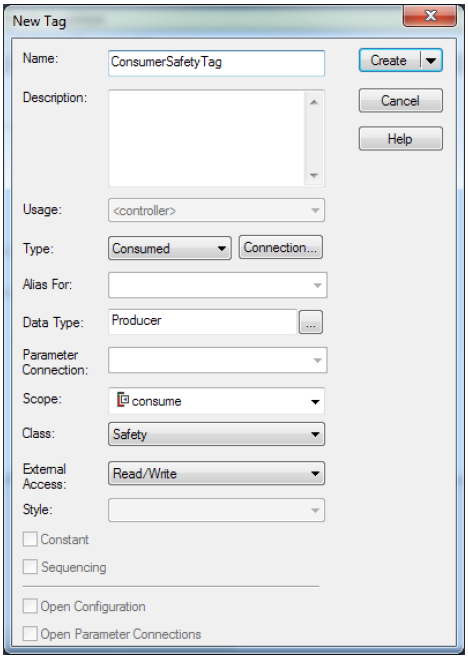
Consume Safety Tag Data

Follow these steps to consume data produced by another controller.

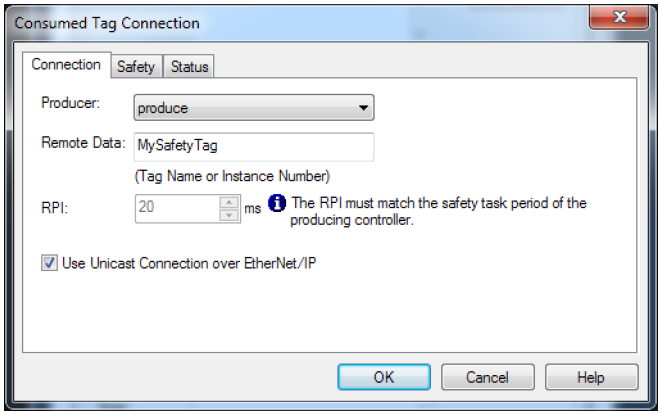
1. In the consumer controller's project, create a user-defined data type identical to the one created in the producer project (the names of the user-defined data types must match).

   The user-defined data type can be copied from the producer project and pasted into the consumer project.
2. Right-click Controller Tags and choose New Tag.

3. Set the Type as Consumed, the Class as Safety, and the Data Type to the user-defined data type you created in step 1.



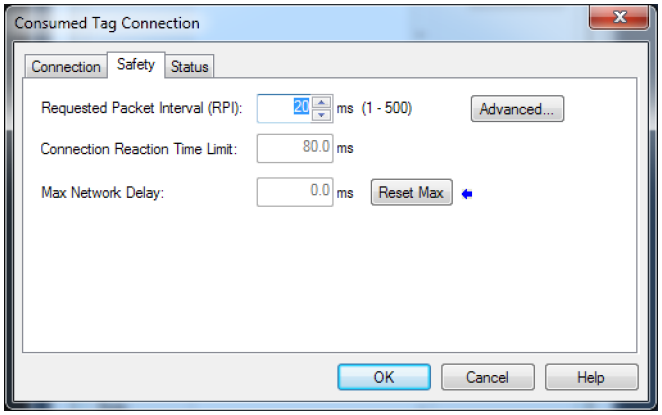
4. Click Connection to open the Consumed Tag Connection dialog box.



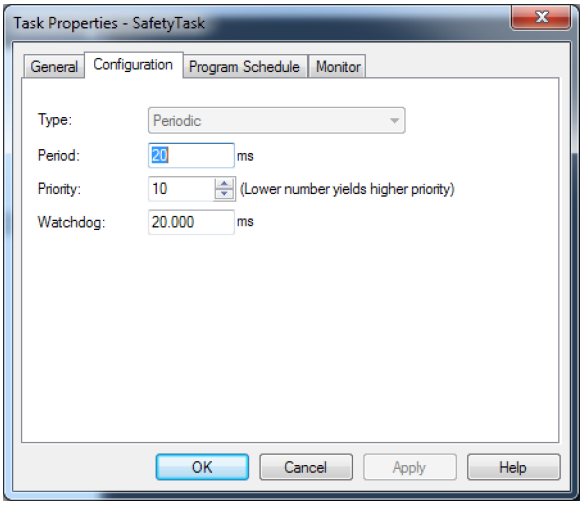
5. From the Producer pull-down menus, select the controller that produces the data.
6. In the Remote Data field, enter the name of the produced tag.
7. Click the Safety tab.

8. In the Requested Packet Interval (RPI) field, enter the RPI for the connection in 1 ms increments. The default is 20 ms.
   - The RPI specifies the period when data updates over a connection. The RPI of the consumed safety tag must match the safety task period of the producing safety project.

Consumer's Project



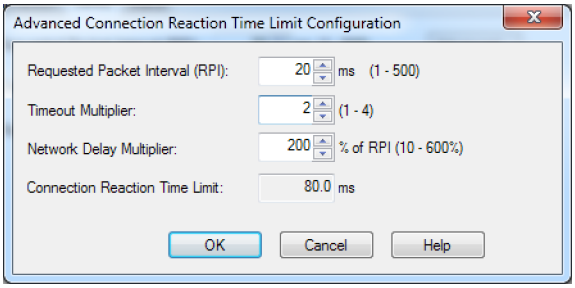
Producer's Project



   - The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. For simple timing constraints, you can achieve an acceptable Connection Reaction Time Limit by adjusting the safety task period of the producing controller which adjusts the RPI.
   - The Max Network Delay is the maximum observed transport delay from the time that the data was produced until the time the data was received. When online, click Reset Max to reset the Max Network Delay.
9. If the Connection Reaction time limit is acceptable, click OK.

   If a safety consumed tag has the error code: "16#0111 Requested Packet Interval (RPI) out of range," check that the consumed tag RPI matches the producer's safety task period.

10. If your application has more complex requirements, click Advanced on the Safety tab to access the Advanced Connection Reaction Time Limit parameters.



   - The Timeout Multiplier determines the number of RPIs to wait for a packet before declaring a connection timeout.
   - The Network Delay Multiplier defines the message transport time that is enforced by the CIP Safety protocol. The Network Delay Multiplier specifies the round-trip delay from the producer to the consumer and back to the producer.

   You can use the Network Delay Multiplier to increase or decrease the Connection Reaction Time Limit.

ATTENTION: If you decrease the timeout multiplier or network delay multiplier below the defaults, this could cause nuisance safety connection losses. Wireless networks can require you to increase the values above the default.

Table 6 - More Resources

Resource	Description
GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM 012	Provides more information on setting the RPI and understanding how the Max. Network Delay, Timeout Multiplier, and Network Delay Multipliers affect the Connection Reaction Time
Monitor Safety Connections on page 95	Contains information on the CONNECTION_STATUS predefined data type
Logix 5000 Controllers Produced and Consumed Tags Programming Manual, publication 1756-PM011	Provides detailed information on using produced and consumed tags

Safety Tag Mapping

Standard Tags in Safety Routines (Tag Mapping)

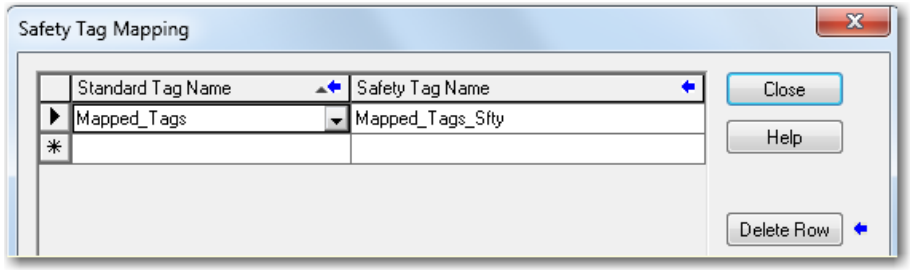
A safety routine cannot directly access standard tags. To allow standard tag data to be used within safety task routines and synchronize standard and safety actions, the GuardLogix controllers provide a safety tag mapping feature that lets standard tag values be copied into safety task memory.

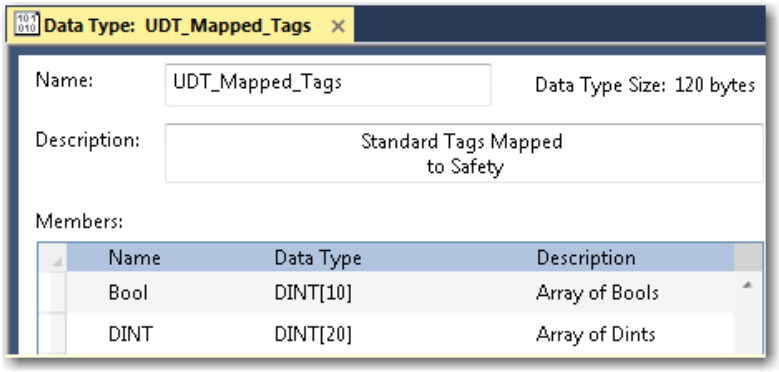
Mapped tags are copied from the standard tags to their corresponding safety tags at the beginning of the safety task. This can increase the safety task scan time.

Standard task routines can directly read safety tags.

Because a download is required to change tag mapping, mapping a structure of information provides programming standardization and flexibility during commissioning. See the example in Figure 23.

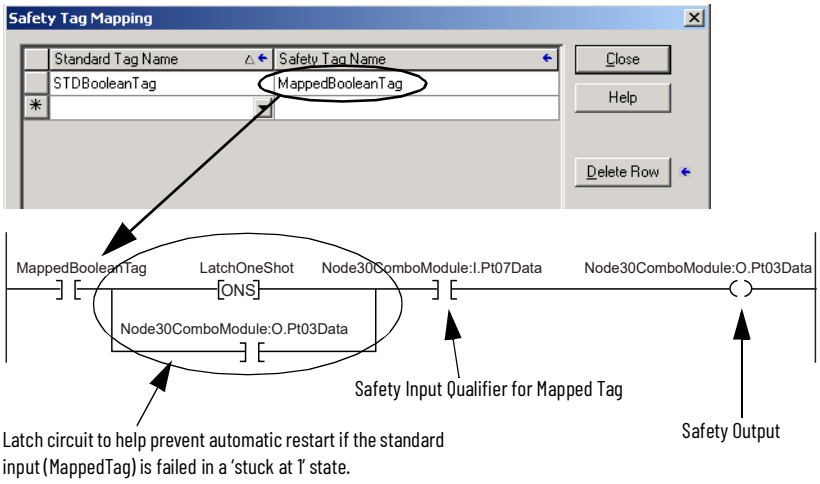
Figure 23 - Mapped Tag Structure





ATTENTION: When you use standard data in a safety routine, you are responsible for providing a more reliable means to make sure that the data is used in an appropriate manner. The use of standard data in a safety tag does not make it safety data. You must not try to prevent safety function operation with standard tag data.
This example illustrates how to qualify the standard data with safety data.

Qualify Standard Data with Safety Data



Restrictions

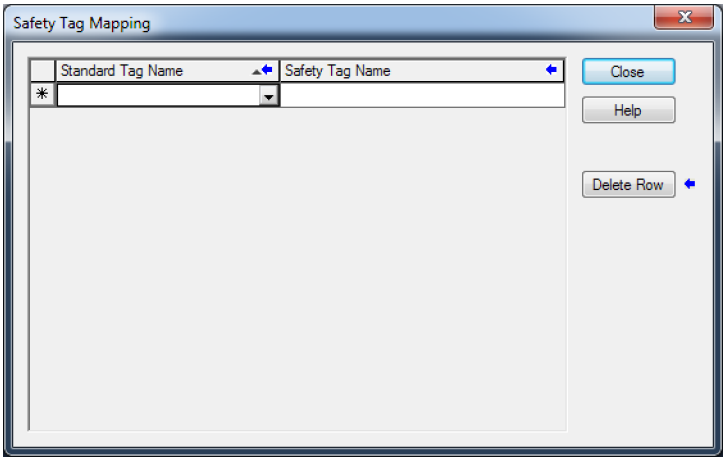
Safety tag mapping is subject to these restrictions:

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

ATTENTION: When using standard data in a safety routine, you must verify that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a SIL 2/PLd or SIL 3/PLe safety output with standard tag data.
For more information, see the GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012.

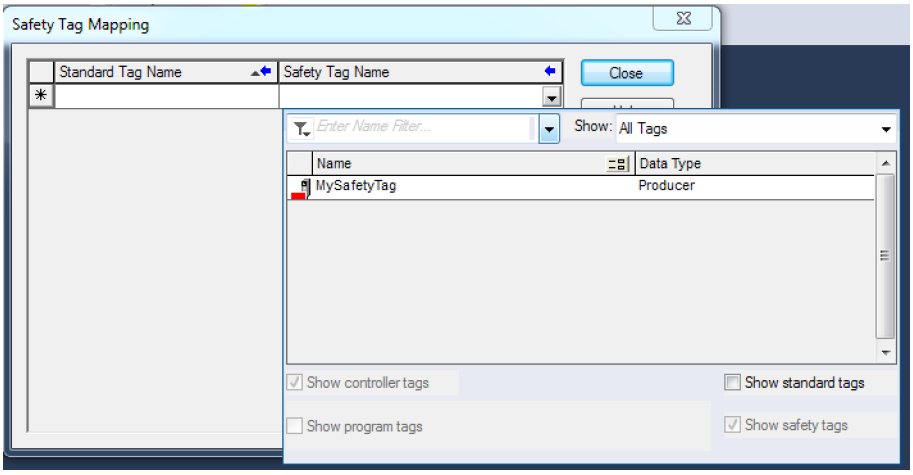
Create Tag Mapping Pairs

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



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

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



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

Monitor Tag Mapping Status

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

Table 7 - Tag Mapping Status Icons

Cell Contents	Description
Empty	Tag mapping is valid.
	When offline, the X icon indicates that tag mapping is invalid. You can move to another row or close the Safety Tag Mapping dialog box.(1) When online, an invalid tag map results in an error message explaining why the mapping is invalid. You cannot move to another row or close the Safety Tag Mapping dialog box if a tag mapping error exists.
	Indicates the row that currently has the focus.
	Represents the Create New Mapped Tag row.
	Represents a pending edit.

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

For more information, see the tag mapping restrictions on page 81.

Custom Tag Initialization During Prescan

Only safety tags that are configured as constant value tags are captured as part of the safety signature.

IMPORTANT When you use non-constant safety tag values for a safety critical operation, you must initialize the non-constant safety tags before Run mode.

Give special consideration to instructions that use pseudo-operands, such as the following:

- .PRE value for TON, TOF, RTO, CTD and CTU
- .LEN value for FAL and FSC.

Unless modified by the application, pseudo-operands are initialized only once when the application is downloaded. For details, see the “Pseudo-operand Initialization” online Help topic.

Before the controller is in Run mode, you must initialize the .PRE and .LEN values for the preceding instruction tags and other non-constant safety tags that are used in a safety critical operation. Initialize these values by using one of these methods:

- A first scan subroutine
- An Add-On Instruction prescan routine

For more information about how to perform a custom tag initialization during prescan, see the Logix 5000 Controllers Design Considerations Reference Manual, publication 1756-RM094.

The following example describes how to use the SaveSnapshot routine to copy non-constant safety tag values to the safetyPrescanInitUDT backup, which consists of safety tag types, such as CTU preset, FAL length, TON preset, DINT array, REAL, and BOOL.

EXAMPLE Once the application is downloaded and configured, toggle the saveSnapshot tag to call the SaveSnapshot routine to initialize safetyPrescanInitUDT.

Upon subsequent transitions to RUN mode, the prescan routine of safetyPrescanInitAOI reinitializes the non-constant safety tag values from the safetyPrescanInitUDT backup.

Figure 24 - Main Routine

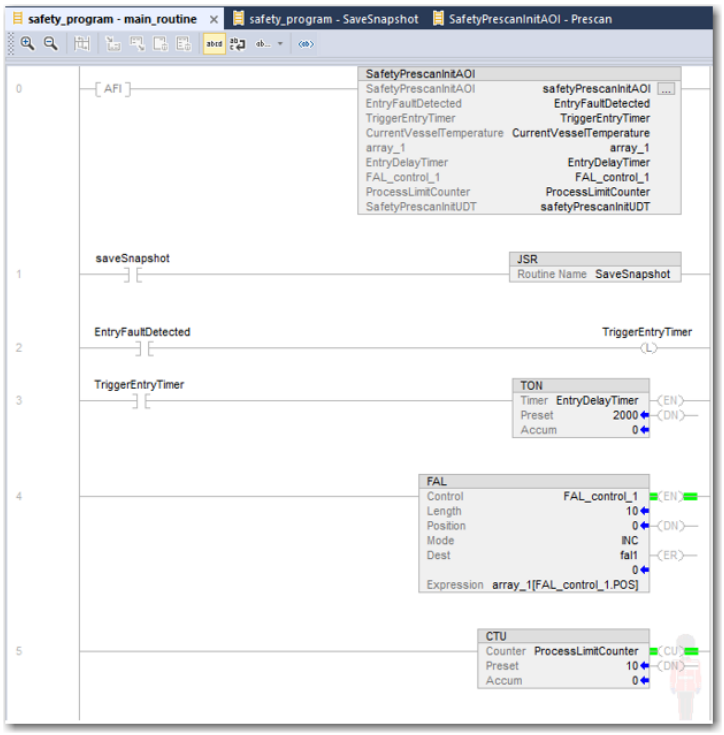


Figure 25 - SaveSnapshot Routine

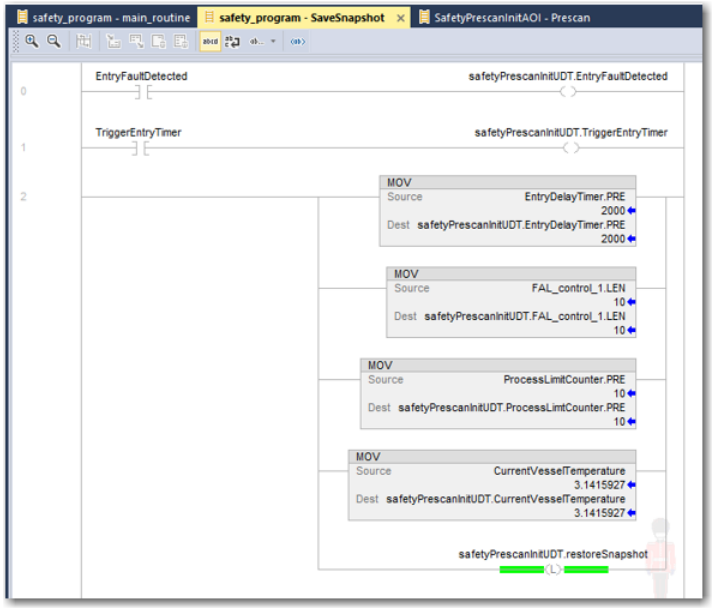
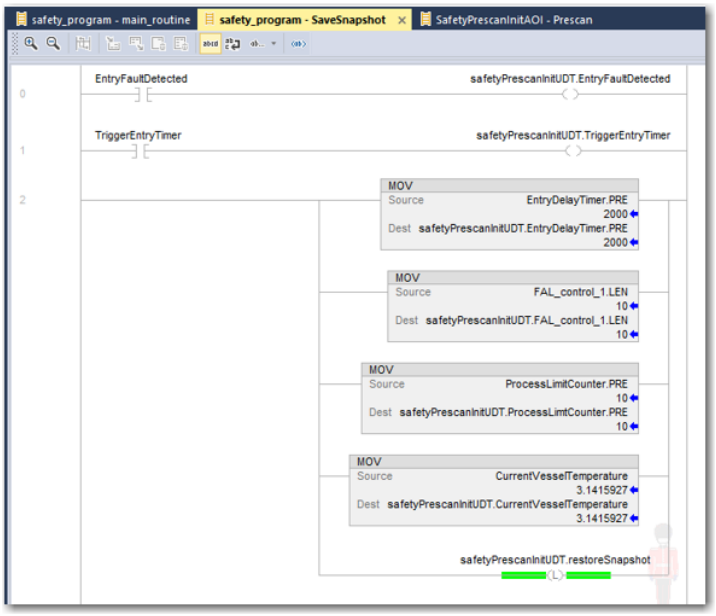


Figure 26 - Add-On Instruction Prescan Initialization Routine



Notes:

Monitor Status and Handle Faults

The GuardLogix® architecture provides you with many ways to detect and react to faults in the system. The first way that you can handle faults is to verify that you have completed the checklists for your application as described in Appendix D.

Status Indicators

For details on status indicator operation, see the user manual for the controller:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

IMPORTANT Status indicators do not provide excellent reliability for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

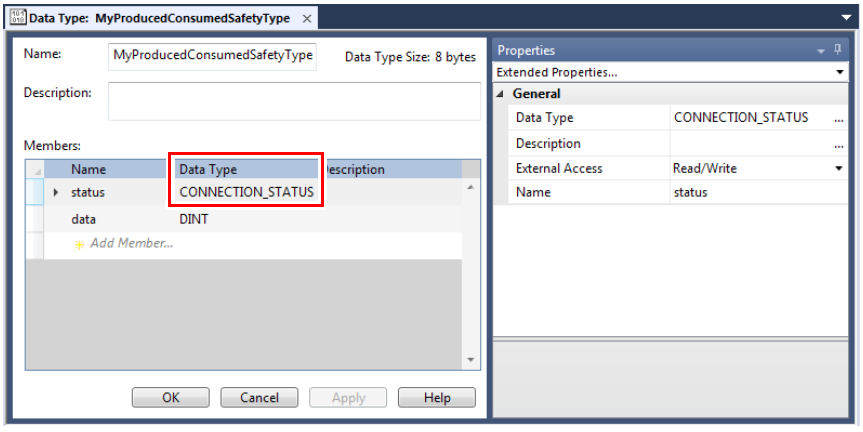
Monitor System Status

You can view the status of safety tag connections. You can also determine current operating status by interrogating various device objects. It is your responsibility to determine what data is most appropriate to initiate a shutdown sequence.

CONNECTION_STATUS Data

The first member of the tag structure that is associated with safety input data and produced/consumed safety tag data contains the status of the connection. This member is a pre-defined data type called CONNECTION_STATUS.

Figure 27 - Data Type Dialog Box



The first 2 bits of the CONNECTION_STATUS data type contain the RunMode and ConnectionFaulted status bits of a device. Table 8 describes the combinations of the RunMode and ConnectionFaulted states.

Table 8 - Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	The producing device is actively controlling the data. 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 safe state.
0 = Idle	1 = Faulted	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to safe state.
1	1	Invalid state.

ATTENTION: Safety I/O connections and produced/consumed connections cannot be automatically configured to fault the controller if a connection is lost and the system transitions to the safe state. Therefore, if you must detect a device fault to be sure that the system maintains the required SIL level, you must monitor the safety I/O CONNECTION_STATUS bits and initiate the fault via program logic.

Input and Output Diagnostics

Guard I/O™ modules provide pulse test and monitoring capabilities. If the module detects a failure, it sets the offending input or output to its safe state and reports the failure to the controller. The failure indication is made via input or output status and is maintained for a configurable amount of time after the failure is repaired.

IMPORTANT You are responsible for providing application logic to latch these I/O failures and to verify that the system restarts properly.

I/O Device Connection Status

The CIP Safety™ protocol allows the recipients of I/O data to determine the status of that data:

- The controller detects input connection failures and then sets all input data to the safe state and the associated input status to faulted.
- The output device detects output connection failures and then de-energizes its outputs.
- Generally, the safety controller also has input connections from output devices. The safety controller determines the status of these input connections, but the input connection status is not the primary mechanism to de-energize outputs.

IMPORTANT You are responsible for application logic to latch these I/O failures, and to verify that the system restarts properly.

De-energize to Trip System

GuardLogix controllers are part of a de-energize to trip system, which means that zero is the safe state. Some, but not all, safety I/O device faults cause all device inputs or outputs to be set to safe state. Faults that are associated to a specific input channel result in that specific channel being set to a safe state. For example, a pulse test fault that is specific to channel 0 results in channel 0 input data being set to the safe state. If a fault is general to the device and not to a specific channel, the combined status bit displays the fault status and all device data is set to the safe state.

For information on how to use GuardLogix safety application instructions, see Appendix F and the GuardLogix Safety Application Instructions Safety Set Reference Manual, publication 1756-RM095.

Get System Value (GSV) and Set System Value (SSV) Instructions

The GSV and SSV instructions let you get (GSV) and set (SSV) controller system data that is stored in device objects. When you enter a GSV/SSV instruction, the programming software displays the valid object classes, object names, and attribute names for each instruction. Restrictions exist for using the GSV and SSV instructions with safety components.

IMPORTANT	The safety task cannot perform GSV or SSV operations on standard attributes. The attributes of safety objects that the standard task can write are only for diagnostic purposes. They do not affect safety task execution.

For more information on which safety attributes are accessible via GSV and SSV instructions, see the user manual for your controller:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

For general information about GSV and SSV instructions, see the Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003.

Safety Faults

Faults in the GuardLogix 5580 and Compact GuardLogix 5380 system can be:

- Recoverable controller faults
- Nonrecoverable controller faults
- Nonrecoverable safety faults in the safety application
- Recoverable safety faults in the safety application

Nonrecoverable Controller Faults

These faults occur when the internal diagnostics of the controller discovers a fault. If a nonrecoverable controller fault occurs, standard and safety task execution stops and outgoing connections stop. Safety I/O devices respond to the loss of output data by transitioning to the safe state. Recovery requires that you download the application program again.

Nonrecoverable Safety Faults in the Safety Application

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

When the safety task encounters a nonrecoverable safety fault, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

ATTENTION: Overriding a safety fault does not clear the fault. If you override a safety fault, it is your responsibility to prove that operation of your system is still safe.
You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

Several nonrecoverable safety faults can be cleared, with or without a safety task signature, to enable the safety task to run. The safety task inoperable fault requires that you download the application again for the safety task to run.

Recoverable Safety Faults in the Safety Application

If a recoverable fault occurs in a safety program, the system can halt the execution of the safety task, depending upon if the Program Fault Handler in the safety program (if one exists) handles the fault.

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

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

If the recoverable safety fault is not handled, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to reduce the risk of these faults, rather than handling them at runtime.

ATTENTION: Overriding a safety fault does not clear the fault. If you override a safety fault, it is your responsibility to prove that operation of your system is still safe.
You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault.

View Faults

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

The status display on the controller also shows fault codes with a brief status message. For more information about status indicators, see the following:

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

Fault Codes

GuardLogix 5580 and Compact GuardLogix 5380 controllers show fault codes on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD or MINORFAULTRECORD attribute.

This manual links to Logix 5000 Controller and I/O Fault Codes, publication, 1756-RD001; the file automatically downloads when you click the link.

Develop a Fault Routine for Safety Applications

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

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

ATTENTION: You must provide proof to your certifying agency that your system can continue to operate safely after an override of a safety fault. The occurrence of recoverable faults is an indication that the application code is not protecting itself from invalid data values or conditions. Consider modifying the application to eliminate these faults, rather than handling them at runtime.

The controller supports two levels for handling major faults in a safety application:

- Safety Program Fault Routine
- Controller Fault Handler

Both routines can use the GSV and SSV instructions as described on page 92.

Each safety 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 safety task faults and shuts down.

When the safety task faults, a standard major recoverable fault is also logged, and the controller proceeds to execute the controller fault handler, if one exists. If the controller fault handler handles this fault, then the standard tasks continue to run, even though the safety task remains faulted.

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

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

The Logix 5000 Controllers Major and Minor Faults Programming Manual, publication 1756-PM014, provides details on creating and testing a fault routine.

Use GSV/SSV Instructions in a Safety Application

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

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

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

Access FaultRecord Attributes

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

Table 9 - Parameters for Accessing FaultRecord Attributes

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

Capture Fault Information

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

For more information on using the GSV and SSV instructions in safety applications, refer to the Input/Output Instructions chapter of the Logix 5000 Controllers General Instructions Reference Manual, publication 1756-RM003.

1756-L8SP Safety Partner Fault

The 1756-L8SP safety partner has an OK status indicator.

If the SIL configuration is set to SIL 2, and a Safety Partner is installed in the slot next the Safety Primary, these actions occur:

- On the Safety Partner, the OK status indicator flashes red.
- The controller logs a Type 14, Code 12 minor fault that indicates that the controller is configured for SIL 2, and a Safety Partner is present.
- The Studio 5000 Logix Designer® application refuses to download a SIL 2 application.

Monitor Safety Status

You can use the following to monitor the controller status:

- The Online bar in the Logix Designer application.
- The Safety tab in the Controller Properties dialog box.

View Status via the Online Bar

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

Figure 28 - Status Buttons

Controller Status

When the Controller Status button Rem Prog is selected as shown in Figure 28, the online bar shows the controller's mode (Remote Program) and status (OK). The Energy Storage OK indicator combines the status of the primary controller and the safety partner.

If either or both have an energy storage fault, the status indicator illuminates. The I/O indicator combines the status of standard and safety I/O. The I/O with the most significant error status is displayed next to the status indicator.

Forces status

The Forces Status button No Forces indicates Forces or No Forces. When the button is selected, the online bar shows whether I/O or SFC forces is enabled or disabled and installed or not installed. The ForcesStatus menu contains commands to remove, enable, or disable all forces.

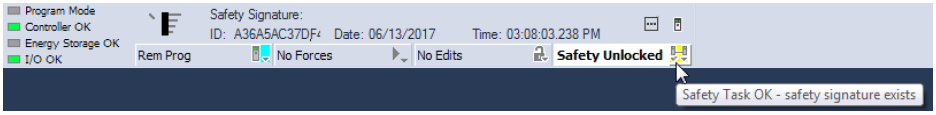
Online Edit status

The Online Edit Status button No Edits indicates whether edits or no edits exist in the online ladder routine or function block diagram. When the button is selected, the online bar shows the edit state of the controller. If edits are made by another user, this area will also shows a textual description of the edits.

Safety Status

When you click the Safety Status button Safety Unlocked, the online bar displays the safety signature.

Figure 29 - Safety Signature Online Display



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

When a safety signature exists, the icons include a small check mark.

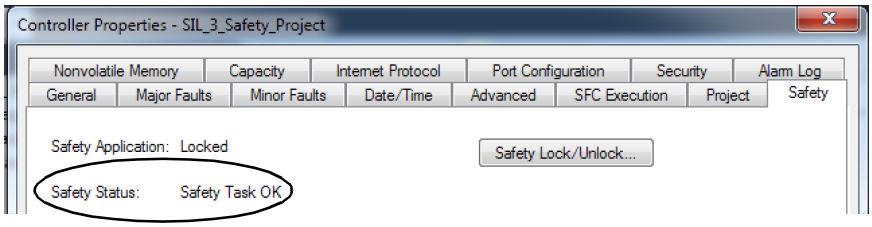
Table 10 - Safety Status Icon

If the safety status is	This icon appears	
	SIL 2/PLd Application, both online and offline	SIL 3/PLe Application
Safety Unlocked		The controller is not safety-locked and online. The controller is not safety-locked and offline.
Safety-locked		The controller is safety-locked and online. The controller is safety-locked and offline.
Safety Faulted		
Safety Task Inoperable	The controller is not safety-locked and the safety task is inoperable The controller is safety-locked and the safety task is inoperable. There is a safety fault and the safety task is inoperable.	

View Status via the Safety Tab

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

Figure 30 - Safety Task Status

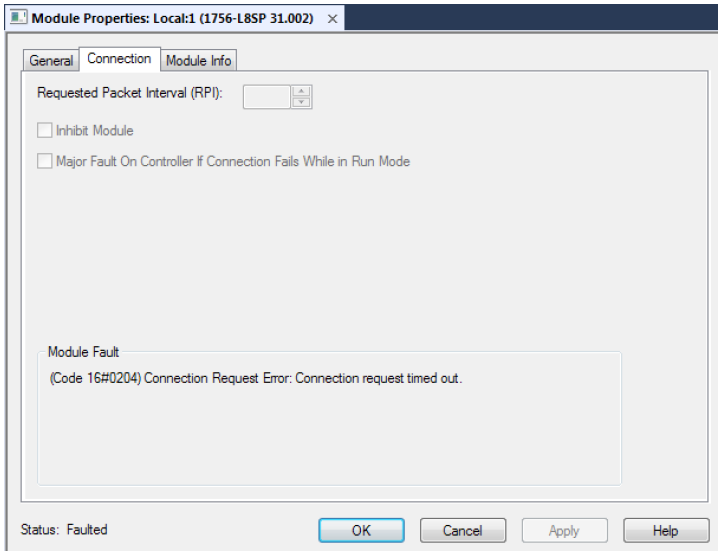


- Safety partner is missing or unavailable (SIL 3).
- Safety partner hardware is incompatible with the primary controller.
- Safety partner firmware is incompatible with the primary controller.
- Safety task inoperable.
- Safety task OK.

Except for safety task OK, the descriptions indicate that nonrecoverable safety faults exist.

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

Figure 31 - Safety Partner Status



Monitor Safety Connections

For tags associated with consumed safety data, you can monitor the status of safety connections by using the CONNECTION_STATUS member. For monitoring input and output connections, safety I/O tags have a connection status member called SafetyStatus. Both data types contain 2 bits: ConnectionFaulted and RunMode.

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) for any reason, the safety data is reset to zero and the RunMode value is set to Idle State (0).

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. For safety I/O connections, the RunMode is always inverse the ConnectionFaulted status. It does not provide unique data.

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

Table 11 - Safety Connection Status

ConnectionFaulted Status	RunMode Status	Safety Connection Operation
0 = Valid	1 = Run	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Valid	0 = Idle	The connection is active and the producing device is in the Idle state. The safety data is reset to zero. This applies to consumed connections only.
1 = Faulted	0 = Idle	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero and the RunMode value is set to Idle State (0).
1 = Faulted	1 = Run	Invalid state.

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

Utilizing Status

Connection Status(.ConnectionFaulted) is the status of the safety connection between the safety controller and safety I/O module. When the connection is operating properly, this bit is LO (0). When the connection is NOT operating properly, this bit is HI (1). When the connection status is HI (connection not operating properly), all other module defined tags are LO and considered invalid data.

Point Status is available for both safety inputs (.PtxxInputStatus) and safety outputs (.PtxxOutputStatus). When a point status tag is HI (1), it indicates that individual channel is functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which this channel resides is operating properly.

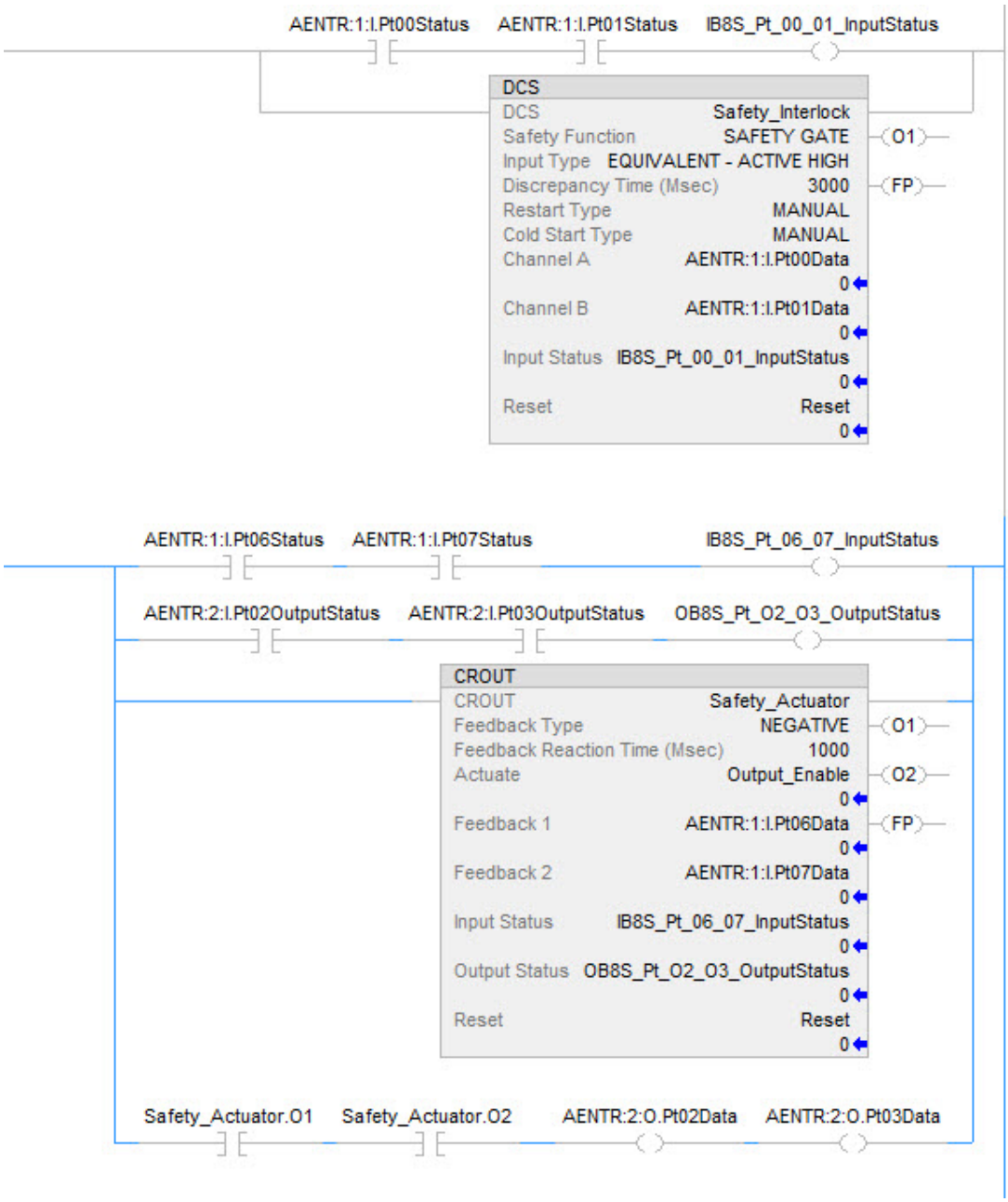
Combined Status is also available for both safety inputs (.CombinedInputStatus) and safety outputs (.CombinedOutputStatus). When the combined status tag is HI (1), it indicates that all input or output channels on the module are functioning and wired correctly, and that the safety connection between the safety controller and the safety I/O module on which these channels reside is operating properly.

Whether combined status or point status is used is application-dependent. Point status simply provides more granular status.

The dual-channel safety instructions have built in safety I/O status monitoring. Input status and Output status are parameters for the safety input and output instructions. The DCS instruction (and other dual-channel safety instructions) has input status for input channels A and B. The CROUT instruction has input status for Feedbacks 1 and 2, and has output status for the output channels that are driven by the CROUT outputs O1 and O2. The status tags used in these instructions must be HI (1) for the safety instruction output tags (O1 for input instructions and O1/O2 for CROUT) to be energized.

For proper safety instruction operation, it is important to drive the input status and output status tags BEFORE/ABOVE the safety instruction as shown in Figure 32.

Figure 32 - Instruction Examples



When you use instructions, such as XIC and OTE, you are responsible for interrogating the safety I/O status:

- Before you use a safety input channel as an interlock, verify that the safety input channel status is HI (1).
- Before you energize a safety output channel, verify that the safety output channel status is HI (1).

Notes:

Safety Instructions

ATTENTION: These safety instructions are the only instructions that can be used in the safety tasks in SIL 2 or SIL 3 applications.

For the latest information on certified instructions, see our safety certificates and revision release list at http://www.rockwellautomation.com/global/certification/safety.page.

Safety Instructions

The following tables list the safety application instructions that are certified for use in SIL 2 or SIL 3 applications.

If you use Logix Designer version 17 or later, use the newer, preferred instructions in Table 12. For a list of preferred instructions in place of the corresponding legacy instructions, see the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM096.

Table 12 - Safety Instructions

Mnemonic	Name	Purpose
CROUT	Configurable Redundant Output	Controls and monitors redundant outputs.
DCA	Dual Channel Input - Analog (integer version)	Monitors two analog values for deviation and range tolerance.
DCAF	Dual Channel Input - Analog (floating point version)	
DCS	Dual Channel Input - Stop	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch.
DCST	Dual Channel Input - Stop With Test	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device.
DCSTL	Dual Channel Input - Stop With Test and Lock	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device. It can monitor a feedback signal from a safety device and issue a lock request to a safety device.
DCSTM	Dual Channel Input - Stop With Test and Mute	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability to initiate a functional test of the stop device and the ability to mute the safety device.
DCM	Dual Channel Input - Monitor	Monitors dual-input safety devices.
DCSRT	Dual Channel Input - Start	Energizes dual-input safety devices whose main function is to start a machine safely, for example an enable pendant.
SMAT	Safety Mat	Indicates whether the safety mat is occupied.
THRSe	Two-Hand Run Station – Enhanced	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control one output. Features configurable channel-to-channel discrepancy time and enhanced capability for bypassing a two-hand run station.
TSAM	Two Sensor Asymmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged asymmetrically.
TSSM	Two Sensor Symmetrical Muting	Automatically disables the protective function of a light curtain temporarily, by using two muting sensors that are arranged symmetrically.
FSBM	Four Sensor Bi-directional Muting	Automatically disables the protective function of a light curtain temporarily, by using four sensors that are arranged sequentially before and after the sensing field of the light curtain.

Table 13 - Metal Form Instructions

Mnemonic	Name	Purpose
CBCM	Clutch Brake Continuous Mode	Used for press applications where continuous operation is desired.
CBIM	Clutch Brake Inch Mode	Used for press applications where minor slide adjustments are required, such as press setup.
CBSSM	Clutch Brake Single Stoke Mode	Used in single-cycle press applications.
CPM	Crankshaft Position Monitor	Used to determine the slide position of the press.
CSM	Camshaft Monitor	Monitors motion for the start, stop, and run operations of a camshaft.
EPMS	Eight-position Mode Selector	Monitors eight safety inputs to control one of the eight outputs that correspond to the active input.
AVC	Auxiliary Valve Control	Controls an auxiliary valve that is used with a main valve.
MVC	Main Valve Control	Controls and monitors a main valve.
MMVC	Maintenance Manual Valve Control	Used to drive a valve manually during maintenance operations.

For more information about the safety application instructions in Table 14, see Appendix F.

Table 14 - RSLogix 5000 Software, Version 14 and Later, Safety Application Instructions

Mnemonic	Name	Purpose
ENPEN	Enable Pendant	Monitors two safety inputs to control one output and has a 3-s inputs-inconsistent timeout value.
ESTOP	E-stop	Monitors two safety inputs to control one output and has a 500-ms inputs-inconsistent timeout value.
RIN	Redundant Input	Monitors two safety inputs to control one output and has a 500-ms inputs-inconsistent timeout value.
ROUT	Redundant Output	Monitors the state of one input to control and monitor two outputs.
DIN	Diverse Input	Monitors two diverse safety inputs to control one output and has a 500-ms inputs-inconsistent timeout value.
FPMS	5-position Mode Selector	Monitors five safety inputs to control one of the five outputs that corresponds to the active input.
THRS	Two-handed Run Station	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control one output.
LC	Light Curtain	Monitors two safety inputs from a light curtain to control one output.

Routines in the safety task can use the ladder diagram safety instructions in Table 15.

Table 15 - Ladder Diagram Safety Instructions

Type	Mnemonic	Name	Purpose
Array (File)	COP (1)	Copy	Copy binary data from one tag to another (no type conversion).
	FAL(2)	File Arithmetic and Logic	Perform copy, arithmetic, logic, and function operations on data that is stored in an array.
	FLL	File Fill	Fill the elements of an array with the Source Value, while leaving the source value unchanged.
	FSC	File Search and Compare	Compare the values in an array, element by element.
	SIZE	Size In Elements	Find the size of a dimension of an array.
Bit	XIC	Examine If Closed	Examines the data bit to set or clear the rung condition.
	XIO	Examine If Open	Examines the data bit to set or clear the rung condition.
	OTE	Output Energize	Controls a bit (it performs both Set and Clear operations based on rung state).
	OTL	Output Latch	Set a bit (retentive).
	OTU	Output Unlatch	Clear bit (retentive).
	ONS	One Shot	Allows an event to occur one time.
	OSR	One Shot Rising	Sets an output bit for one scan on the false-to-true (rising) edge of rung state.
	OSF	One Shot Falling	Sets an output bit for one scan on the true-to-false (falling) edge of rung state.
Timer	TON	On-delay timer	Time how long a timer is enabled.
	TOF	Off-delay timer	Time how long a timer is disabled.
	RTO	Retentive Timer On	Accumulate time.
	CTU	Count Up	Count up.
	CTD	Count Down	Count down.
	RES	Reset	Reset a timer or counter.

Table 15 - Ladder Diagram Safety Instructions (Continued)

Type	Mnemonic	Name	Purpose
Compare	CMP(2)	Compare	Perform a comparison on the arithmetic operations that you specify in the expression.
	EQU	Equal To	Test whether two values are equal.
	GEQ	Greater Than Or Equal To	Test whether one value is greater than or equal to a second value.
	GRT	Greater Than	Test whether one value is greater than a second value.
	LEQ	Less Than Or Equal To	Test whether one value is less than or equal to a second value.
	LES	Less Than	Test whether one value is less than a second value.
	MEQ	Masked Comparison for Equal	Pass source and compare values through a mask and test whether they are equal.
	NEQ	Not Equal To	Test whether one value is not equal to a second value.
	LIM	Limit Test	Test whether a value falls within a specified range.
Move	CLR	Clear	Clear a value.
	MOV	Move	Copy a value.
	MVM	Masked Move	Copy a specific part of an integer.
	SWPB	Swap Byte	Rearrange the bytes of a value.
Logical	AND	Bitwise AND	Perform bitwise AND operation.
	NOT	Bitwise NOT	Perform bitwise NOT operation.
	OR	Bitwise OR	Perform bitwise OR operation.
	XOR	Bitwise Exclusive OR	Perform bitwise exclusive OR operation.
Program Control	JMP	Jump To Label	Scan of logic jumps to a labeled location within the same routine.
	LBL	Label	Identifies a target location for a JMP instruction.
	JSR	Jump to Subroutine	Jump to a separate routine.
	RET	Return	Return the results of a subroutine.
	SBR	Subroutine	Accept data that is passed to a subroutine by the JSR instruction.
	TND	Temporary End	Mark a temporary end that halts routine execution.
	MCR	Master Control Reset	Forces every rung in a section of logic to execute in the False state.
	AFI	Always False Instruction	Forces a rung to false (rung continues to execute).
	NOP	No Operation	Insert a placeholder in the logic.
	EVENT(3)	Trigger Event Task	Trigger one execution of an event task.
Math/ Compute	ADD	Add	Add two values.
	CPT (2)	Compute	Perform the arithmetic operation that is defined in the expression.
	SUB	Subtract	Subtract two values.
	MUL	Multiply	Multiply two values.
	DIV	Divide	Divide two values.
	MOD	Modulo	Determine the remainder after one value is divided by a second value.
	SQR	Square Root	Calculate the square root of a value.
	NEG	Negate	Take the opposite sign of a value.
	ABS	Absolute Value	Take the absolute value of a value.
Trigonometric	ATAN2	Arc Tangent 2	Compute the arc tangent in radians of **y/x** based on the signs of both values to determine the correct quadrant. **IMPORTANT:** The accuracy of the results has been confirmed to 6 decimal places.
I/O	GSV(4)	Get System Value	Get controller status information.
	SSV(4)	Set System Value	Set controller status information.

(1) When using the COP instruction in a safety routine, you must verify that the length is a constant and that the source and destination length are the same.
(2) Advanced instructions, such as SIN, COS, and TAN, are not supported in safety routines.
(3) The event instruction triggers a scan of the standard task.
(4) For special considerations when using the GSV and SSV instructions, see the ControlLogix® 5580 and GuardLogix® 5580 Controllers User Manual, publication 1756-UM543, or the CompactLogix™ 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001.

Table 16 - Drive Safety Instructions (1)

Mnemonic	Name	Purpose
SS1	Safe Stop 1	The Safe Stop 1 instruction monitors the deceleration of an axis according to the specified velocity ramp to zero speed and controls its output (O1) to initiate Safe Torque Off (STO).
SS2	Safe Stop 2	The Safe Stop 2 instruction initiates and monitors the motor deceleration within set limits to verify that the motor is brought to an operational stop. Once stopped, SS2 continues to monitor the operational stop of the motor.
SOS	Safe Operating Stop	The Safe Operating Stop instruction monitors the speed or position of a motor or axis to verify that the deviation from standstill speed or position is not more than a defined amount.
SLS	Safely-limited Speed	The Safely-limited Speed instruction monitors the speed of an axis and sets the SLS Limit output if the speed exceeds the Active Limit input value for the instruction.
SLP	Safe Limited Position	The Safely-limited Position instruction monitors the position of a motor or axis to verify that the position does not deviate above or below defined limits.
SDI	Safe Direction	The Safe Direction instruction monitors position of a motor or axis to detect movement of more than a defined amount in the unintended direction.
SBC	Safe Brake Control	The Safe Brake Control (SBC) instruction: • Controls safety outputs that actuate a brake. • Sets timing between brake and Torque Off Request outputs. • Monitors brake feedback and I/O status.
SFX	Safe Feedback Scaling	The Safety Feedback Interface instruction converts motor velocity and position feedback from a drive module into user scaling units. It also defines an absolute reference position.

(1) Motion safety instructions are available when using a GuardLogix® 5580 controller, Compact GuardLogix 5380, and safe speed or position inputs with the Studio 5000 Logix Designer® application (version 31 or later).

IMPORTANT If you use Motion Direct Commands with a Kinetix® 5500 drive, Kinetix 5700 servo drive, or a PowerFlex® 527 drive, see the user manual for the drive for information on how to use this feature in safety applications.

- Kinetix 5500 Servo Drives User Manual, publication 2198-UM001
- Kinetix 5700 Servo Drives User Manual, publication 2198-UM002
- PowerFlex® 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002
- PowerFlex 755/755T Integrated Safety - Safe Torque Off Option Module User Manual, publication 750-UM004
- PowerFlex 755/755T Integrated Safety Functions Option Module User Manual, publication 750-UM005

Table 17 - Additional Resources

Resource	Description
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides more information on the safety application instructions.
Logix 5000 Controllers Generals Instructions Reference Manual, publication 1756-RM003	Provides information on the Logix 5000 instruction set that includes general, motion, and process instructions.

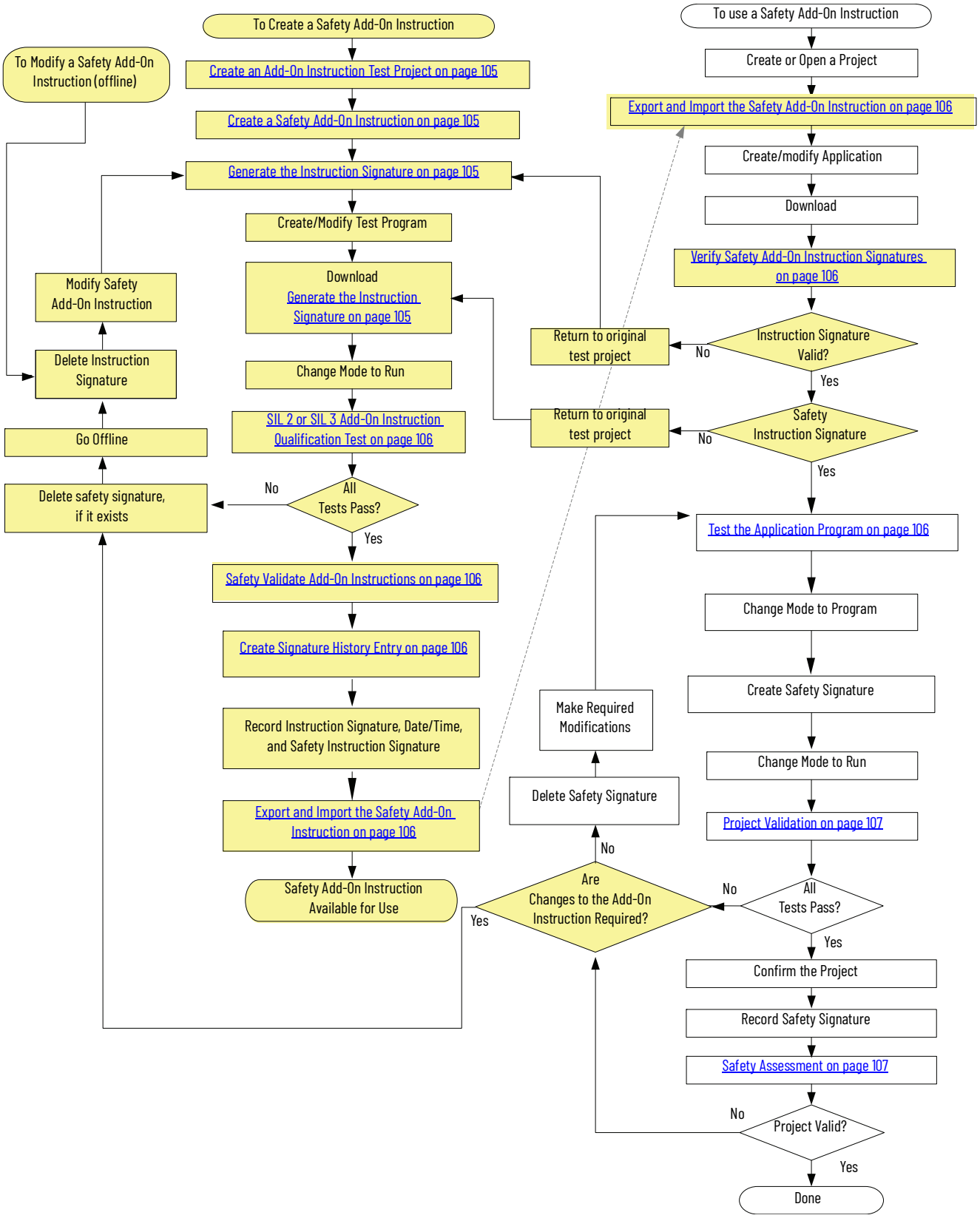
Create and Use a Safety Add-On Instruction

With the Studio 5000 Logix Designer® application, you can create safety Add-On Instructions. Safety Add-On Instructions let you encapsulate commonly used safety logic into one instruction, which makes it modular and easier to reuse.

Safety Add-On Instructions use the instruction signature of high-integrity Add-On Instructions and also a safety instruction signature for use in safety-related functions up to and including SIL 3.

Figure 33 on page 104 shows the steps that are required to create a safety Add-On Instruction and then use that instruction in a safety application program. The shaded items are steps unique to Add-On Instructions. See the links for an explanation of those topics.

Figure 33 - Flowchart for Creating and Using Safety Add-On Instructions



Create an Add-On Instruction Test Project

You must create a unique test project to create and test the safety Add-On Instruction. This project must be a separate and dedicated project to minimize any unexpected influences. Follow the guidelines for projects that are described in Create the Project on page 58.

Create a Safety Add-On Instruction

For guidance in how to create Add-On Instructions, see the Logix 5000 Controllers Add-On Instruction Programming Manual, publication 1756-PM010.

Generate the Instruction Signature

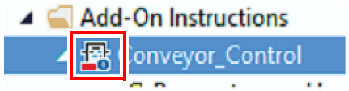
The instruction signature lets you quickly determine if the instruction has been modified. Each Add-On Instruction can have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and can sometimes be required for regulated industries. Use it when your application calls for a higher level of integrity.

The instruction signature consists of an ID number and time stamp that identifies the contents of the Add-On Instruction at a given point in time.

Once generated, the instruction signature seals the Add-On Instruction, which helps prevent it from being edited while the signature is in place. This restriction includes rung comments, tag descriptions, and any instruction documentation that was created. When the instruction is sealed, you can perform only these actions:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

When an instruction signature has been generated, the Studio 5000 Logix Designer application displays the instruction definition with the seal icon.



IMPORTANT If you protect your Add-On Instruction with the source protection feature in the Studio 5000 Logix Designer application, enable source protection before you generate the instruction signature.

The Safety Instruction Signature

When a sealed safety Add-On Instruction is downloaded for the first time, a safety instruction signature is automatically generated. The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction.

IMPORTANT Checking or clearing the Report Overflow Faults checkbox in the controller properties changes the safety instruction signature ID for safety Add-On Instructions that include math instructions.

SIL 2 or SIL 3 Add-On Instruction Qualification Test

Safety Add-On Instruction tests must be performed in a separate, dedicated application to verify that unintended influences are minimized. You must follow a well-designed test plan and perform a unit test of the safety Add-On Instruction that exercises all possible execution paths through the logic, including the valid and invalid ranges of all input parameters.

Safety Validate Add-On Instructions

An independent, third-party review of the safety Add-On Instruction can be required before the instruction is approved for use. An independent, third-party validation may be required for functional safety certification.

Create Signature History Entry

The signature history provides a record for future reference. A signature history entry consists of the instruction signature, the name of the user, the time stamp value, and a user-defined description. Up to six history entries can be stored. You must be offline to create a signature history entry.

The Signature Listing report in the Studio 5000 Logix Designer application prints the instruction signature, the time stamp, and the safety instruction signature. To print the report, right-click Add-On Instruction in the Controller Organizer and choose Print>Signature Listing.

Export and Import the Safety Add-On Instruction

When you export a safety Add-On Instruction, choose the option to include all referenced Add-On Instructions and user-defined data types in the same export file. By including referenced Add-On Instructions, you make it easier to preserve the signatures.

When importing Add-On Instructions, consider these guidelines:

- You cannot import a safety Add-On Instruction into a standard controller project.
- You cannot import a safety Add-On Instruction into a safety controller project that has been safety-locked or one that has a safety signature.
- You cannot import a safety Add-On Instruction while online.
- If you import an Add-On Instruction with an instruction signature into a project where referenced Add-On Instructions or user-defined data types are not available, you may need to remove the signature.

For more information, see the Import/Export Project Components Programming Manual, publication 1756-PM019.

Verify Safety Add-On Instruction Signatures

After you download the application project that contains the imported safety Add-On Instruction, you must compare the instruction signature value, the date and time stamp, and the safety instruction signature values with the original values you recorded before you exported the safety Add-On Instruction. If they match, the safety Add-On Instruction is valid and you can continue with the validation of your application.

Test the Application Program

This step consists of any combination of Run and Program mode, online or offline program edits, upload and download, and informal testing that is required to get an application to run properly.

Project Validation

Perform an engineering test of the application, including the safety system. For more information about requirements, see Validate the Project on page 60.

Safety Assessment

An independent, third-party review of the safety system can be required before the system is approved for operation. An independent, third-party validation may be required for functional safety certification. For more information about safety assessments, see the Machinery SafeBook 5.

Notes:

Reaction Times

The input reaction time is the time from when the signal changes on an input terminal to when safety data is sent to the GuardLogix controller.

The output reaction time is the time from when safety data is received from the GuardLogix controller to when the output terminal changes state.

For information on how to determine the input and output reaction times, see the product documentation for your specific safety I/O device.

Connection Reaction Time Limit

The Connection Reaction Time Limit (CRTL) is the maximum age of safety packets on the associated connection. If the age of the data that is used by the consuming device exceeds the CRTL, a connection fault occurs.

The CRTL is defined by these three values.

Value	Default	Description
Requested Packet Interval (RPI)	10 ms (Input RPI)	How often the input and output packets are placed on the wire (network).
Timeout Multiplier	2	The Timeout Multiplier is the number of retries before timing out.
Network Delay Multiplier	200	The Network Delay Multiplier accounts for any known delays on the wire. When these delays occur, timeouts can be avoided using this parameter.

If you adjust these values, then you can adjust the connection reaction time limit. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state (OFF).

IMPORTANT The default values generate an Input connection reaction time limit of 40 ms. If no edits are made to the defaults, verify this connection reaction time limit is used in the safety reaction time calculations.

IMPORTANT For applications with safety I/O, especially large banks of POINT Guard I/O™ Safety modules, the default connection reaction time limit can result in connection loss to the safety I/O modules. In these cases, it may be necessary to increase the values from their defaults. Make sure the new connection reaction time limit is used in the safety reaction time calculations.

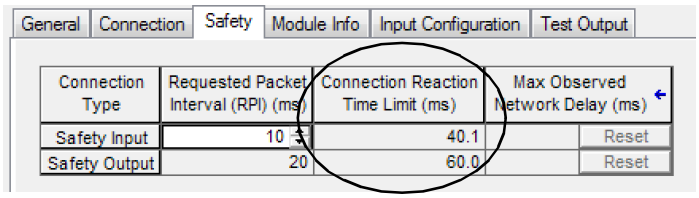
The following equations determine the CRTL:

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 CRTL is shown on the Safety tab of the Module Properties dialog box.

Figure 34 - Connection Reaction Time Limit



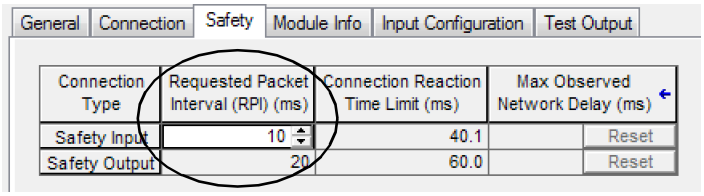
Specify the Requested Packet Interval (RPI)

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

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

The CRTL is adjusted immediately when the RPI is changed via the Logix Designer® application.

Figure 35 - Requested Packet Interval



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

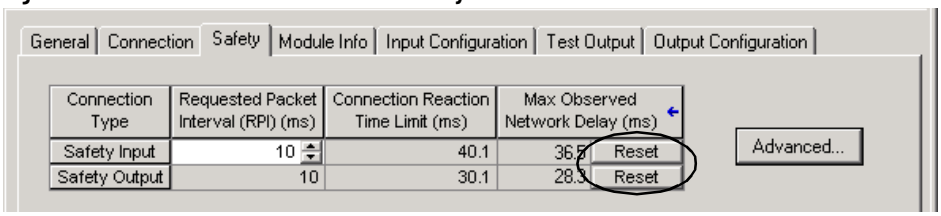
See System Reaction Time on page 15 for safety task period details.

For typical applications, the default CRTL for input connections of 4 x RPI and the default CRTL for output connections of 3 x RPI is usually sufficient. For more complex requirements, use the Advanced button to modify the Connection Reaction Time Limit parameters, as described on page 115.

View the Maximum Observed Network Delay

The Maximum Observed Network Delay is shown on the Safety tab of the Module Properties dialog box. When online, click Reset to reset the Maximum Observed Network Delay.

Figure 36 - Reset the Max Observed Network Delay

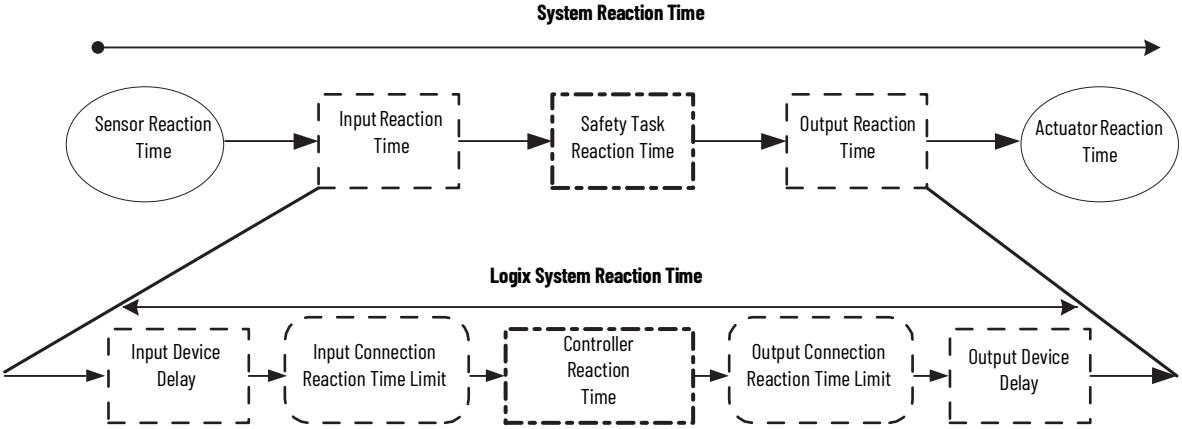


System Reaction Time

To determine the system reaction time of any control chain, you must add up the reaction times of all the components of the safety chain.

System Reaction Time = Sensor Reaction Time + Logix System Reaction Time + Actuator Reaction Time

Figure 37 - System Reaction Time



Safety Task Reaction Time

The safety task reaction time is the worst-case delay from any input change that is presented to the controller until the output producer sets the processed output. Use this equation to determine the safety task reaction time:

Safety task reaction time = (safety task period + safety task watchdog) × 1.01

The multiplier is for potential clock drift.

Safety Task Period and Safety Task Watchdog

The safety task period is the interval at which the safety task executes.

The safety task watchdog time is the maximum permissible time for safety task processing. If the time to process a safety task exceeds the safety task watchdog time, a nonrecoverable safety fault occurs in the controller, which results in a transition to the safe state (off).

You define the safety task watchdog time, which must be less than or equal to the safety task period.

The safety task watchdog time is set in the task properties window of the Studio 5000 Logix Designer application. This value can be modified online, regardless of controller mode, but it cannot be changed when the controller is safety-locked or once a safety signature is created.

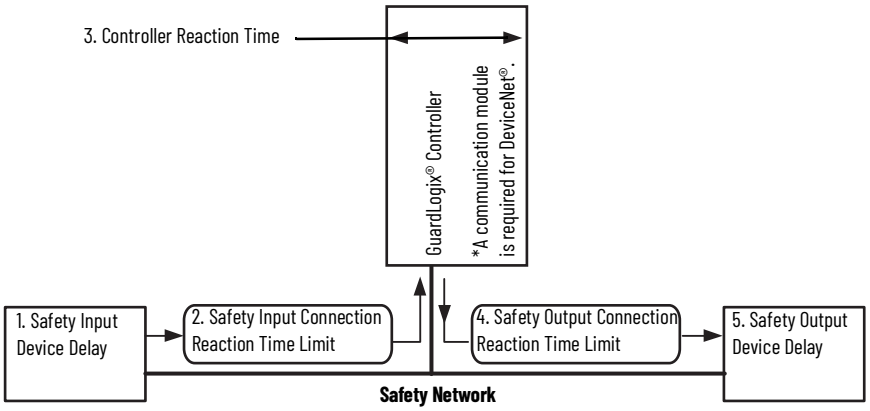
Logix System Reaction Time

The following sections provide information on how to calculate the Logix system reaction time for a simple input-logic-output chain and for a more complex application by using produced/consumed safety tags in the logic chain.

Simple Input-logic-output Chain

This section describes the Logix system reaction time for any simple input to logic to output chain.

Figure 38 - Logix System Worst-case Reaction Time for Simple Input to Logic to Output



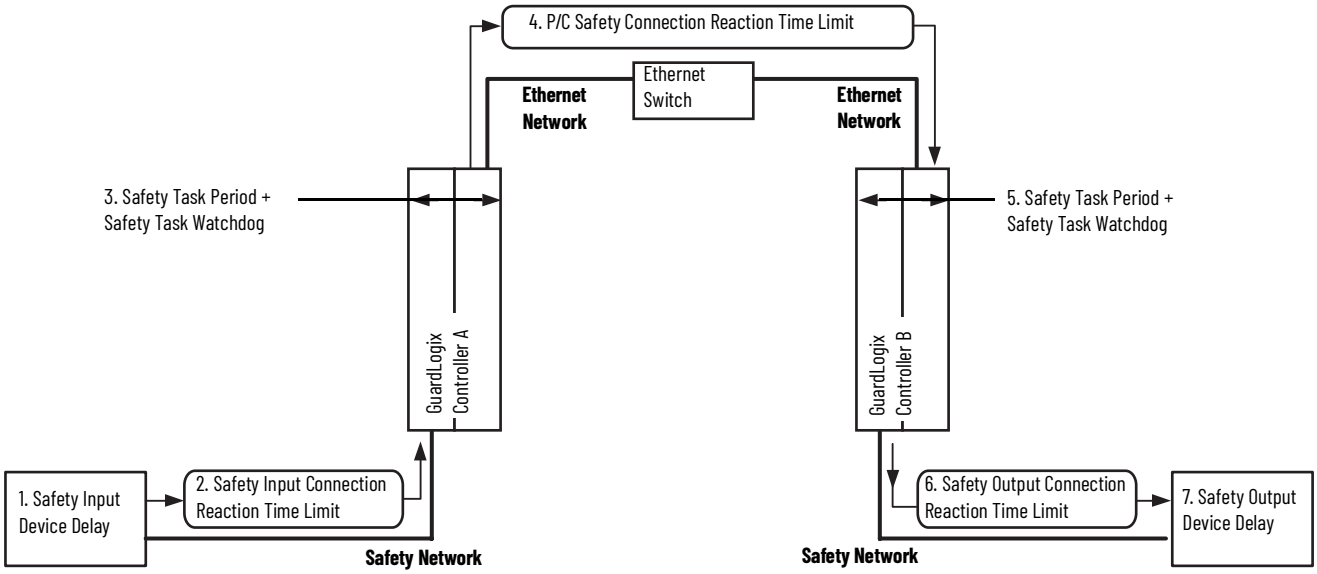
The Logix system reaction time for any simple input to logic to output chain consists of these five components:

1. Safety input device reaction time (plus input delay time, if applicable)
2. Safety Input Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety input device connection RPI.)
3. Controller reaction time (see Safety Task Reaction Time on page 111)
4. Safety Output Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Studio 5000 Logix Designer® application, this value is a multiple of the safety task period.)
5. Safety output device reaction time

Logic Chain Using Produced/Consumed Safety Tags

This section describes the Logix system reaction time for any input to controller A logic to controller B logic to output chain.

Figure 39 - Logix System Reaction Time for Input to Controller A Logic to Controller B Logic to Output Chain



The Logix system reaction time for any input to controller A logic to controller B logic to output chain consists of these seven components:

1. Safety input device reaction time (plus input delay time, if applicable)
2. Safety Input Connection Reaction Time Limit
3. Safety Task Period plus Safety Task Watchdog time for Controller A
4. Produced/Consumed Safety Connection Reaction Time Limit (Read from the Safety tab of the consumed tag connection.)
5. Safety Task Period plus Safety Task Watchdog time for Controller B
6. Safety Output Connection Reaction Time Limit
7. Safety output device reaction time

Factors That Affect Logix Reaction-time Components

A number of factors can influence the Logix Reaction Time components that are described in the previous sections.

Table 18 - Factors Affecting Logix System Reaction Time

These Reaction Time Components	Are Influenced by the Following Factors
Input device delay	Input device reaction time
	On-Off and Off-On delay settings for each input channel, if applicable
Safety Input Connection Reaction Time Limit	Input device settings for: • Requested Packet Interval (RPI) • Timeout Multiplier • Network Delay Multiplier
	The amount of network communication traffic(1)
	The EMC environment of the system(1)
Safety Task Period and Safety Task Watchdog	Safety Task Period setting
	Safety Task Watchdog setting
	The number and execution time of instructions in the safety task(2)
	Any higher priority tasks that preempt safety task execution(2)
Produced/Consumed Safety Connection Reaction Time Limit	Consumed tag settings for: • RPI • Timeout Multiplier • Network Delay Multiplier
	The amount of network communication traffic(1)
	The EMC environment of the system(1)
Output Connection Reaction Time Limit	Safety Task Period setting
	Output device settings for: • Timeout Multiplier • Network Delay Multiplier
	The amount of network communication traffic(1)
	The EMC environment of the system(1)
Output module delay	Output module reaction time

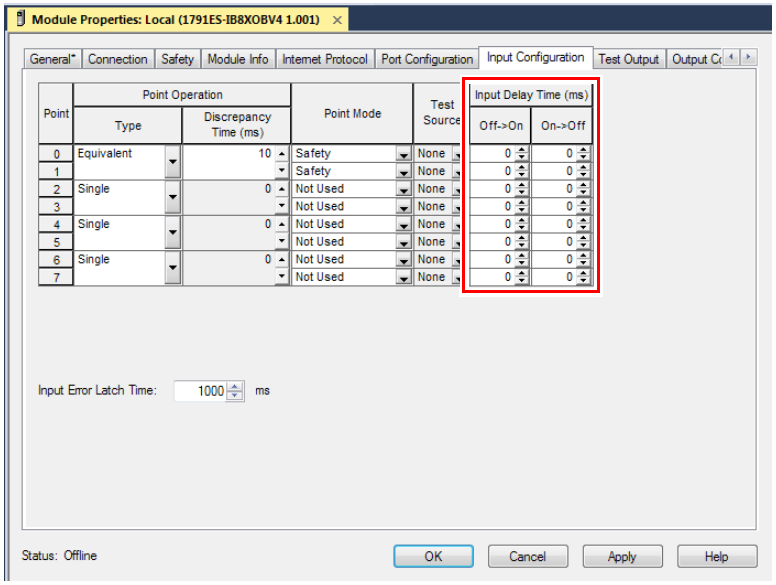
(1) Network traffic and EMC create a lower limit for the values that you can successfully use for Timeout Multiplier and Network Delay Multiplier.
(2) The instructions in your safety task and any higher priority tasks in the controller create a lower limit for the values that you can successfully use for Safety Task Period and Safety Task Watchdog.

The following sections describe how to access data or settings for many of these factors.

Configure Guard I/O Input Module Delay Time Settings

To configure input module delay time in the Studio 5000 Logix Designer application, follow these steps.

1. In the configuration tree, right-click your Guard I/O™ module and choose Properties.
2. Click the Input Configuration tab.
3. Adjust the input delay time as required for your application.



Configure or View the Input and Output Safety Connection Reaction Time Limits

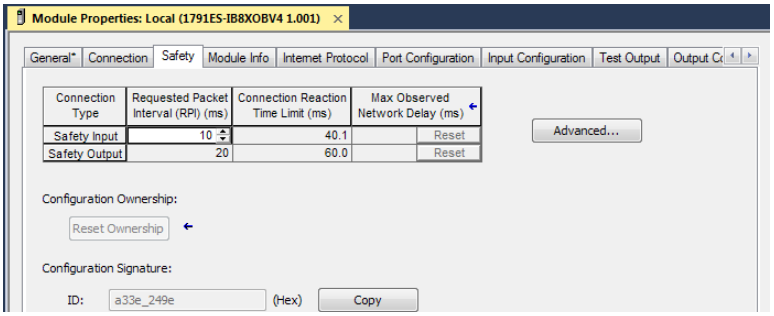
The following three values define the Connection Reaction Time Limit (CRTL).

Value	Description
Requested Packet Interval (RPI)	How often the input and output packets are placed on the wire (network).
Timeout Multiplier	The Timeout Multiplier is the number of retries before timing out.
Network Delay Multiplier	The Network Delay Multiplier accounts for any known delays on the wire. When these delays occur, timeouts can be avoided using this parameter.

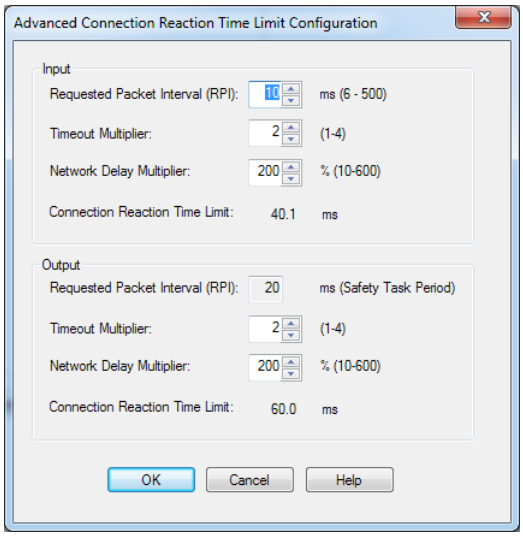
If you adjust these values, then you can adjust the Connection Reaction Time Limit. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state.

To view or configure these settings, follow these steps.

1. In the configuration tree, right-click your safety I/O device and choose Properties.
2. Click the Safety tab.



3. Click Advanced to open the Advanced Connection Reaction Time Limit dialog box.



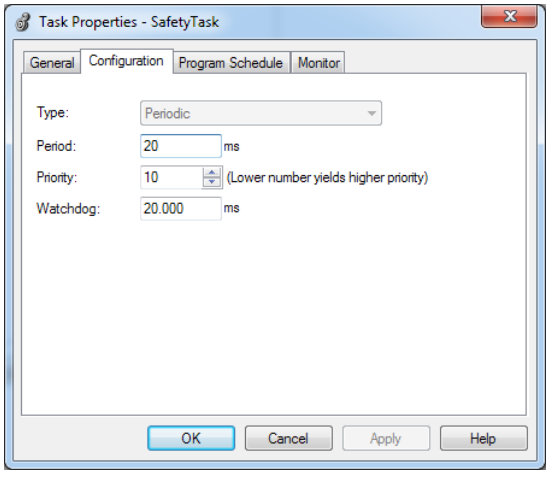
IMPORTANT The Timeout Multiplier and Network Delay Multiplier provide resilience for variations in network reliability and performance.

Use caution when reducing the values of these parameters as this increases the likelihood of false trips.

Configure the Safety Task Period and Watchdog

The safety task is a periodic timed task. You select the task period, priority, and watchdog time via the Task Properties - Safety Task dialog box in your Studio 5000 Logix Designer project.

To access the safety task period and watchdog time settings, right-click the Safety Task and choose Properties.

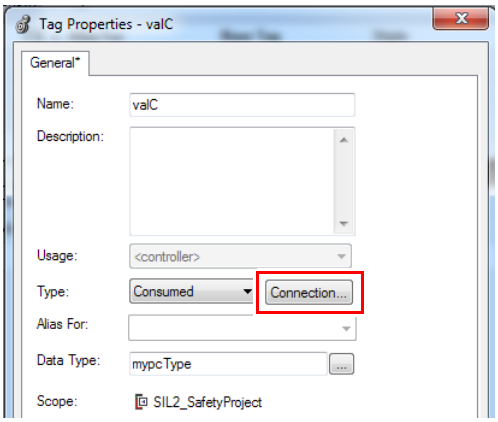


The priority of the safety task is not a safety concern, as the safety task watchdog monitors if a higher priority task interrupts the task.

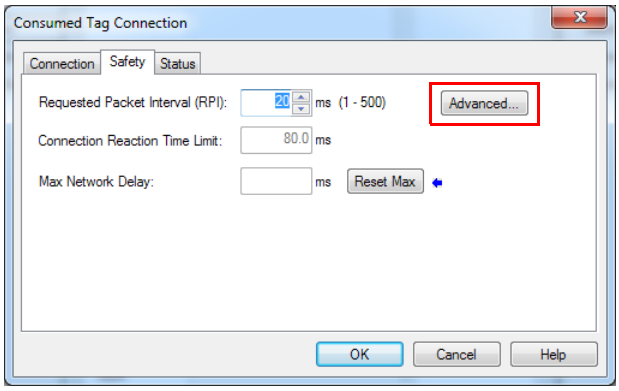
Access Produced/Consumed Tag Data

To view or configure safety-tag connection data, follow these steps.

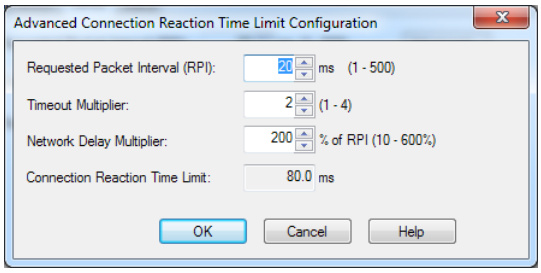
1. In the configuration tree, right-click Controller Tags and choose Edit tags.
2. In the Tag Editor, right-click the name of the tag and choose Edit Properties.
3. Click Connection.



4. On the Safety tab, click Advanced.



5. You can view or edit the current settings in the Advanced dialog box.



See the following for more information.

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 User Manual, publication 5069-UM001

Notes:

Checklists for GuardLogix Safety Applications

The checklists in this appendix are required to plan, program, and start a GuardLogix® safety application. They can be used as planning guides and during project validation testing. If used as planning guides, the checklists can be saved as a record of the plan.

The checklists on the following pages provide a sample of safety considerations and are not intended to be a complete list of items to verify. Your particular safety application can have additional safety requirements, for which we have provided space in the checklists.

Make copies of the checklists and keep these pages for future use.

Checklist for GuardLogix Controller System

Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
Number	**System Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using only the certified components for your SIL level, with the corresponding firmware release, as listed at https://www.rockwellautomation.com/global/certification/safety.page	☐	☐	
2	Have you calculated the safety response time of the system for each safety function?	☐	☐	
3	Does the response time of the system' include both the user-defined safety-task program watchdog (software watchdog) time and the safety task rate/period?	☐	☐	
4	Is the system response time in proper relation to the process safety time?	☐	☐	
5	Have probability (PFD/PFH) values been calculated for each safety function?	☐	☐	
6	Have you performed all appropriate project validation tests?	☐	☐	
7	Have you created a prescan routine to initialize safety critical data?	☐	☐	
8	Have you determined how your system can handle faults?	☐	☐	
9	Does each network in the safety system have a unique SNN?	☐	☐	
10	Is each Safety device configured with the correct SNN?	☐	☐	
11	Have you generated a safety signature?	☐	☐	
12	Have you uploaded and recorded the safety signature for future comparison?	☐	☐	
13	After a download, have you verified that the safety signature in the controller matches the recorded safety signature?	☐	☐	
14	Do you have an alternate mechanism in place to preserve the safety integrity of the system when making online edits?	☐	☐	
15	Have you considered the checklists for using SIL inputs and outputs, which are listed on page 120?	☐	☐	
		☐	☐	
		☐	☐	

Checklist for GuardLogix System				
		☐	☐	
		☐	☐	
		☐	☐	

Checklist for Safety Inputs

For programming or startup, an individual checklist can be completed for every safety input in the system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Input Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
SIL Input Channels				
Number	**Input Device Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed project validation tests on the system and devices?	☐	☐	
3	Are control, diagnostics, and alarm functions performed in sequence in application logic?	☐	☐	
4	Have you uploaded and compared the configuration of each device to the configuration sent by the configuration tool?	☐	☐	
5	Are devices wired in compliance with the target standard and required safety level?	☐	☐	
6	Have you verified that the electrical specifications of the sensor and input are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Checklist for Safety Outputs

For programming or startup, an individual requirement checklist must be completed for every safety output in the system. This method is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Output Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
SIL Output Channels				
Number	**Output Device Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed project validation tests on the devices?	☐	☐	
3	Have you uploaded and compared the configuration of each device to the configuration sent by the configuration tool?	☐	☐	
4	Have you verified that test outputs are not used as safety outputs?	☐	☐	
5	Are devices wired in compliance with the target standard and required safety level?	☐	☐	
6	Have you verified that the electrical specifications of the output and the actuator are compatible?	☐	☐	
		☐	☐	

Output Checklist for GuardLogix System				
		☐	☐	
		☐	☐	
		☐	☐	

Checklist to Develop a Safety Application Program

Use the following checklist to help maintain safety when you create or modify a safety application program.

Checklist for GuardLogix Application Program Development				
Company				
Site				
Project Definition				
Number	**Application Program Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using version 31 or later[1] [2]of the Studio 5000 Logix Designer® application, the GuardLogix system programming tool?	☐	☐	
2	Were the programming guidelines in Chapter 7 followed during the creation of the safety application program?	☐	☐	
3	Does the safety application program contain only a ladder diagram?	☐	☐	
4	Does the safety application program contain only those instructions that are listed in Appendix A as suitable for safety application programming?	☐	☐	
5	Does the safety application program clearly differentiate between safety and standard tags?	☐	☐	
6	Are only safety tags used for safety routines?	☐	☐	
7	Have you verified that safety routines do not attempt to read from or write to standard tags?	☐	☐	
8	Have you verified that no safety tags are aliased to standard tags and vice versa?	☐	☐	
9	Is each safety output tag correctly configured and connected to a physical output channel?	☐	☐	
10	Have you verified that all mapped tags have been conditioned in safety application logic?	☐	☐	
11	Have you defined the process parameters that the fault routines monitor?	☐	☐	
12	Have you sealed any safety Add-On Instructions with an instruction signature and recorded the safety instruction signature? Optional for one time use Add-On Instructions. Required Add-On Instructions are reused on different applications.	☐	☐	
13	Has an independent safety reviewer reviewed the program (if necessary)?	☐	☐	
14	Has the review been documented and signed?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) The Studio 5000 Logix Designer® application, version 31 or later, supports GuardLogix 5580 and Compact GuardLogix 5380 controllers.
(2) To obtain the latest software and firmware, see the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at https://www.rockwellautomation.com/global/support/pcdc.page.

Notes:

GuardLogix Systems Safety Data

The following examples show probability of a dangerous failure on demand (PFD) and average frequency of a dangerous failure per hour (PFH) values for GuardLogix® 1001 SIL 2 system or 1002 SIL 3 system.

Useful Life

The useful life of GuardLogix controllers is 20 years.

Safety Data

For safety I/O devices safety data, including PFD and PFH values, see the manuals for those products, as listed in the Additional Resources on page 8.

Data for Rockwell Automation machine safety products is now available in the form of a library file to be used with the Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA).

The library file is available for download at https://www.rockwellautomation.com/en-us/capabilities/industrial-safety-solutions/safety-system-development-tools.html.

Product Failure Rates

The data in the following tables applies to mission times up to and including 20 years.

Table 19 - Safety Parameters

Attribute	GuardLogix 5580 Controllers and Safety Partner (1) (2)	GuardLogix 5580 Controller (1) (2)	Compact GuardLogix 5380 SIL 2 Controller	Compact GuardLogix 5380 SIL 3 Controller
Safety Function Architecture (HFT) (3)	1	0	0	1
No Part/ No Effect Detected Failure Rate (λ_{NPED}) [hr]	2.80E-06	2.58E-06	4.04E-06	3.17E-06
Safe Failure Rate (λ_S) [failures/hr]	7.24E-07	6.61E-07	7.33E-07	6.26E-07
Dangerous Failure Rate (λ_D) [failures/hr]	7.10E-07	6.61E-07	7.33E-07	6.13E-07
Dangerous Detected Failure Rate (λ_{DD}) [failures/hr]	7.10E-07	6.54E-07	7.26E-07	6.13E-07
Dangerous Undetected Failure Rate (λ_{DU}) [failures/hr]	7.38E-11	6.40E-09	7.23E-09	6.45E-11
Automatic Diagnostic Test Interval (T_D) [hr]	–	<SRT	<SRT	–
Useful Life [yr]	20	20	20	20
Systematic Capability (SC)	3	3	3	3

(1) These values are product failure rates to be used when the product is represented as a block in a reliability block diagram (RBD).
(2) These product failure rates are valid for ambient temperatures up to 60 °C (140 °F) and altitudes of up to 2000 m (6561.7 ft). See publication 1756-TD001 and 1756-IN048.
(3) The HFT specified here is the product internal HFT.

Table 20 - Safety Calculations

Attribute	GuardLogix 5580 Controllers and Safety Partner	GuardLogix 5580 Controller	Compact GuardLogix 5380 SIL 2 Controller	Compact GuardLogix 5380 SIL 3 Controller
PFD_{ave} (Mission Time 20 yr)	6.46E-06	5.61E-04	6.33E-04	6.26E-06
PFH	7.38E-11	6.40E-09	7.23E-09	6.45E-11
STR	4.23E-06	3.90E-06	5.50E-06	4.41E-06
$MTTF_d$ [yr]	160.82	172.74	155.66	186.08

Assumptions for safety calculations:

- Component failure rates are constant over the life of the product.
- All detected failures (safe and dangerous) result in the safe state (MRT=0).
- Within the specified useful life (20 years), no proof test is needed.

$$PFD_{ave} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

$$STR = \lambda_S + \lambda_{DD} + \lambda_{NPED}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTF_d = \frac{1}{\lambda_d}$$

$$PFH = \lambda_{DU}$$

RSLogix 5000 Software, Version 14 and Later, Safety Application Instructions

IMPORTANT This appendix is relevant when using any of the original safety application instructions released in RSLogix 5000® software, version 14, in Table 14. The safety application instructions in Table 12 and Table 13 are preferred for new applications.

Diverse Input Fault Handling

All safety input values that are associated with a particular connection are set to safe state when a CIP Safety™ connection fault condition is detected. When using diverse input pairs, one of the inputs uses a value of one to initiate the safety function. This requires safety logic that evaluates fault conditions, so that the safety function is executed when an input fault occurs (even though the input value remains at zero).

I/O Status Fault Latching

The following diagrams provide examples of the application logic that is required to latch and reset I/O failures. The examples show the logic necessary for input only modules, and for input and output combination modules. The examples use the Combined Status feature of the I/O modules, which presents the status of all input channels in one Boolean variable. Another Boolean variable represents the status of all output channels. This approach reduces the amount of I/O conditioning logic that is required and forces the logic to shut down all input or output channels on the affected module.

Use Figure 40 on page 126 to determine which rungs of logic are required for different application situations. Input Fault Latch and Reset Flowchart on page 126 shows logic that overwrites the actual input-tag variables while a fault condition exists. If the actual input state is required for troubleshooting while the input failure is latched, use the logic shown in Ladder Diagram Example 1 on page 127. This logic uses internal tags that represent the inputs to be used in the application logic. While the input failure is latched, the internal tags are set to their safe state. While the input failure is not latched, the actual input values are copied to the internal tags.

Use the Ladder Diagram Example 2 on page 128 to determine which rungs of application logic in Output Fault Latch and Reset Flowchart on page 129 are required.

Figure 40 - Input Fault Latch and Reset Flowchart

Figure 41 - Ladder Diagram Example 1

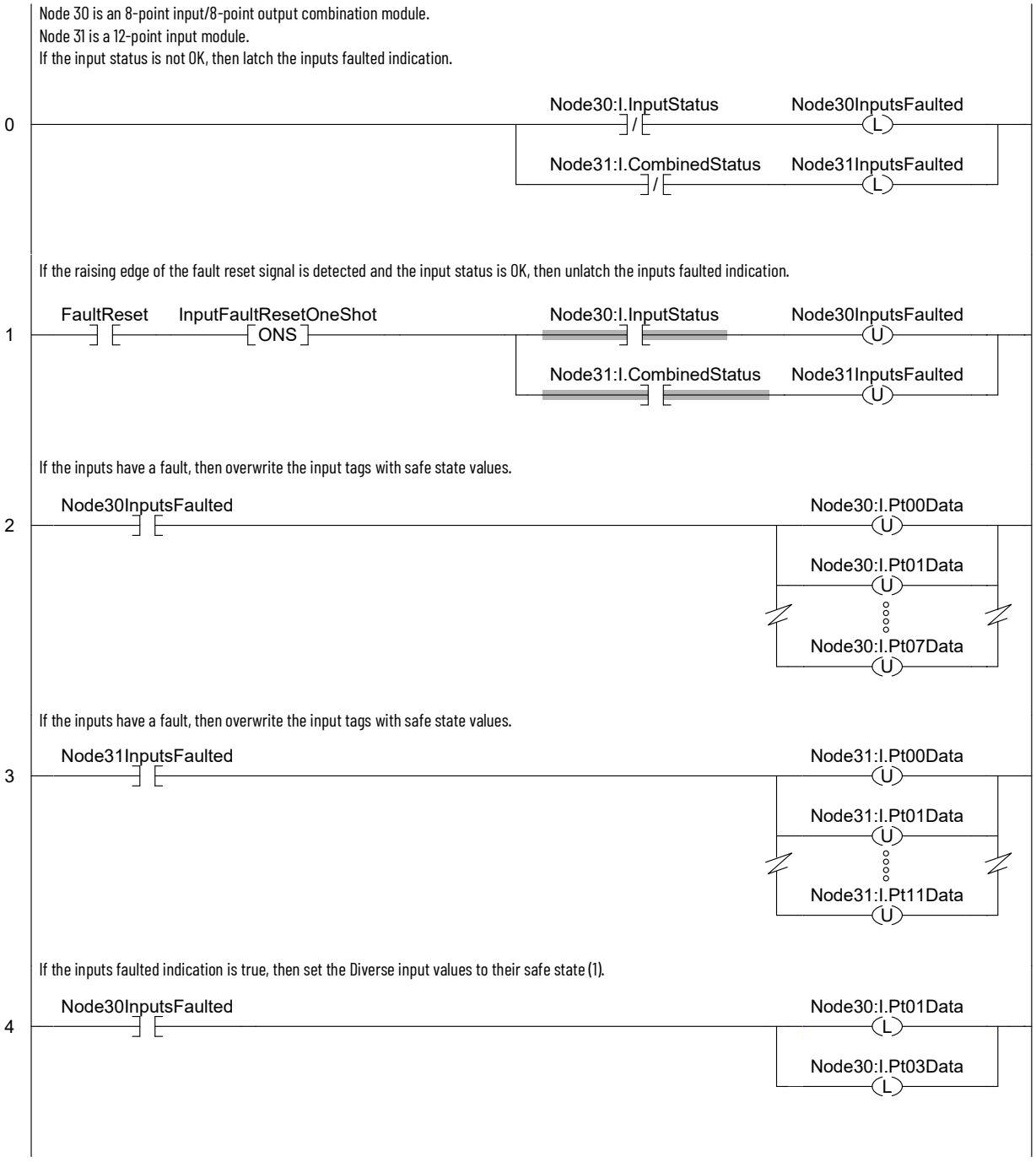


Figure 42 - Ladder Diagram Example 2

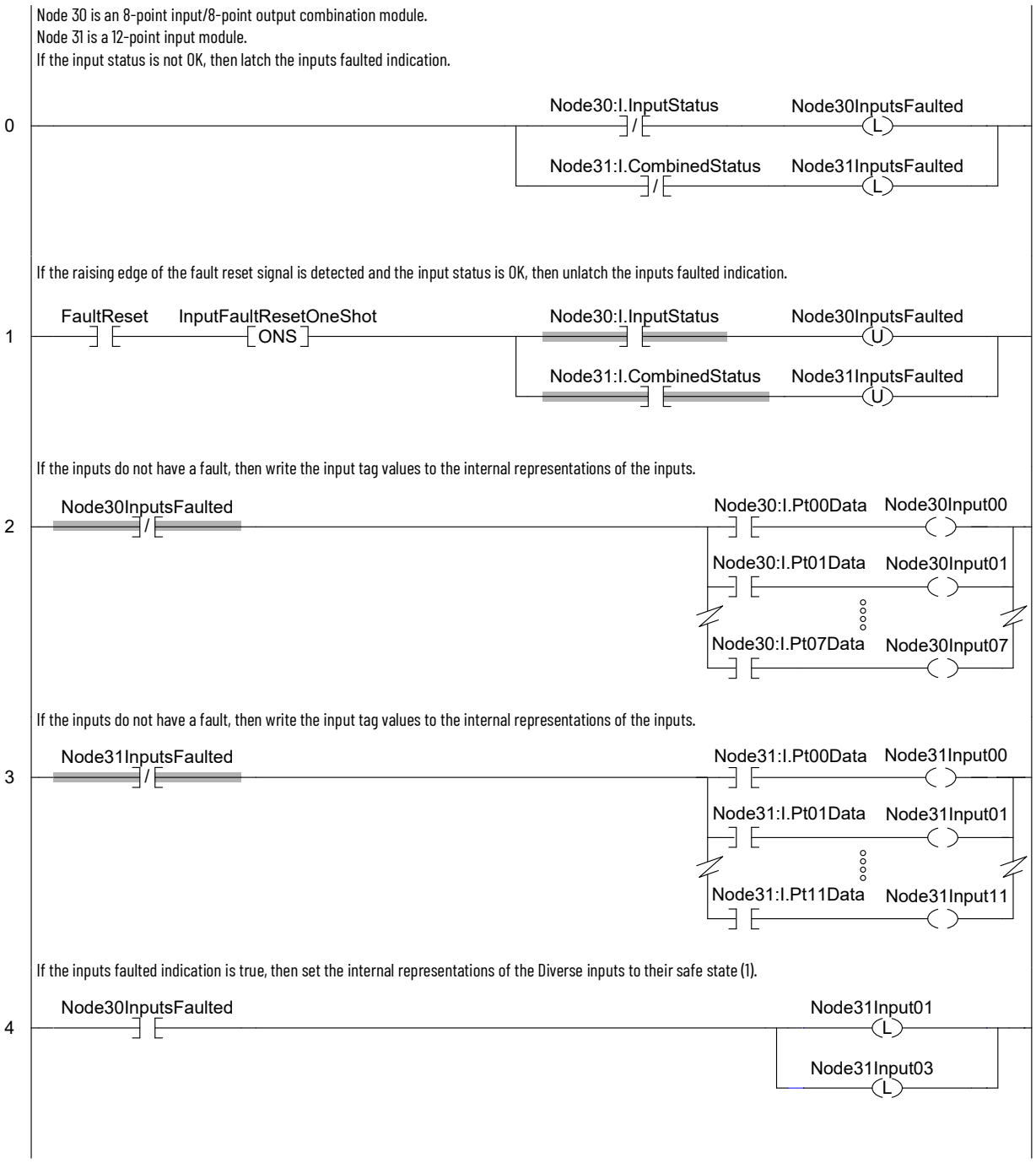


Figure 43 - Output Fault Latch and Reset Flowchart

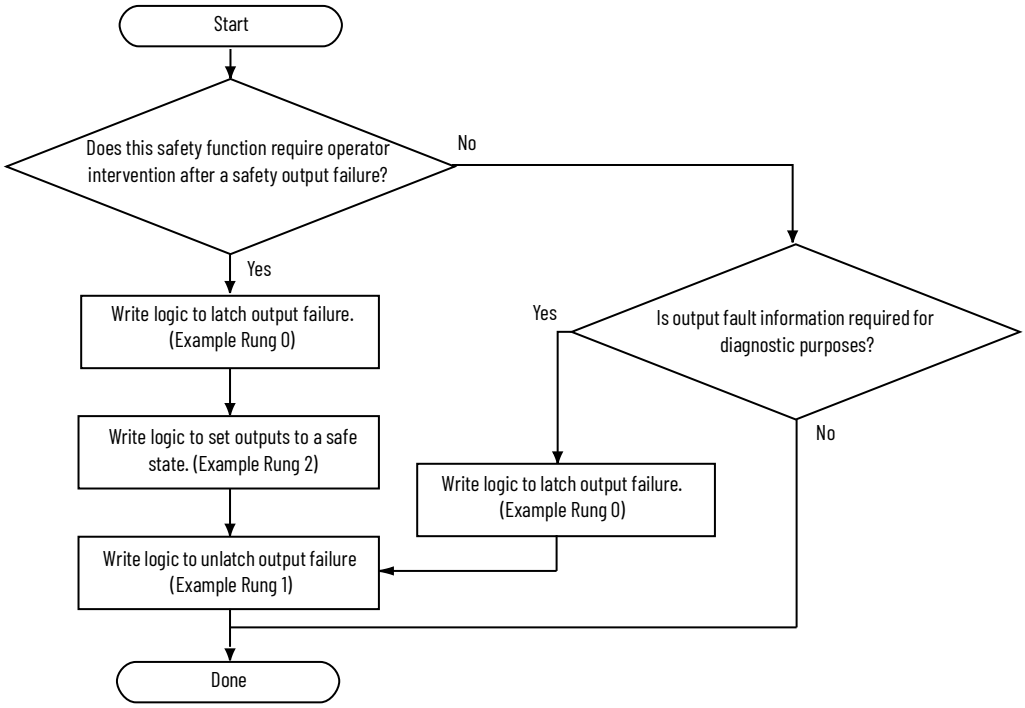
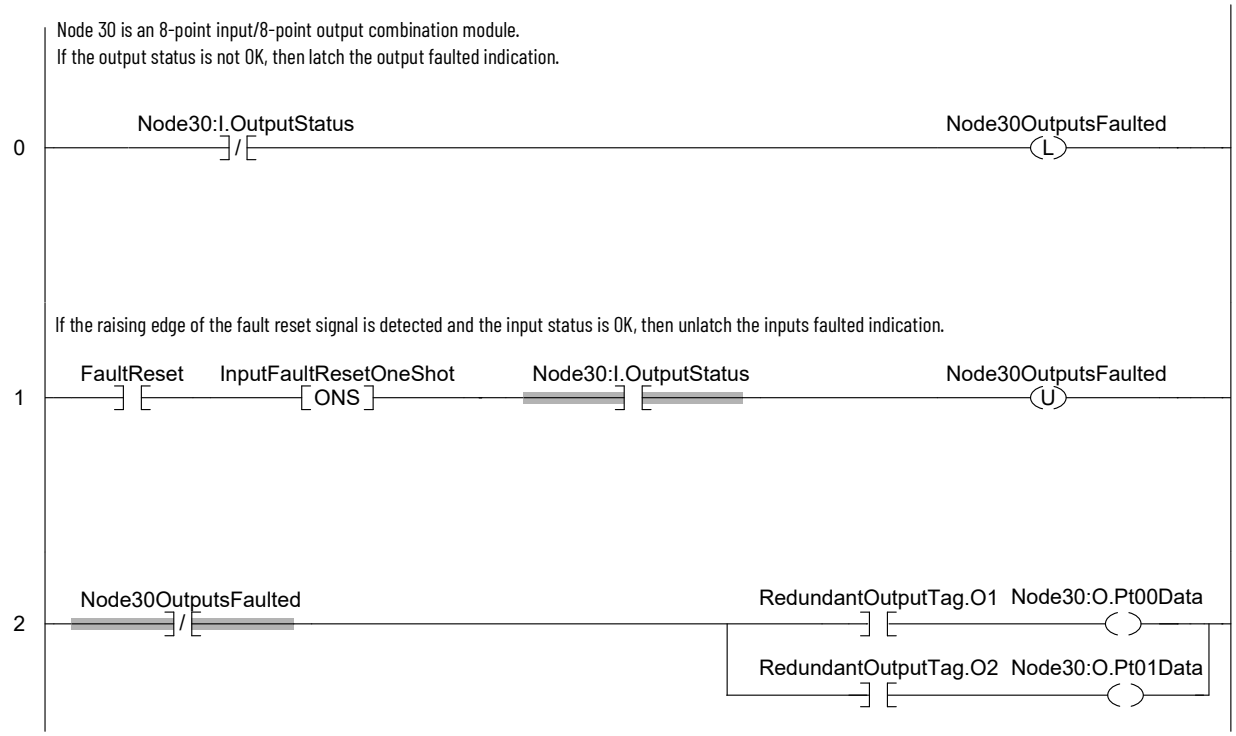


Figure 44 - Ladder Diagram Example 3



Notes:

The following terms and abbreviations are used throughout this manual. For definitions of terms that are not listed here, see the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

1oo1 (one-out-of-one) Identifies the programmable electronic controller architecture. 1001 is a single-channel system.

1oo2 (one-out-of-two) Identifies the programmable electronic controller architecture. 1002 is a dual-channel system.

accept edits Action that is taken to accept and download online edit changes. See also pending edits.

Add-On Instruction An instruction that you create as an add-on to the Logix instruction set. Once defined, an Add-On Instruction can be used like any other Logix instruction and can be used across various projects. An Add-On Instruction is composed of parameters, local tags, logic routine, and optional scan-mode routines.

assemble edits You assemble edits when you have made online edit changes to the controller program and want the changes to become permanent, because you no longer need the ability to test, untest, or cancel the edits.

Average frequency of a dangerous failure (PFH) The probability of a system to have a dangerous failure occur per hour.

cancel edits Action that is taken to reject and delete any unassembled online edit changes.

CIP™ (Common Industrial Protocol) An industrial communication protocol that is used by Logix 5000-based automation systems on EtherNet/IP™, ControlNet®, and DeviceNet® communication networks.

CIP Safety™ (Common Industrial Protocol – safety certified) SIL 2-rated or SIL 3-rated version of CIP.

configuration signature A number that uniquely identifies the configuration of a device. The configuration signature is composed of an ID number, date, and time.

detected failure A failure that diagnostic tests, proof tests, operator intervention, or through normal operation detect.

diagnostic coverage (DC) The ratio of the dangerous detected failure rate to the dangerous failure rate.

European norm. (EN) The official European standard.

get system value (GSV) A user application instruction that retrieves specified controller status information and places it in a destination tag.

hardware fault tolerance The HFT equals *n*, where *n*+1 faults could cause the loss of the safety function. An HFT of 1 means that 2 faults are required before safety is lost.

instruction signature The instruction signature consists of an ID number and date/time stamp that identifies the contents of the Add-On Instruction definition at a given point in time.

lambda (λ) Designation of a failure rate.

maximum SIL (SILCL) Maximum SIL claim limit for a SCS (safety-related control system) subsystem in relation to architectural constraints and systematic safety integrity (from IEC 62061).

MT (mission time) The length of time over which the device maintains the stated PFD, PFH, and λ ratings before replacement is required.

network delay multiplier This value represents the transport time of a message across the communication network. See also timeout multiplier.

nonrecoverable controller fault A fault that forces all processing to be ended and requires controller power to be cycled from off to on. The user program is not preserved and must be redownloaded.

nonrecoverable safety fault A fault, which even though properly handled by the fault handling mechanisms that are provided by the safety controller and implemented by the user, ends all safety task processing, and requires external user action to restart the safety task.

online Situation where you are monitoring/modifying the program in the controller.

overlap When a task (periodic or event) is triggered while the task is still executing from the previous trigger.

partnership The primary controller and safety partner must both be present in SIL 3, and the hardware and firmware must be compatible for partnership to be established.

pending edits A change to a routine that has been made in the Studio 5000 Logix Designer® application, but has not yet been communicated to the controller by accepting the edit.

Performance Level (PL) The discrete level that is used in the EN ISO 13849-1, to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

periodic task A task that the operating system triggers at a repetitive period. Whenever the time expires, the task is triggered and its programs are executed. Data and outputs that the programs in the task establish retain their values until the next execution of the task or until another task manipulates them. Periodic tasks always interrupt the continuous task.

personal computer (PC) Computer that is used to interface with and control a Logix-based system via the Studio 5000® environment.

primary controller The processor in a dual-processor controller that performs standard controller functionality and communicates with the safety partner to perform safety-related functions.

Probability of a dangerous failure on demand (PFD) The average probability of a dangerous failure on demand.

recoverable fault A fault, which when properly handled by implementing the fault handling mechanisms that are provided by the controller, does not force user logic execution to be ended.

requested packet interval (RPI) How frequently the originating application requires the transmission of data from the target application.

routine A set of logic instructions in one programming language, such as a ladder diagram. Routines provide executable code for the project in a controller. Each program has a main routine. You can also specify optional routines.

safe failure fraction (SFF) The sum of safe failures plus the sum of dangerous detected failures divided by the sum of all failures.

safety Add-On Instruction An Add-On Instruction that can use safety application instructions. In addition to the instruction signature used for high-integrity Add-On Instructions, safety Add-On Instructions feature a SIL 2 or SIL 3 safety instruction signature for use in safety-related functions.

safety application instructions Safety Instructions that provide safety-related functionality. They have been certified to SIL 3 for use in safety routines.

safety component Any object, task, program, routine, tag, or module that is marked as a safety-related item.

safety input A combination of produced and consumed safety tags, mapped safety inputs, and inputs from safety modules.

safety instruction signature The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction. The signature is used to verify the integrity of the safety Add-On Instruction during downloads to the controller.

safety integrity level (SIL) A relative level of risk-reduction that is provided by a safety function, or to specify a target level of risk reduction.

safety I/O Safety I/O has most of the attributes of standard I/O except it features mechanisms that are certified to SIL 2 or SIL 3 for data integrity.

safety network number (SNN) Uniquely identifies a network across all networks in the safety system. You are responsible for assigning a unique number for each safety network or safety subnet within a system. The safety network number constitutes part of the Unique Node Identifier (UNID).

safety partner The processor in a dual-processor controller that works with the primary controller to perform safety-related functions in a SIL 3 system.

safety program A safety program has all attributes of a standard program, except that it can be scheduled only in a safety task. The safety program consists of zero or more safety routines. It cannot contain standard routines or standard tags.

safety protocol A network communication method that is designed and certified for transport of data with high integrity.

safety routine A safety routine has all attributes of a standard routine except that it is valid only in a safety program and that it consists of one or more instructions suitable for safety applications. (See Appendix A on page 99 for a list of Safety Application Instructions and standard Logix Instructions that can be used in safety routine logic.)

safety tags A safety tag has all attributes of a standard tag except that the GuardLogix® controller provides mechanisms that are certified to SIL 2 or SIL 3 to help protect the integrity of their associated data. They can be program-scoped or controller-scoped.

safety task A safety task has all attributes of a standard task except that it is valid only in a GuardLogix controller and that it can schedule only safety programs. Only one safety task can exist in a GuardLogix controller. The safety task must be a periodic/timed task.

safety task period The period at which the safety task executes.

safety task reaction time The sum of the safety task period plus the safety task watchdog. This time is the worst case delay from any input change that is presented to the GuardLogix controller until the processed output is available to the producing connection.

safety signature The safety signature is composed of a safety signature ID, and a timestamp (date and time when the safety signature ID is generated). The safety signature is used to verify the integrity of the safety application program during downloads to the controller.

safety signature ID A value, which the firmware calculates, that uniquely represents the logic and configuration of the safety system. The safety signature ID is independent of the timestamp.

safety task watchdog The maximum time that is allowed from the start of safety task execution to its completion. Exceeding the safety task Watchdog triggers a nonrecoverable safety fault.

set system value (SSV) A user application instruction that sets controller system data.

standard Any object, task, tag, program, or component in your project that is not a safety-related item (that is, standard controller refers generically to a ControlLogix® or CompactLogix™ controller).

standard component Any object, task, tag, program, and so on, that is not marked as being a safety-related item.

standard controller As used in this document, standard controller refers generically to a ControlLogix or CompactLogix controller.

symbolic addressing A method of addressing that provides an ASCII interpretation of the tag name.

system reaction time The worst case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safe state. System reaction time includes sensor and actuator Reaction Times, Input and Output Reaction Times (including network connection delays), and the Controller Reaction Time.

systematic capability (SC) A confidence that the systematic safety integrity meets the requirements of the specified safety integrity level (SIL). (from IEC 61508-4)

task A scheduling mechanism for executing a program. A task provides scheduling and priority information for a set of one or more programs that execute based on certain criteria. Once a task is triggered (activated), all programs assigned (scheduled) to the task execute in the order in which they are displayed in the controller organizer.

test edits Once online edits have been accepted, there are two versions of user logic residing in controller memory. The Test Edits command in the Studio 5000 Logix Designer application causes the controller to execute the new, edited version of user logic. The original, unedited version of user logic is still in controller memory, but is not executed. See untest edits.

timeout multiplier This value determines the number of messages that can be lost before declaring a connection error. See also network delay multiplier.

undetected failure A failure that is undetected by diagnostic tests, proof tests, operator intervention, or through normal operation.

untest edits Once online edits have been accepted, there are two versions of user logic residing in controller memory. The Untest Edits command in the Studio 5000 Logix Designer application causes the controller to execute the original, unedited version of user logic. The new, edited version of user logic is still in controller memory, but is not executed. See test edits.

valid connection Safety connection is open and active, with no errors.

A

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at rok.auto/pec.

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

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846
UNITED KINGDOM: Rockwell Automation Ltd. Pitfield, Kiln Farm Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication 1756-RM012F-EN-P - November 2022
Supersedes Publication 1756-RM012E-EN-P - March 2022