Safety Reference Manual

Original Instructions

Allen-Bradley

GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems

Catalog Numbers 1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L8SP, 1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK, 1756-L8SPK, 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

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

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

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

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

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

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

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

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

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

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

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

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

Chapter 4

CIP Safety and Safety Network Numbers

Chapter 5

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

Chapter 6

Safety Application Development

Chapter 7

Monitor Status and Handle Faults

Appendix A

Safety Instructions

Appendix B

Create and Use a Safety Add-On Instruction

Reaction Times

Appendix C

Checklists for GuardLogix Safety Applications

Appendix D

GuardLogix Systems Safety Data

Appendix E

Studio 5000 Logix Designer Application, Version 31 or Later, Safety-application Instructions

Appendix F

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 9.

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.

Summary of Changes

This manual contains new and updated information as indicated in the following table.

Topic	Page
Updated Preface introduction text	7
Updated Safety Partner text	16
Added Important table to Compact GuardLogix 5380 Controller Hardware section	17
Updated Safety Concept Assumptions section	47
Updated title of Table 9	72
Updated Product Failure Rates section	96

Terminology

This section defines terms that are used in this manual.

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

Also, the term ‘SIL 2’ represents SIL 2, SIL CL2, and PLd, and ‘SIL 3’ represents SIL 3, SIL CL3, and PLe.

For common abbreviations and other definitions, see the Glossary on page 103.

Additional Resources

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

Resource	Description
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.
1756 ControlLogix and GuardLogix Controllers Technical Data, publication 1756-TD001	Lists product specifications and certifications for ControlLogix and GuardLogix controllers.
CompactLogix 5380 Controllers Specifications, publication 5069-TD002	Lists product specifications and certifications for CompactLogix 5380 controllers and Compact GuardLogix 5380 controllers.
ControlLogix Chassis and Power Supply Installation Instructions, publication 1756-IN005	Provides information on how to install various ControlLogix chassis and power supplies.
CompactLogix 5380 Controllers Installation Instructions, publication 5069-IN014	Provides information on how to install CompactLogix 5380 controllers.
Replacement Guidelines: Logix5000 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
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety Application instruction set.
GuardLogix 5580 Controllers Installation Instructions, publication 1756-IN048	Provides information on how to install GuardLogix 5580 controllers.
Kinetix 5700 Safe Monitor Functions Safety Reference Manual, publication 2198-RM001	Describes the integrated stopping functions and safe monitoring functions with a Logix5000™ controller and Kinetix® 5700 servo drives.
Compact 5000 Safety Sinking Input Module Installation Instructions, publication 5069-IN020	Describes how to install the 5069-IB8S module.
Compact 5000 Configurable Safety Output Module Installation Instructions, publication 5069-IN021	Describes how to install the 5069-OBV8S module.
Compact 5000 Digital and Safety I/O Modules User Manual, publication 5000-UM004	Describes how to use Compact 5000™ digital and safety I/O modules, including how to use some of the modules in safety applications.
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.
POINT Guard I/O Safety Modules User Manual, publication 1734-UM013	Provides information on how to install and use POINT Guard I/O™ modules.
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.
Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Provides information on the Logix5000 instruction set that includes general, motion, and process instructions.
Logix Common Procedures Programming Manual, publication 1756-PM001	Provides information on programming Logix5000 controllers, including how to manage project files, organize tags, program and test routines, and handle faults.
Logix5000 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.
DeviceNet Modules in Logix5000 Control Systems User Manual, publication DNET-UM004	Provides information on how to use the 1756-DNB module in a Logix5000 control system.
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication ENET-UM001	Provides information on how to use the 1756-ENBT module in a Logix5000 control system.
ControlNet Modules in Logix5000 Control Systems User Manual, publication CNET-UM001	Provides information on how to use the 1756-CNB module in Logix5000 control systems.
Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087	Provides information on how to estimate the execution time and memory use for instructions.
Logix Import Export Reference Manual, publication 1756-RM084	Provides information on how to use the Studio 5000 Logix Designer Import/Export utility.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation® industrial system.
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page.

To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales office.

Safety Integrity Level (SIL) Concept

SIL Certification

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

Controller System	IEC 61508	IEC 62061	ISO 13849-1
	Type-approved and certified for use in safety applications up to and including:	Suitable for use in safety applications up to and including:	Suitable for use in safety applications up to and including:
GuardLogix 5580 controller systems	SIL 2(2) SIL 3(3)	SIL CL2(2) SIL CL3(3)	Performance Level PLd (Cat. 3)(2) Performance Level PLe (Cat. 4)(3)
Compact GuardLogix 5380 SIL 2 controller systems (1)	SIL 2	SIL CL2	Performance Level PLd (Cat. 3)

(1) Compact GuardLogix 5380 controller catalog numbers with a '2' at the end, for example, 5069-L3*xxxxx*S2, are for use in safety applications up to and including SIL 2.

(2) Primary controller that is used without a safety partner.

(3) Primary controller that is used with a safety partner.

IMPORTANT In the remainder of this publication:

- SIL 2 represents SIL 2, SIL CL2, and PLd
- SIL 3 represents SIL 3, SIL CL3, 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.

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 overall safety function
- The GuardLogix portion of the overall safety function
- How other devices (for example, HMI) are connected, while operating outside the function

Figure 1 - Example SIL 3 System

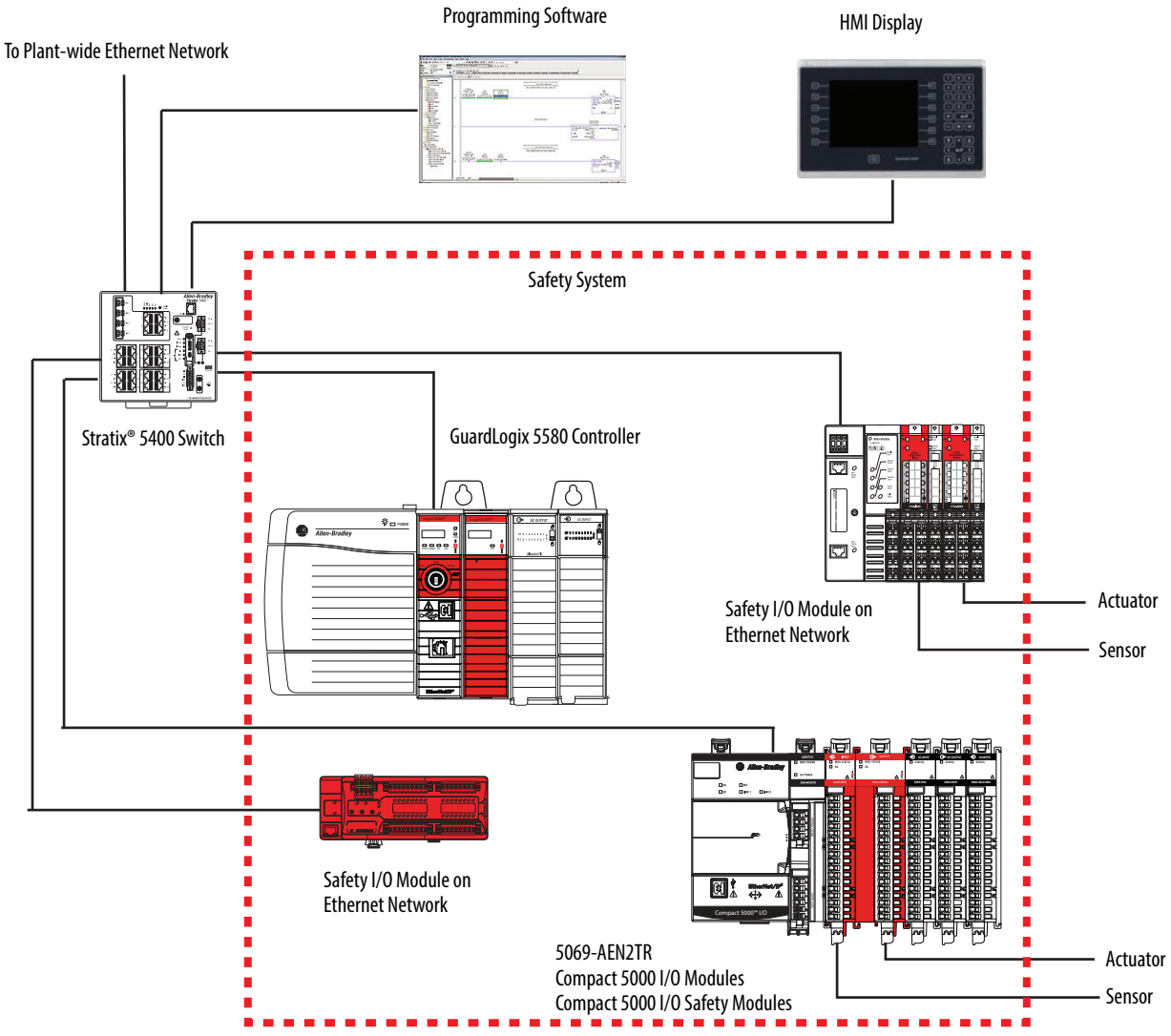
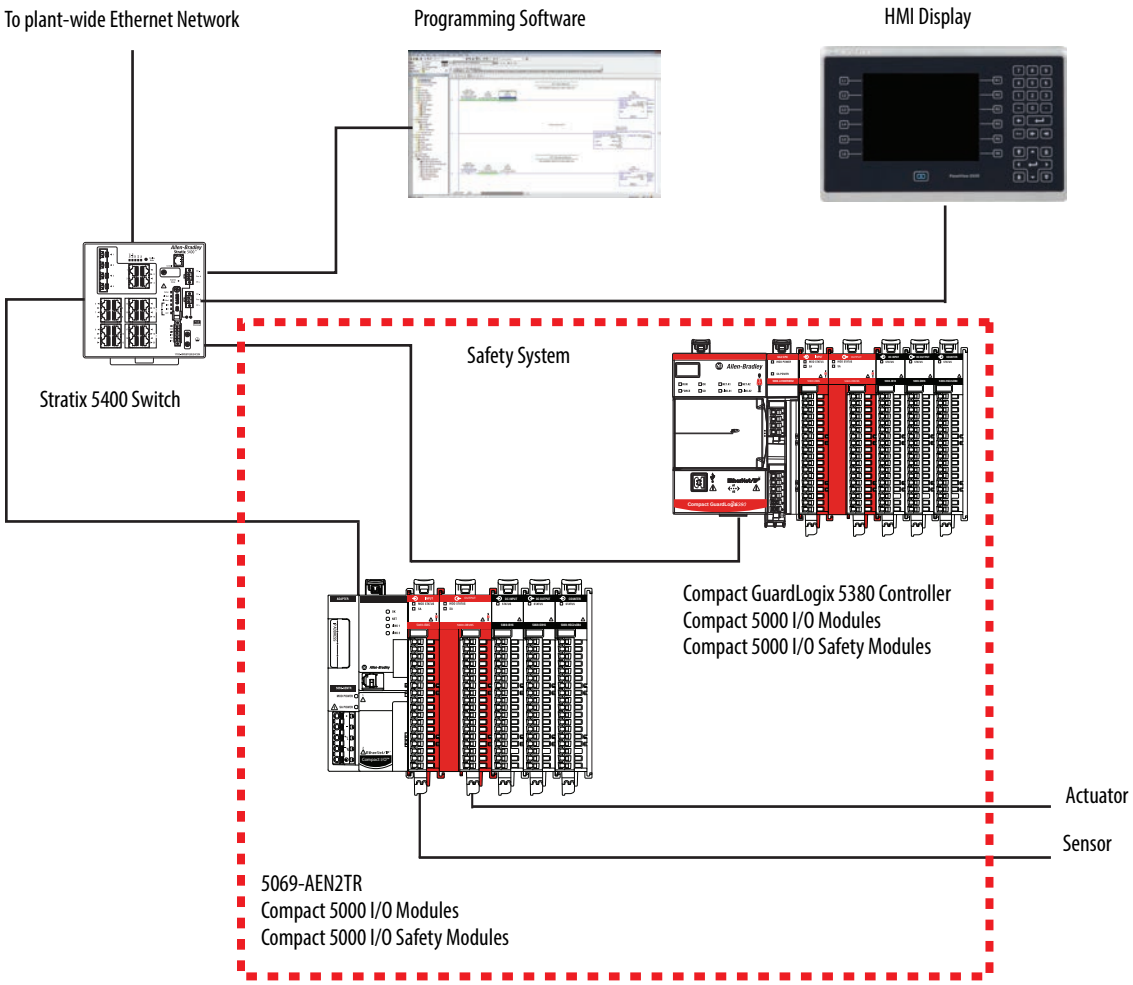


Figure 2 - Example SIL 2 System



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.

See http://www.rockwellautomation.com/global/certification/overview.page for Declarations of Conformity, Certificates, and other certification details.

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 may 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.

IMPORTANT For more information on reaction time calculation, see Appendix C on page 79.

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.

Contact Information If Device Failure Occurs

If you experience a failure with any safety device, contact your local Rockwell Automation sales office or Allen-Bradley distributor to initiate the following actions:

- Return the device to Rockwell Automation 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.

GuardLogix Controller System

For safety certificate information, see http://www.rockwellautomation.com/global/certification/safety.page. 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 (ControlLogix 558*x*S), which can be used alone in SIL 2 applications, and a safety partner (ControlLogix 558SP), 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

For the most current list of GuardLogix controller and Safety I/O devices certified series and firmware revisions, see the safety certificates at http://www.rockwellautomation.com/global/certification/safety.page.

Firmware revisions are available from the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at http://www.rockwellautomation.com/global/support/pcdc.page.

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 that are certified to the Low Voltage and EMC Directives.

To find certificates for the controllers and I/O modules, see http://www.rockwellautomation.com/global/certification/overview.page.

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 ControlLogix 558SP 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. If the two processors disagree, or cannot communicate with each other, the result is a major non-recoverable controller fault. For information on how to respond to this situation, see article 63983 in the Rockwell Automation® Knowledgebase.

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 capable controller that performs standard and safety control functions for safety-related functions in the Compact GuardLogix control system.

Controller	Cat. No.
Compact GuardLogix 5380 controller	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

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 prevent personal injury resulting from accessibility to live parts.

The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if 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 the Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions, publication 5069-IN014.

For the most current list of GuardLogix controller and Safety I/O devices certified series and firmware revisions, see the safety certificates at http://www.rockwellautomation.com/global/certification/safety.page.

Firmware revisions are available from the Rockwell Automation Product Compatibility and Download Center (PCDC) support website at http://www.rockwellautomation.com/global/support/pcdc.page.

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 http://www.rockwellautomation.com/global/certification/overview.page.

Power Supply

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

Consider the following when you choose a power supply:

- The MP power of the Compact GuardLogix 5380 controller must be powered by a 24V DC SELV/PELV-listed power supply.
- All local 24V DC safety I/O must be powered by a SELV/PELV-listed power supply.
- If the SA power connector of the Compact GuardLogix 5380 controller is used, it must be powered by 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.

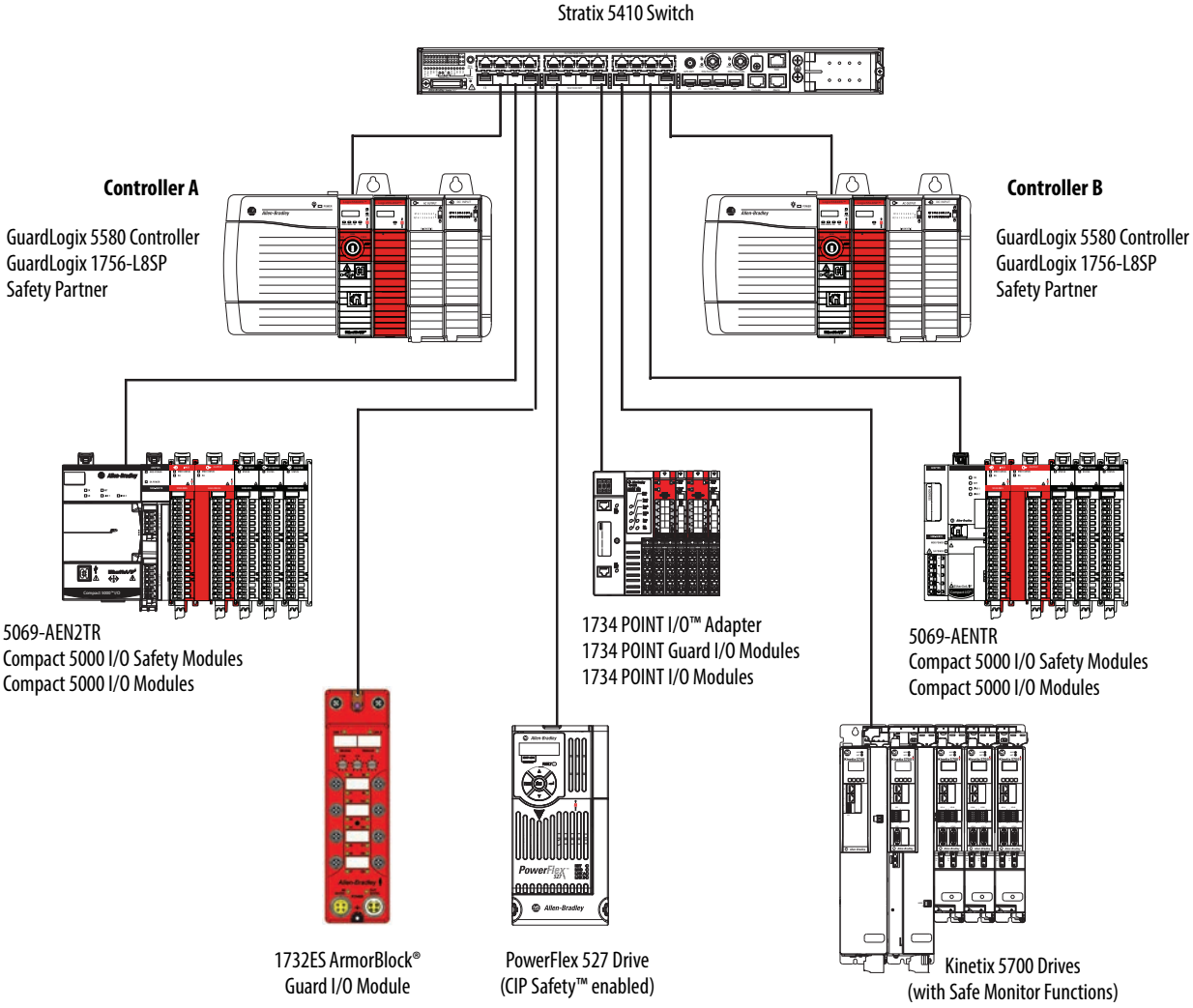
EtherNet/IP Network

The GuardLogix 5580 controller connects 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.

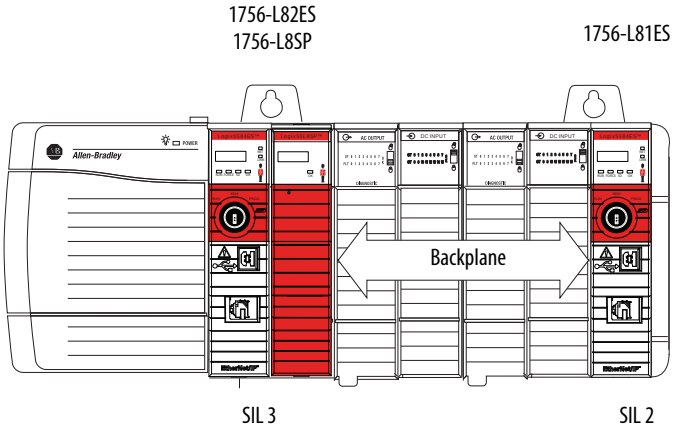
Contact your local Rockwell Automation sales office or Allen-Bradley distributor for other communication interface modules are available for use in the GuardLogix 5580 system.

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.

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

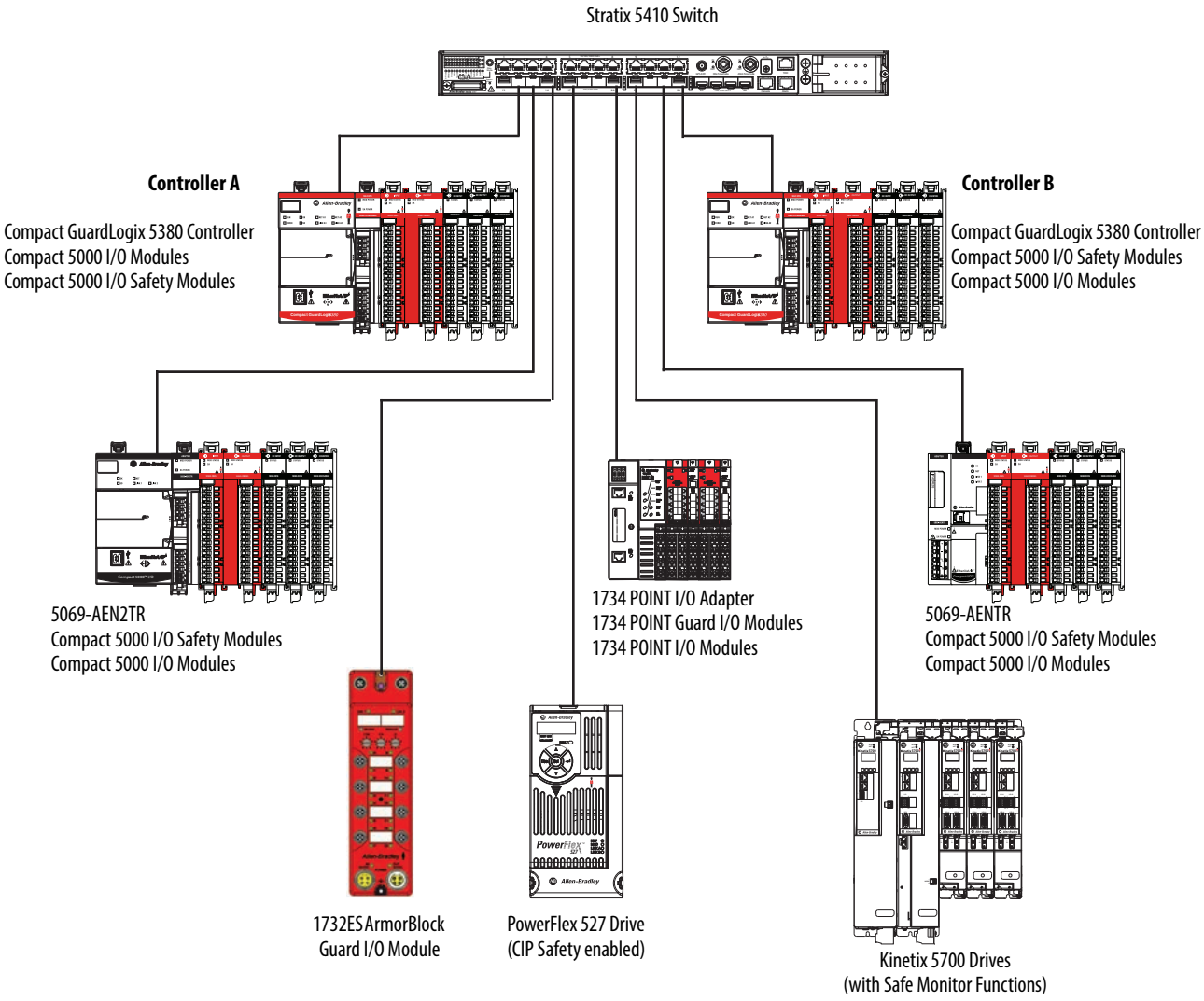


TIP Peer-to-peer safety communication between two GuardLogix 5580 controllers in the same chassis is also possible via the backplane.



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.

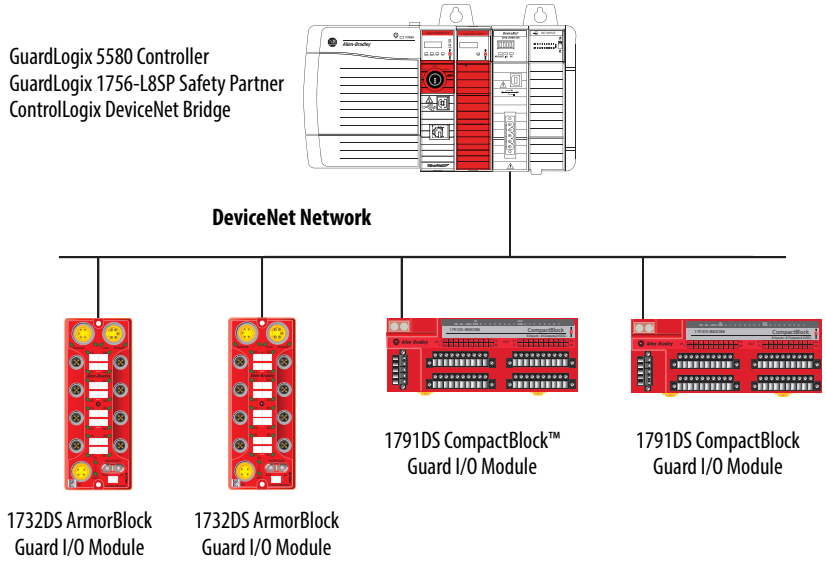
Figure 4 - Compact GuardLogix 5380 Peer-to-peer Communication Via the EtherNet/IP Network



DeviceNet Safety Network

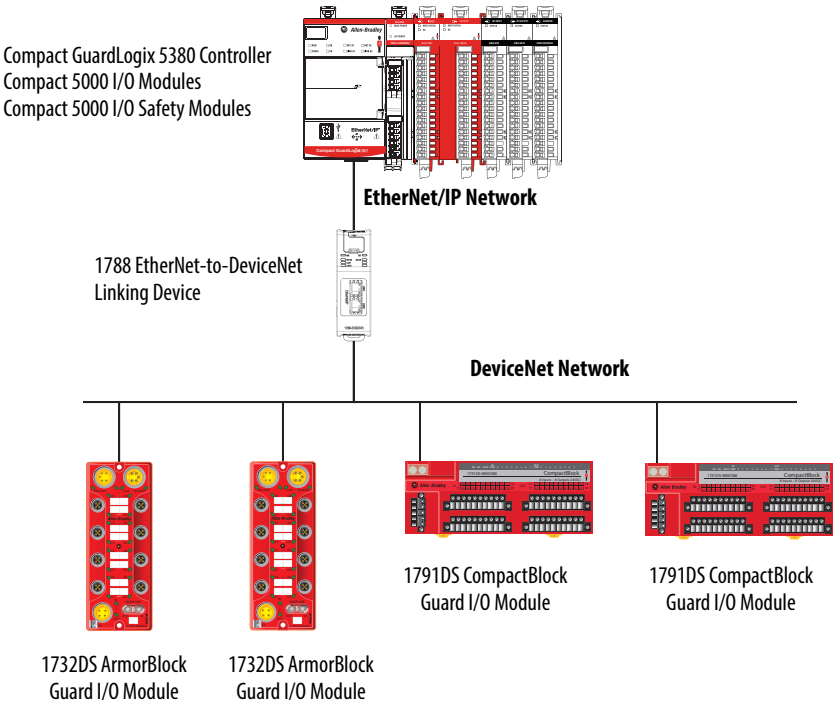
DeviceNet bridges let the GuardLogix controller control and exchange safety data with Safety I/O modules on a DeviceNet network.

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



Programming Overview

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

Use the Studio 5000 Logix Designer application to define the location, ownership, and configuration of I/O devices and controllers and create, test, and debug program logic. Only ladder diagram is supported in the GuardLogix safety task.

See Appendix A on page 69 for information on the set of logic instructions available for safety projects.

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.

Safety I/O for the GuardLogix Control System

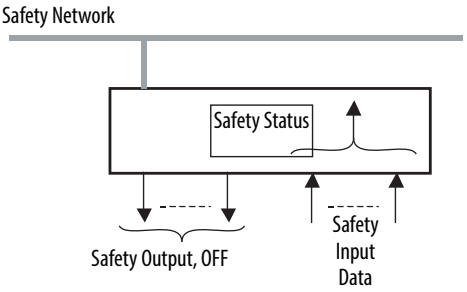
Before you operate a GuardLogix safety system with Safety I/O devices, you must first read, understand, and follow all safety information in the product documentation for those products.

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 can support on-delay and off-delay functions for input signals. In some applications, you must include off-delay, on-delay, or both when you calculate system reaction time.

For example, the On-to-Off delay filter helps to filter out noise that affects the input logic level.

See Appendix C on page 79 for information on system reaction time.

Reaction Time

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.

See Appendix C on page 79 for information on how to calculate the system reaction time.

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.

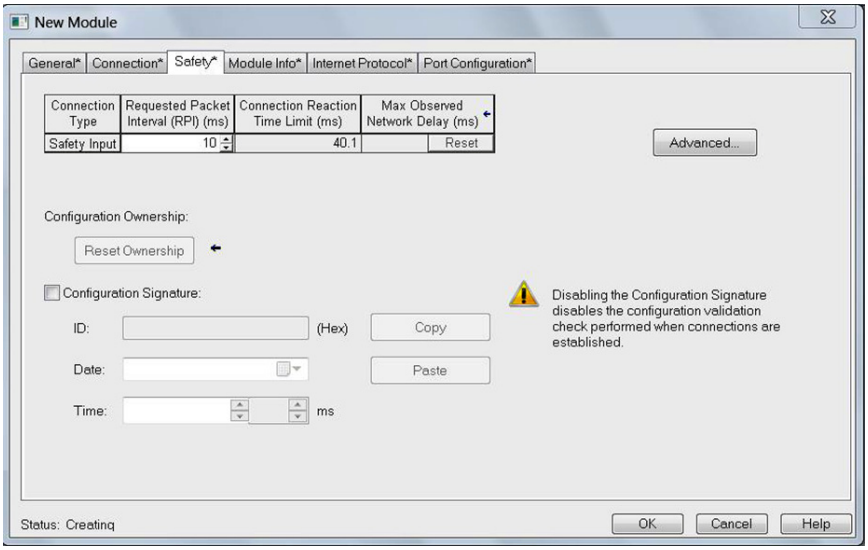
Safety I/O Configuration Signature

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

The configuration signature is calculated from the configuration of the Safety I/O device. The configuration signature is used to verify that the device is configured as expected by the safety application. When you use a GuardLogix controller, you do not have to monitor this signature. The GuardLogix controller automatically monitors the signature. If the configuration signature changes unexpectedly, the safety connection between the controller and I/O module is broken which 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 the configuration signature; and do not allow your system to run without configuration signature.



Safety I/O Device Replacement

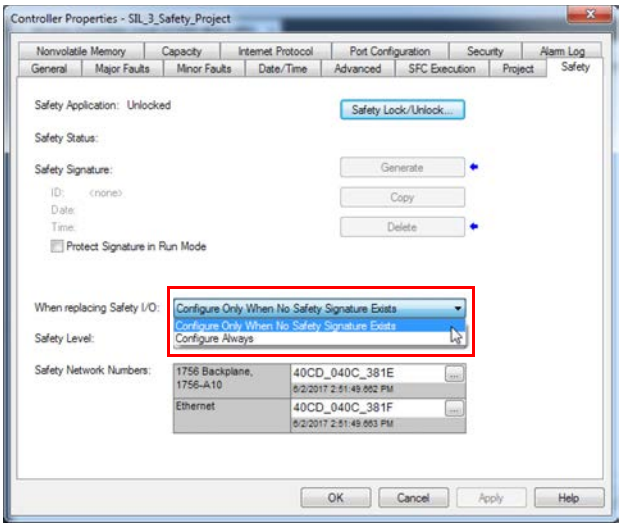
The replacement of safety devices requires that the replacement device is properly configured, and that the operation of the replacement device is verified.

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

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 7 - 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 all of 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 30.

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

CIP Safety and Safety Network Numbers

Unique Node Reference

CIP Safety control systems are composed of CIP Safety devices that are interconnected via communication networks. These networks consist of devices (switches, bridges, adapters, and so on) that 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.

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 assigned to each CIP Safety-capable port.

IMPORTANT It is your responsibility to make sure that all UNIDs are truly 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:

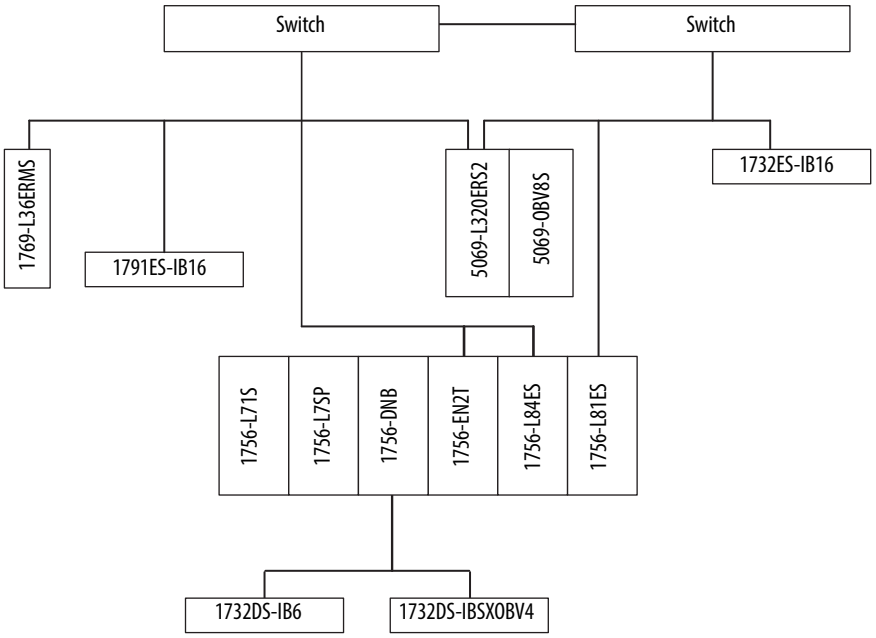
- The backplane of a chassis
- A bank of I/O modules
- An Ethernet subnet within a LAN

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

Routable CIP Safety System

The example system in Figure 8 is not interconnected to another CIP Safety system through a larger, plant-wide Ethernet backbone. Therefore, Figure 8 illustrates the extent of a routable CIP Safety system.

Figure 8 - Safety System Example



In this example:

- 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 creating controller projects, the Studio 5000 Logix Designer application generates an SNN value automatically whenever it recognizes a new subnet that 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.

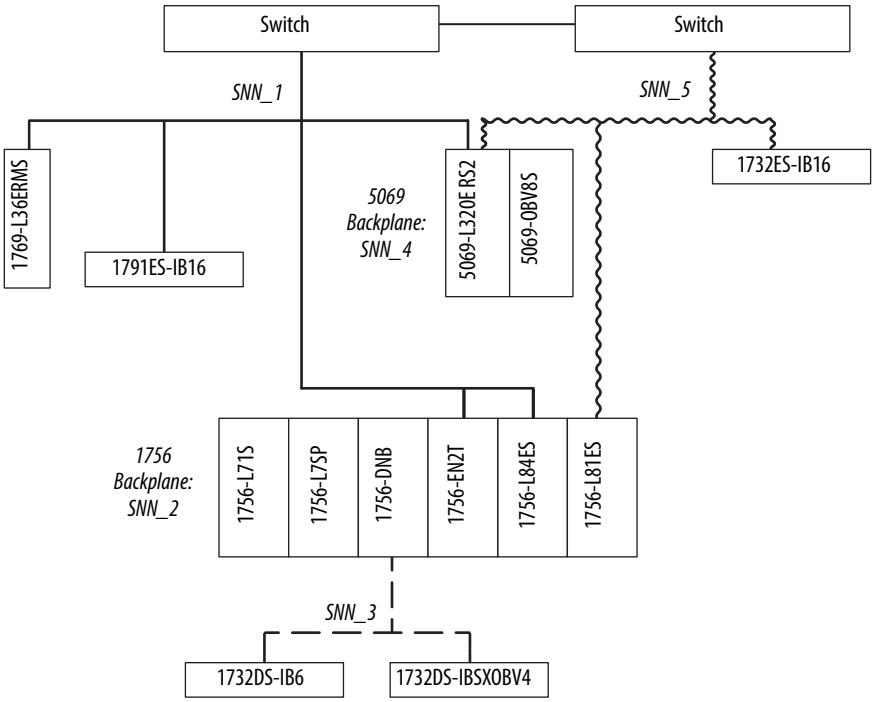
If the entire CIP Safety system consists of one controller project, these automatically generated SNN values are sufficient.

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

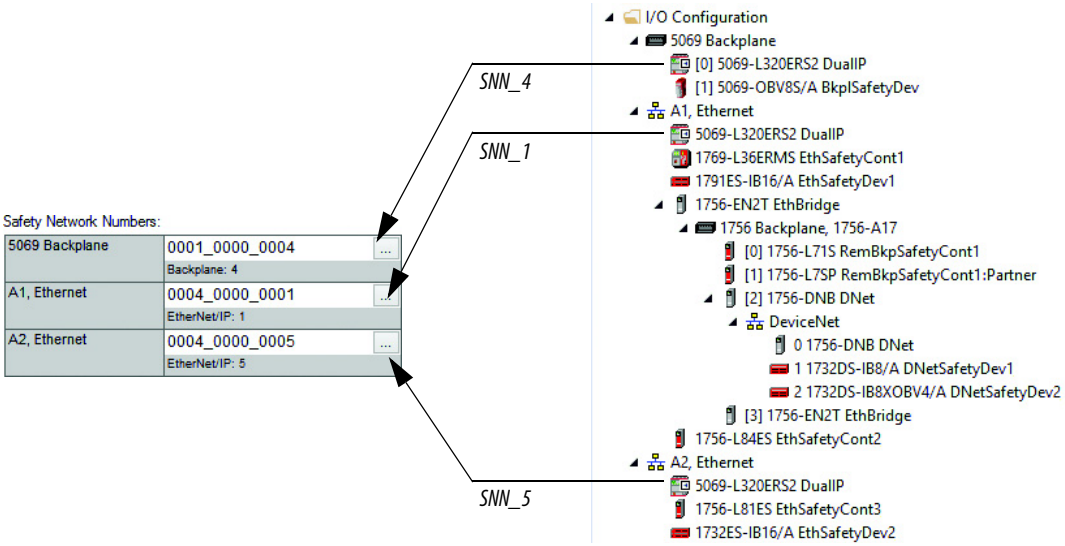
Figure 9 - Example SNN Assignment



Subnet	Type	Line	SNN Assignment
SNN_1	EtherNet/IP	———	1769-L36ERMS Ethernet port, 1791ES-IB16, 5069-L320ERS2 Ethernet port A1 (Figure 10 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-IBSX0BV4
SNN_4	Backplane	None	5069-L320ERS2 backplane (Figure 10 shows the assignment of SNN 0001_0000_0004 to this port) and 5069-OBV8S
SNN_5	EtherNet/IP	~~~	5069-L320ERS2 Ethernet port A2 (Figure 10 shows the assignment of SNN 0004_0000_0005 to this port) and 1732ES-IB16 and the 1756-L81ES Ethernet port.

Figure 10 on page 32 shows how the preceding example relates to the Compact GuardLogix 5380 (catalog number 5069-L320ERS2) Controller Organizer I/O tree.

Figure 10 - 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 allows the Studio 5000 Logix Designer application to assign the correct SNN to each safety I/O module and safety controller added to the project.

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 Studio 5000 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

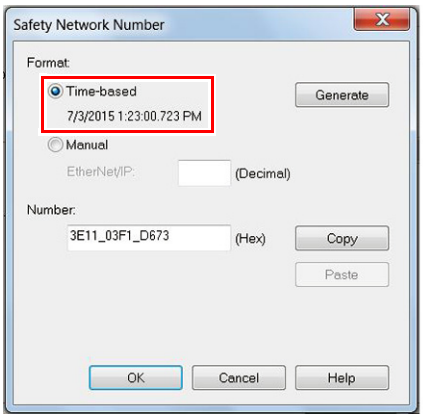
SNNs used by the system are 6-byte hexadecimal numbers. SNNs can be set and viewed in one of two formats:

- 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 11 - 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 9), you must edit the SNNs of the controller to match your network diagram. We recommend that you edit the SNNs before adding devices to the I/O Configuration in Controller Organizer.

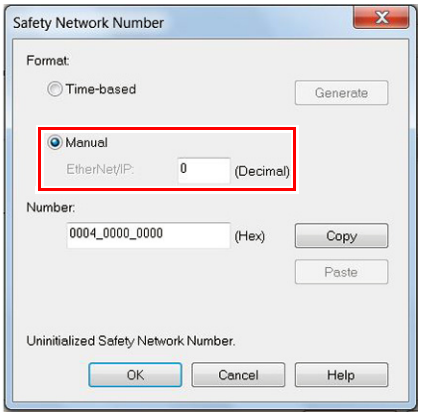
New CIP Safety I/O devices added to ports under an adapter (as opposed to the controller itself) follow similar rules.

- 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 12 - 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 Controllers 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

Differentiate Between Standard and Safety

Because it is a Logix controller, both standard (non-safety-related) and safety-related components can be used in the GuardLogix control system.

You can perform standard automation control from standard tasks within a GuardLogix project. GuardLogix 5580 controllers and Compact GuardLogix 5380 controllers provide the same functionality as other controllers. What differentiates the controllers from standard controllers is that the controllers also provide a SIL 2 or SIL 3 capable safety task.

However, a logical and visible distinction is required between the standard and safety-related portions of the application. The Studio 5000 Logix Designer application provides this differentiation via the safety task, safety programs, safety routines, safety tags, and safety I/O devices.

- GuardLogix 5580 controllers support both SIL 2 and SIL 3 levels of safety control with the safety task. See SIL Certification on page 9.
- Compact GuardLogix 5380 controllers support SIL 2 level of safety control with the safety task. See SIL Certification on page 9.

The Safety Task

IMPORTANT Only the instructions that are listed in Appendix A on page 69 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 (including interruptions by the motion task, which is always a higher priority than any user task).

Configuring the safety task with a higher priority (lower number) can reduce fluctuations in execution time, which 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 Limitations

You specify both the safety task period and the safety task watchdog. 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 on page 79.

The safety task period is limited to a maximum of 500 ms and cannot be modified online. Make sure that the safety task has enough time to finish before it is triggered again. Safety-task watchdog timeout, a nonrecoverable safety fault in the GuardLogix controller, occurs if the Safety Task does not finish before the watchdog expires.

For more information, see Chapter 7 on page 63.

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.

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 requiring only SIL 2. In that case, a SIL 2 capable controller is acceptable. While another machine has multiple safety functions, with at least one risk requiring SIL 3. In that case, a SIL 3 capable controller is required.

As discussed in this publication, 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.

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 the controller.

Regardless of whether you are using the SIL 2 or SIL 3 solution, a safety signature is required for either safety integrity level. See Generate the Safety Signature on page 52 for additional information.

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.

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, using single 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 using safety I/O modules in single channel SIL 2 applications, the following need be considered:

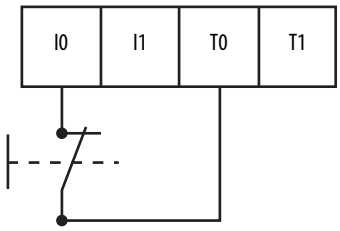
- Input or output channel must be configured for Safety Pulse Test
- Process Safety Time greater than 600 ms (the typical safety I/O pulse test interval) or the demand rate must be less than one demand per minute (for example, one per hour)

CompactBlock Guard I/O (1791 series), ArmorBlock Guard I/O (1732 series), POINT Guard I/O (1734 series), and Compact 5000 I/O Safety (5069 series) 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 13 shows how to wire SIL 2 safety circuits to Guard I/O safety input modules.

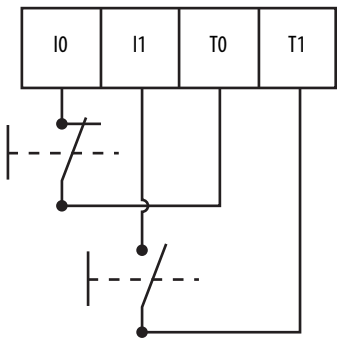
IMPORTANT The test source must be configured for pulse testing.

Figure 13 - Example Input Wiring



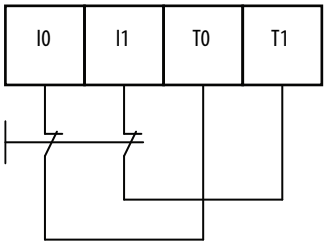
If you have two SIL 2 safety circuits, you can add a second as shown in Figure 14.

Figure 14 - Example Input Wiring in Pairs



A typical SIL 3 wiring diagram is shown in Figure 15.

Figure 15 - 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.

Use of Human Machine Interfaces

Follow these precautions and guidelines for using 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 11.

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.

Read Parameters 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.

Change Parameters in SIL-rated Systems

A parameter change in a safety-related loop via an external (that is, outside the safety loop) device (for example, an HMI) is allowed only with the following restrictions:

- Only authorized, specially trained personnel (operators) can change the parameters in safety-related systems via HMIs.
- The operator that changes a safety-related system via an HMI is responsible for the effect of those changes on the safety loop.
- You must clearly document variables that are to be changed.
- You must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI.
- Changes can be accepted in a safety-related system only if the following sequence of events occurs:
  a. The new parameter value must be sent twice to two different tags; that is, both values must not be written to with one command.
  b. The two standard tags that receive the parameter 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 should read 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.

Safety Programs

A safety program has the attributes of a standard program, except that it can be scheduled only in the safety task. 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. A safety program cannot contain standard routines or standard tags.

Safety Routines

Safety routines have the attributes of standard routines, except that they can exist only in safety programs, cannot read or write standard tags, and can only be done in Ladder Logic. 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 on page 69.

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 attributes of standard tags with the addition of mechanisms to provide data integrity at the configured SIL level (SIL 2 or SIL 3).

Safety tags can be composed of the following:

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

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 Aliasing between standard and safety tags is prohibited in safety applications.

Tags that are classified as safety tags are either controller-scoped or program-scoped. Either standard or safety logic or other communication devices can read controller-scoped safety tags, but only safety logic or another GuardLogix safety controller via a consumed tag can write the controller-scoped safety tags. Program-scoped safety tags are accessible only by local safety routines. These routines reside within a safety program.

Tags that are associated with Safety I/O and produced or consumed safety data must be controller-scoped safety tags.

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.

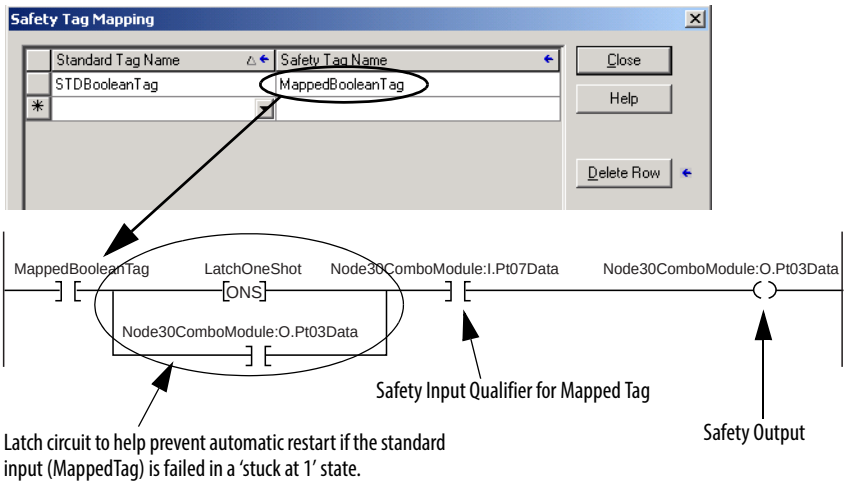
Standard Tags in Safety Routines (Tag Mapping)

Controller-scoped standard tags can be mapped into safety tags, providing you with a mechanism to synchronize standard and safety actions.

ATTENTION: When using 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 directly control a safety output with standard tag data.

This example illustrates how to qualify the standard data with safety data.

Figure 16 - Qualify Standard Data with Safety Data



Safety Application Development

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, meaning that programming errors can be detected by strict adherence to specifications, programming, and naming rules can detect programming errors.
- 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:
  - Validating the overall functionality of the implemented safety functions, including I/O configuration performed by Add-On Profiles (AOP), beyond the limits of the individual devices (boundary testing).
  - Verifying the correct versions of software are used.

Table 1 - 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 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 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 Task logic is being scanned. • All safety task process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.

Table 2 - 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).
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).
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 allows recovery from a Nonrecoverable Safety Fault without redownloading. • Safety signature is unprotected and anyone who has access to the controller can delete it.
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 allows recovery from a Nonrecoverable Safety Fault without redownloading. • Safety signature is protected. You must enter the unlock password to unlock the controller before you can delete the safety signature.

(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 develops 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:

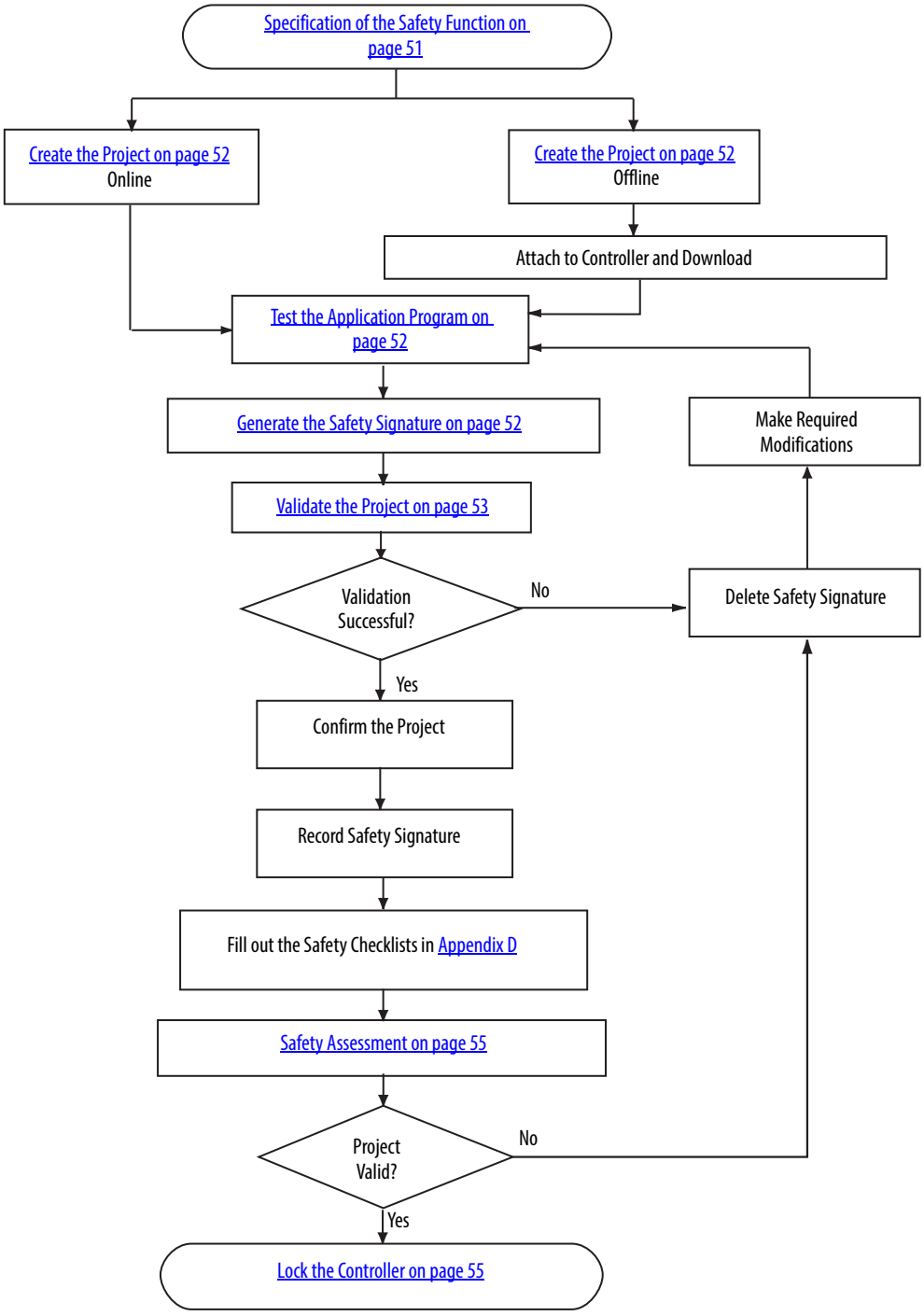
IMPORTANT

- The Studio 5000 Logix Designer application has been certified to clause 7.4.4 of IEC 61508-3 Edition 2 and may 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 may be 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 may 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 54 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 17 - 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 running 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.

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

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.

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

IMPORTANT When the safety application has been validated, there may 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.

You can delete the safety signature only when the GuardLogix controller is safety-unlocked and, if online, the key switch is in the REM or PROG position. When Protect Signature in Run mode is checked, the controller does not allow you to delete the safety signature in Run mode.

You cannot update the firmware when a safety signature exists.

When a safety signature exists, the following actions are not permitted within the safety task:

- Online or offline programming or editing of safety components
- Forcing safety I/O
- Data manipulation of safety components (except through routine logic or another GuardLogix controller)

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 start-up and project validation on the safety application in the context of the new sensors, actuators, wiring, networks, and control system physical equipment.

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.

See Appendix B on page 73 for information about the creation and use of safety Add-On Instructions in SIL 3 applications.

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

Lock the Controller

We recommend that you safety-lock the GuardLogix controller to help protect safety control components from modification. 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. However, safety-locking alone does not satisfy SIL 2 or SIL 3 requirements.

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 controller.

The default state of the controller is safety-unlocked. 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.

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

For more information about the safety-lock feature, 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

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. As a result, all offline safety tag values are updated to the snapshot values saved at the moment the signature was generated. In this case, the option to upload tag values only affects standard 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

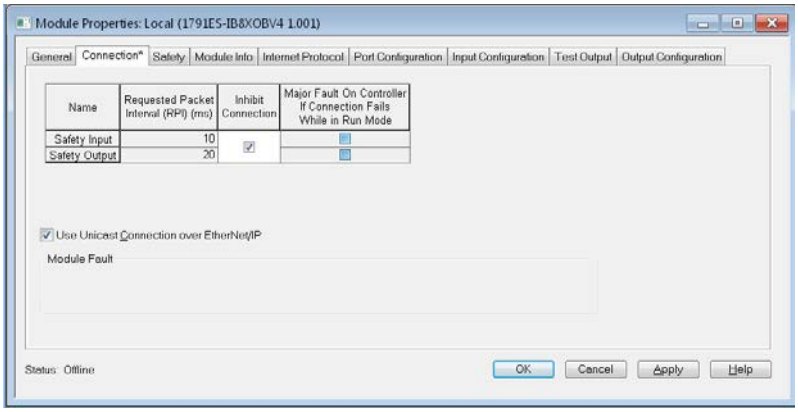
All data that is contained in an I/O, produced, or consumed safety tag, including CONNECTION_STATUS, can be forced while the project is safety-unlocked and no safety signature exists. However, forces must be removed, not just disabled, on all safety tags before the safety project can be safety-locked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

TIP 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 if the application program is safety-locked or a safety signature exists. Follow these steps to inhibit a specific safety I/O device.

1. In the Studio 5000 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.

TIP 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 absolutely 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.
- 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 key switch 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 18 on page 61 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 18 on page 61 shows the process for online editing.

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

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

See Generate the Safety Signature on page 52 and Lock the Controller on page 55 for more information.

For detailed information on how to edit Ladder Logic in the Studio 5000 Logix Designer application while online, see the Logix5000 Controllers Quick Start, publication 1756-QS001.

Modification Impact Test

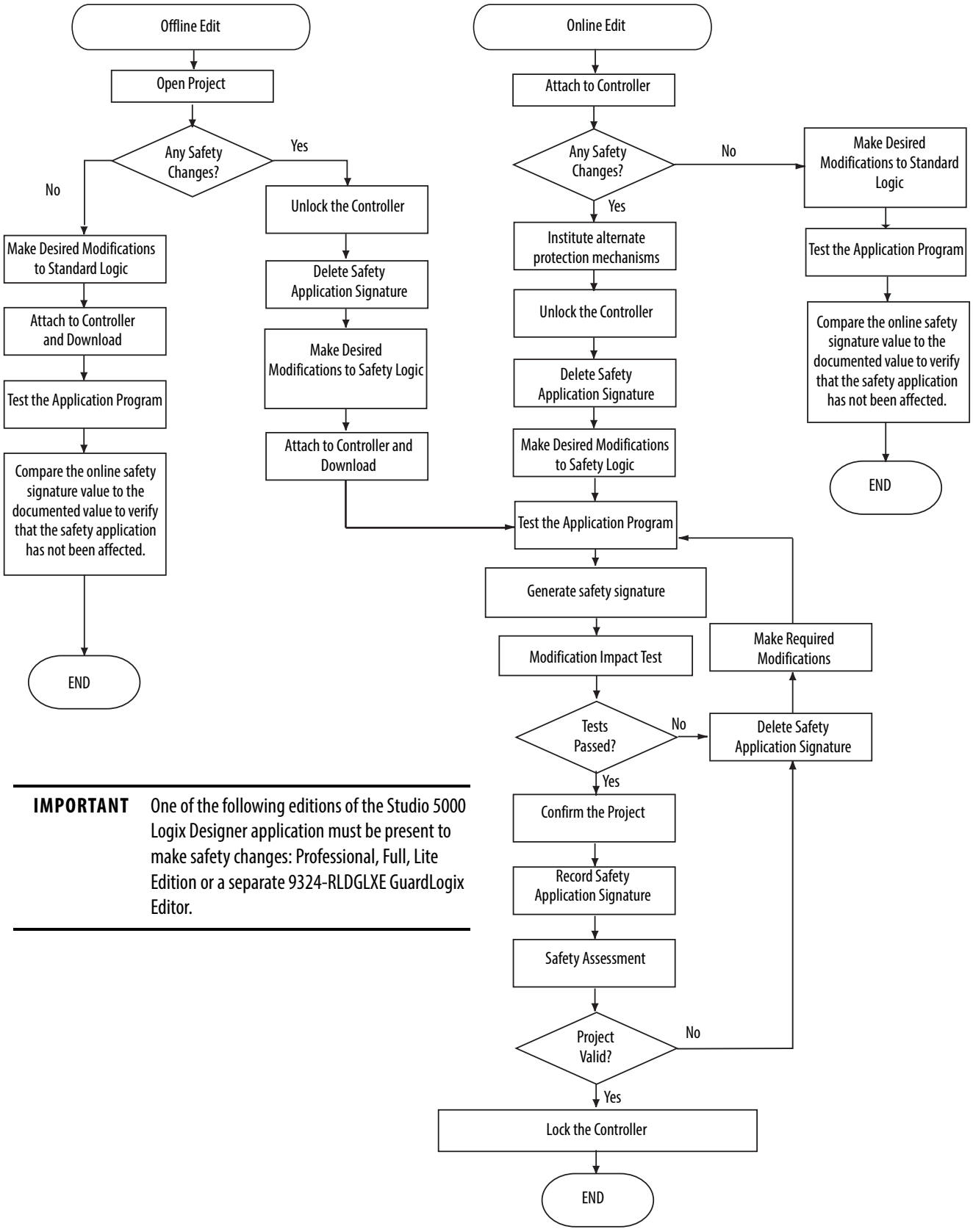
Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system. All appropriate phases of the software safety lifecycle must be conducted as indicated by the impact analysis.

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 18 - Online and Offline Edit Process



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

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 (see Appendix D on page 89).

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 are not reliable indicators for safety functions. Use them only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

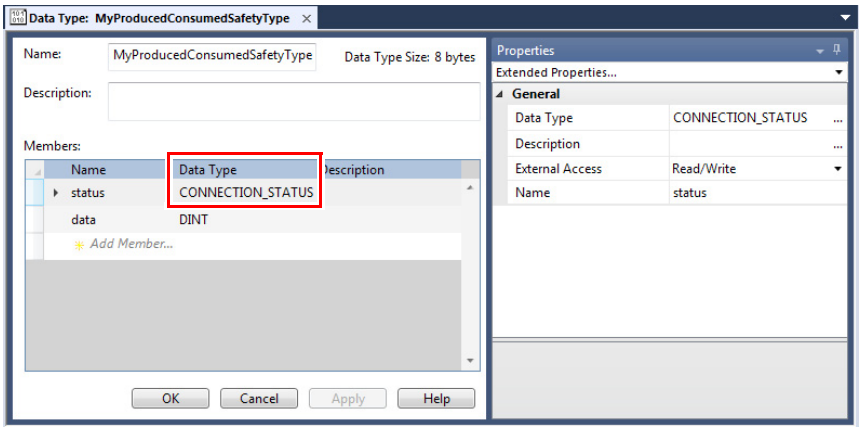
Monitoring System Status

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 19 - Data Type Dialog Box



The first two bits of the CONNECTION_STATUS data type contain the RunMode and ConnectionFaulted status bits of a device. Table 3 describes the combinations of the RunMode and ConnectionFaulted states.

Table 3 - 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, which sets all input data to the safe state and the associated input status to faulted.
- The output device detects output connection failures, which is responsible for de-energizing its outputs.
- Generally, the safety controller also has input connections from output devices; the safety controller determines the status of these input connections, however the input connection status is not the primary mechanism to de-energize the 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 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 on page 97 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 on using GSV and SSV instructions, see the Logix5000 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, safety logic and the safety protocol are terminated. Safety task watchdog and control partnership faults fall into this category.

When the safety task encounters a nonrecoverable safety fault, 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.

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

Recoverable 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 eliminate 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. See more information on status indicators, see:

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

Fault Codes

Table 4 shows the fault codes specific to GuardLogix 5580 and Compact GuardLogix 5380 controllers. The type and code correspond to the type and code that is displayed on the Major Faults tab of the Controller Properties dialog box and in the PROGRAM object, MAJORFAULTRECORD (or MINORFAULTRECORD) attribute.

Table 4 - Major Safety Faults (Type 14)

Code	Cause	Status	Corrective Action
01	Task watchdog expired. User task has not completed in a specified period. A program error caused an infinite loop, the program is too complex to execute as quickly as specified, or higher priority or background tasks are keeping this task from finishing.	Nonrecoverable	Clear the fault. If a safety task signature exists, safety memory is reinitialized and the safety task begins executing. If a safety task signature does not exist, you must redownload the program so the safety task can run. If the application allows, increase the watchdog time.
02	An error exists in a routine of the safety task.	Recoverable	Correct the error in the user-program logic.
07	Safety task is inoperable. This fault occurs when the safety logic is invalid or not present.	Nonrecoverable	Clear the fault. If a safety task signature exists, safety memory is reinitialized via the safety task signature and the safety task begins executing. If a safety task signature does not exist, you must download the program again so the safety task can run.

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

Safety Partner Fault

The 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.

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.

Table 5 - General Safety-application 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 6 - Metal-form Safety-application 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 on RSLogix 5000® instructions, see Appendix F on page 97.

Table 7 - RSLogix 5000 Safety Application Instruction Descriptions

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 these ladder diagram safety instructions.

Table 8 - 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.

Table 8 - Ladder Diagram Safety Instructions (Continued)

Type	Mnemonic	Name	Purpose
Timer	TON	Timer On Delay	Time how long a timer is enabled.
	TOF	Timer Off Delay	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.
Compare	CMP(2)	Compare	Perform a comparison on the arithmetic operations 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.
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 operand is a constant and that the source and destination length are the same.

(2) Advanced operands like 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 9 - 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 Kinetix 5700 ERS4 drives with the Studio 5000 Logix Designer application (V31 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

See the following publications for more information.

Table 10 - Additional Resources

Resource	Description
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides more information on the safety application instructions.
Logix5000 Controllers Generals Instructions Reference Manual, publication 1756-RM003	Provides information on the Logix5000 instruction set that includes general, motion, and process instructions.

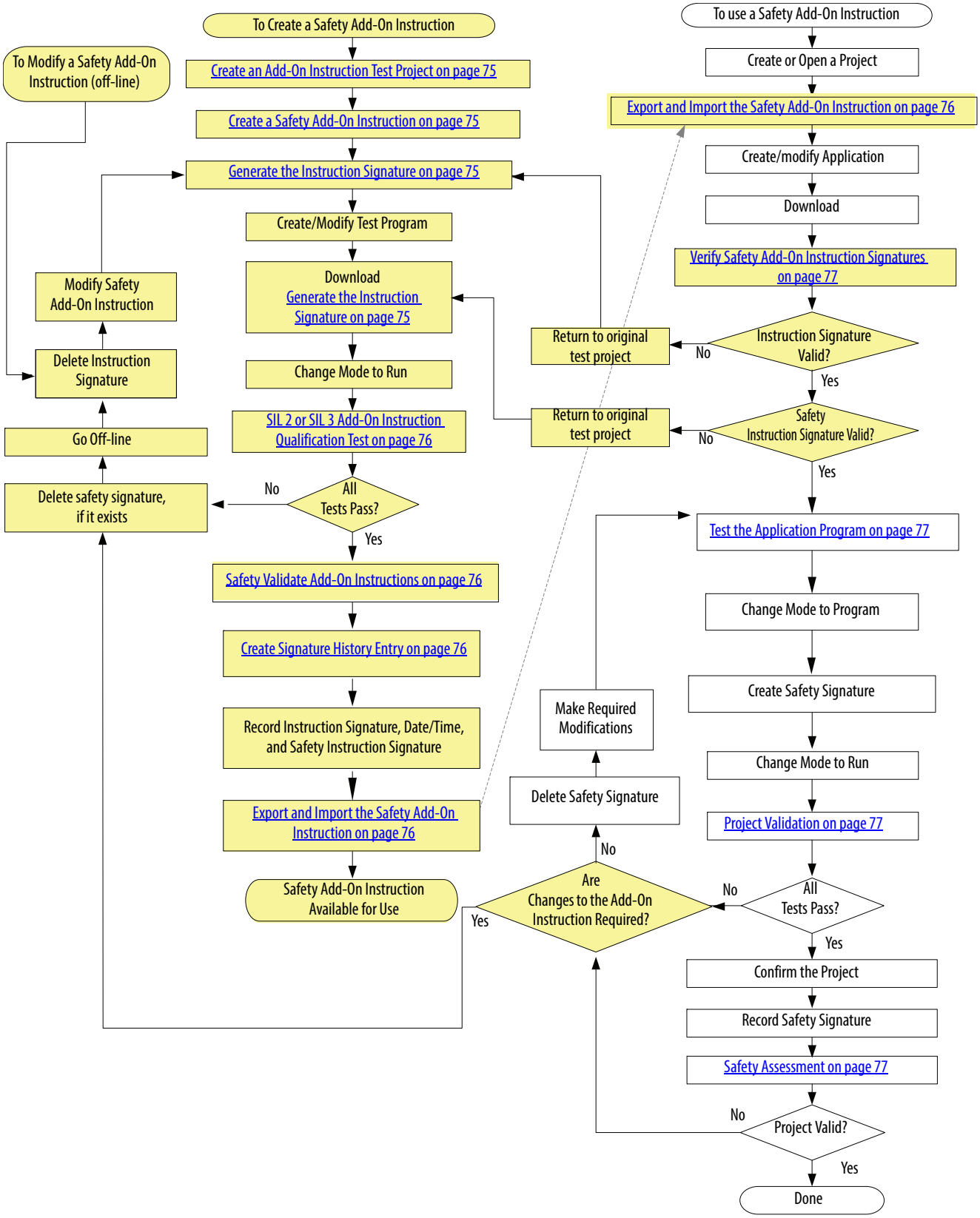
Create and Use a Safety Add-On Instruction

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 20 on page 74 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 20 - Flowchart for Creating and Using Safety Add-On Instructions



Create an Add-On Instruction Test Project

You must create a unique test project, specifically 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 52.

Create a Safety Add-On Instruction

For guidance in how to create Add-On Instructions, see the Logix5000 Controllers Add-On Instruction Programming Manual, publication 1756-PM010.

Generate the Instruction Signature

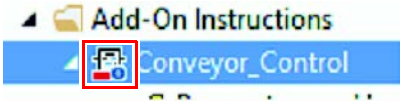
The instruction signature lets you quickly determine if the instruction has been modified. Each Add-On Instruction can have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and can sometimes be required for regulated industries. 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.

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.

TIP 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.

See Validate the Project on page 53 for more information on requirements.

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 on safety assessments, see the Machinery SafeBook 5.

Notes:

Reaction Times

Connection Reaction Time Limit

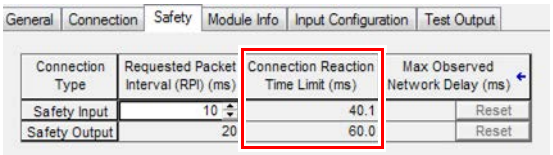
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data that is used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. The following equations determine the Connection Reaction Time Limit:

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

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

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

Figure 21 - Connection Reaction Time Limit



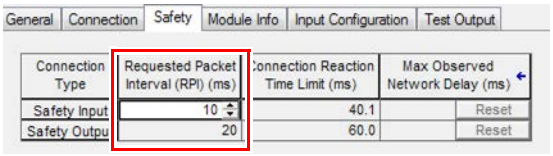
Specify the Requested Packet Interval (RPI)

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 Connection Reaction Time Limit is adjusted immediately when the RPI is changed via the Studio 5000 Logix Designer application.

Figure 22 - 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.

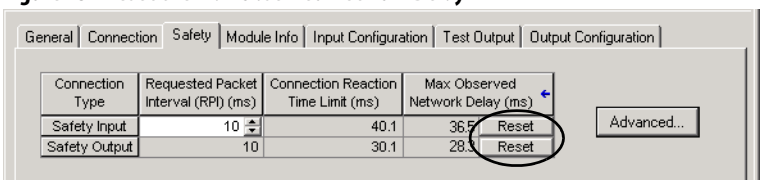
See System Reaction Time on page 13 for safety task period details.

For typical applications, the default Connection Time Reaction Limit for input connections of 4 x RPI and the default Connection Time Reaction Limit 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 84.

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 23 - Reset the Max Observed Network Delay

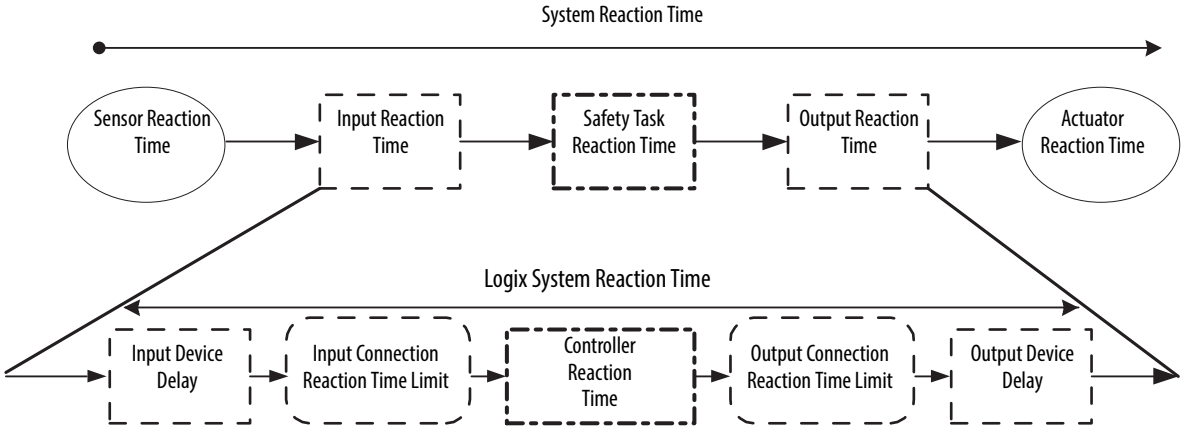


System Reaction Time

To determine the system reaction time (see System Reaction Time on page 13 for details) of any control chain, you must add up the reaction times of all of components of the safety chain.

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

Figure 24 - System Reaction Time



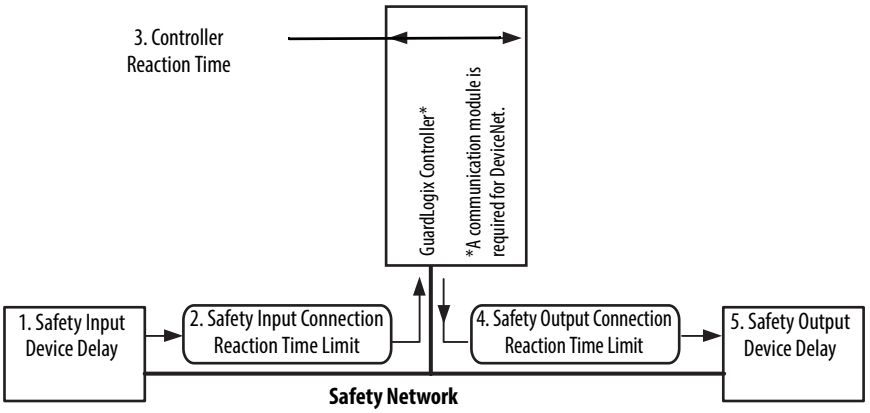
Logix System Reaction Time

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



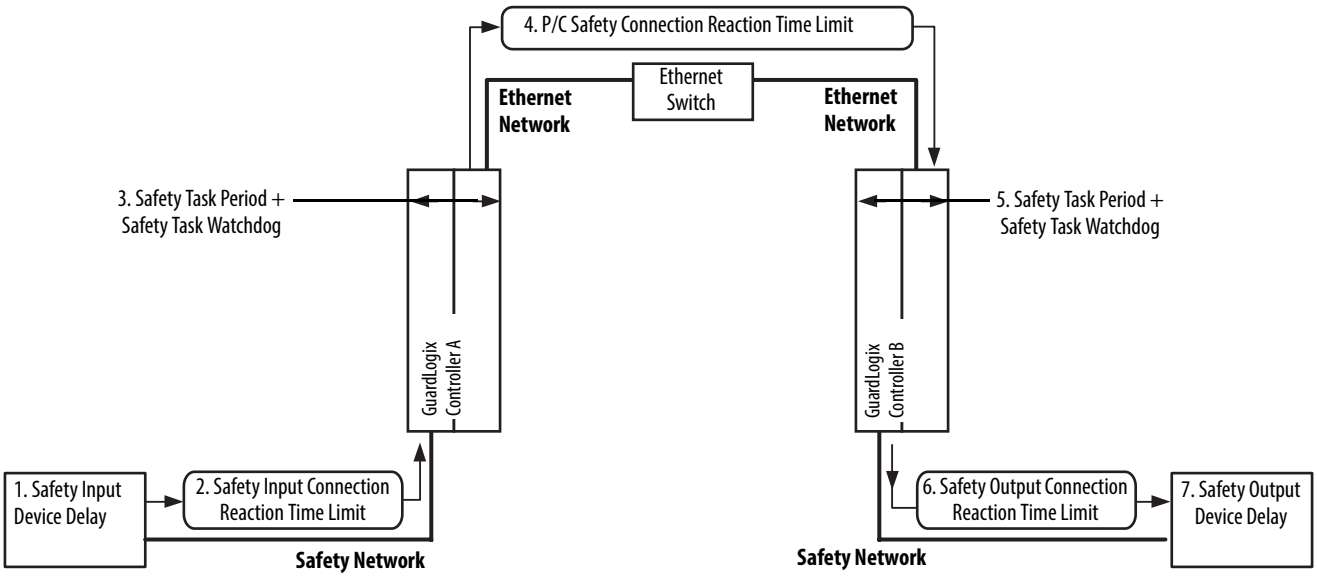
The Logix system reaction time for any simple input to logic to output chain consists of these five components:

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 Studio 5000 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 13)
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 26 - 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 11 - 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 pre-empt 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 you can successfully use for Timeout Multiplier and Network Delay Multiplier.

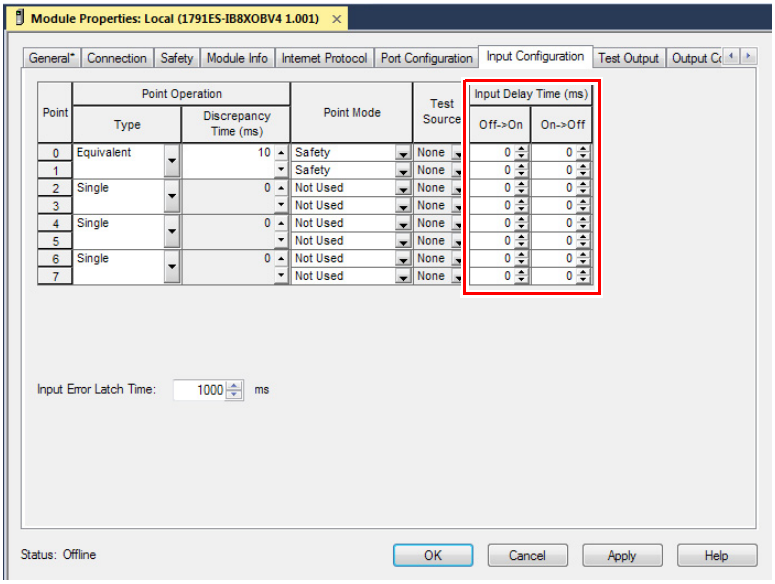
(2) The instructions in your safety task and any higher priority tasks in the controller create a lower limit for the values you can successfully use for Safety Task Period and Safety Task Watchdog

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

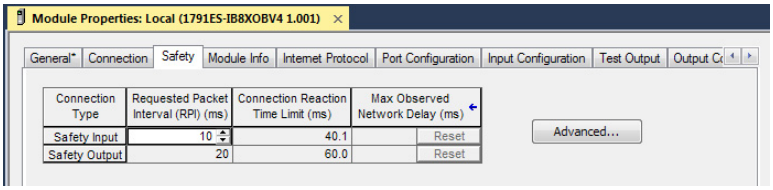
The following three values define the Connection Reaction Time Limit (CRTL).

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.

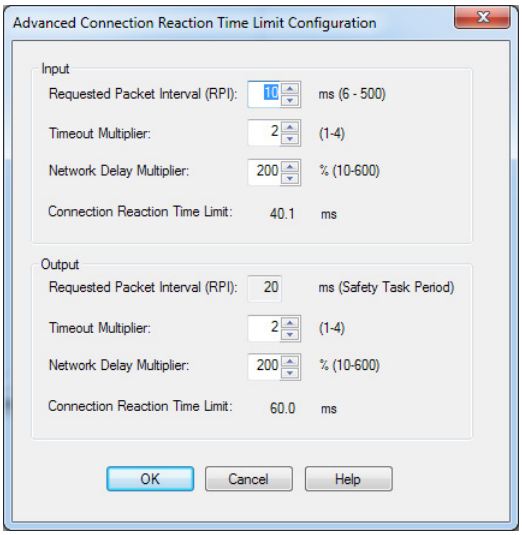
If you adjust these values, then you can adjust the Connection Reaction Time Limit. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state.

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.



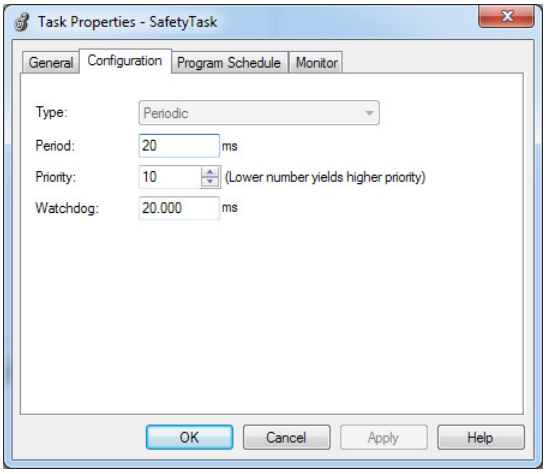
IMPORTANT The Timeout Multiplier and Network Delay Multiplier provide resilience for variations in network reliability and performance.

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.

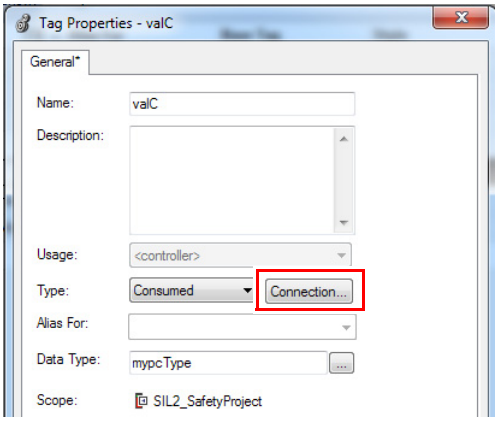


The priority of the safety task is not a safety concern, as the safety task watchdog monitors if a higher priority task interrupts the task.

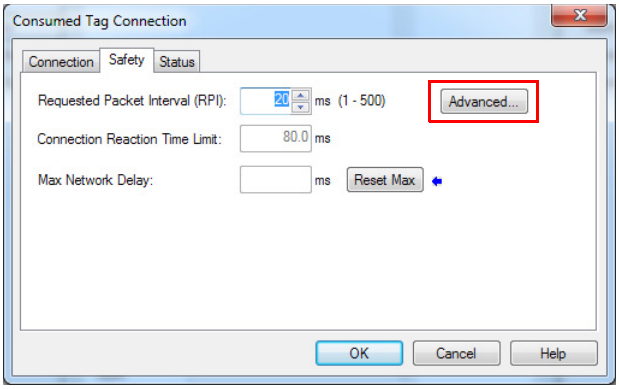
Access Produced/Consumed Tag Data

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

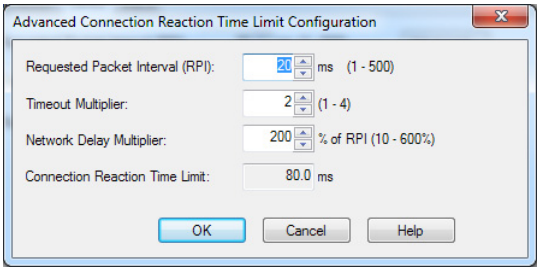
1. In the configuration tree, right-click Controller Tags and choose Edit tags.
2. In the Tag Editor, right-click the name of the tag and choose Edit Properties.
3. Click Connection.



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.

TIP 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 http://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 determined how your system can handle faults?	☐	☐	
8	Does each network in the safety system have a unique SNN?	☐	☐	
9	Is each Safety device configured with the correct SNN?	☐	☐	
10	Have you generated a safety signature?	☐	☐	
11	Have you uploaded and recorded the safety signature for future comparison?	☐	☐	
12	After a download, have you verified that the safety signature in the controller matches the recorded safety signature?	☐	☐	
13	Do you have an alternate mechanism in place to preserve the safety integrity of the system when making online edits?	☐	☐	
14	Have you considered the checklists for using SIL inputs and outputs, which are listed on page 91 and 92?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

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 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				
		Fulfilled		
Number	**Output Device Requirements**	**Yes**	**No**	**Comment**
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 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?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

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 6 on page 47 followed during 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 on page 69 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 http://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 probability of dangerous failure per hour (PFH) values for GuardLogix 1oo1 SIL 2 system or 1oo2 SIL 3 system.

For safety data that includes PFD and PFH values for safety I/O modules, see the manuals for those devices. For more information, see Additional Resources on page 8.

Useful Life

The useful life of GuardLogix controllers is 20 years.

Safety Data

For I/O devices safety data, including PFD and PFH values, see the manuals for those products.

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: http://www.marketing.rockwellautomation.com/safety-solutions/ en/MachineSafety/ToolsAndDownloads/sistema_download.

Product Failure Rates

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

Table 12 - Safety Parameters

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

(1) The HFT specified here is the product internal HFT.
(2) These values are product failure rates to be used when the product is represented as a block in a reliability block diagram (RBD).
(3) 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.

Table 13 - Safety Calculations

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

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).
- Example mission time of 10 or 20 years. Within the specified useful life (20 years), no proof test is needed.

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

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

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

$$MTTF = \frac{1}{\lambda_D}$$

$$PFH = \lambda_{DU}$$

Studio 5000 Logix Designer Application, Version 31 or Later, Safety-application Instructions

IMPORTANT We recommend use of general safety-application instructions (Table 5 on page 69) rather than the instructions detailed in this appendix.

De-energize to Trip System

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).

Use Connection Status Data to Initiate a Fault Programmatically

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 the Input Fault Latch and Reset Flowchart on page 98 to determine which rungs of logic are required for different application situations. Ladder Diagram Example 1 on page 99 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 2 on page 100. 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 Output Fault Latch and Reset Flowchart on page 101 to determine which rungs of application logic in Ladder Diagram Example 3 on page 101 are required.

Figure 27 - Input Fault Latch and Reset Flowchart

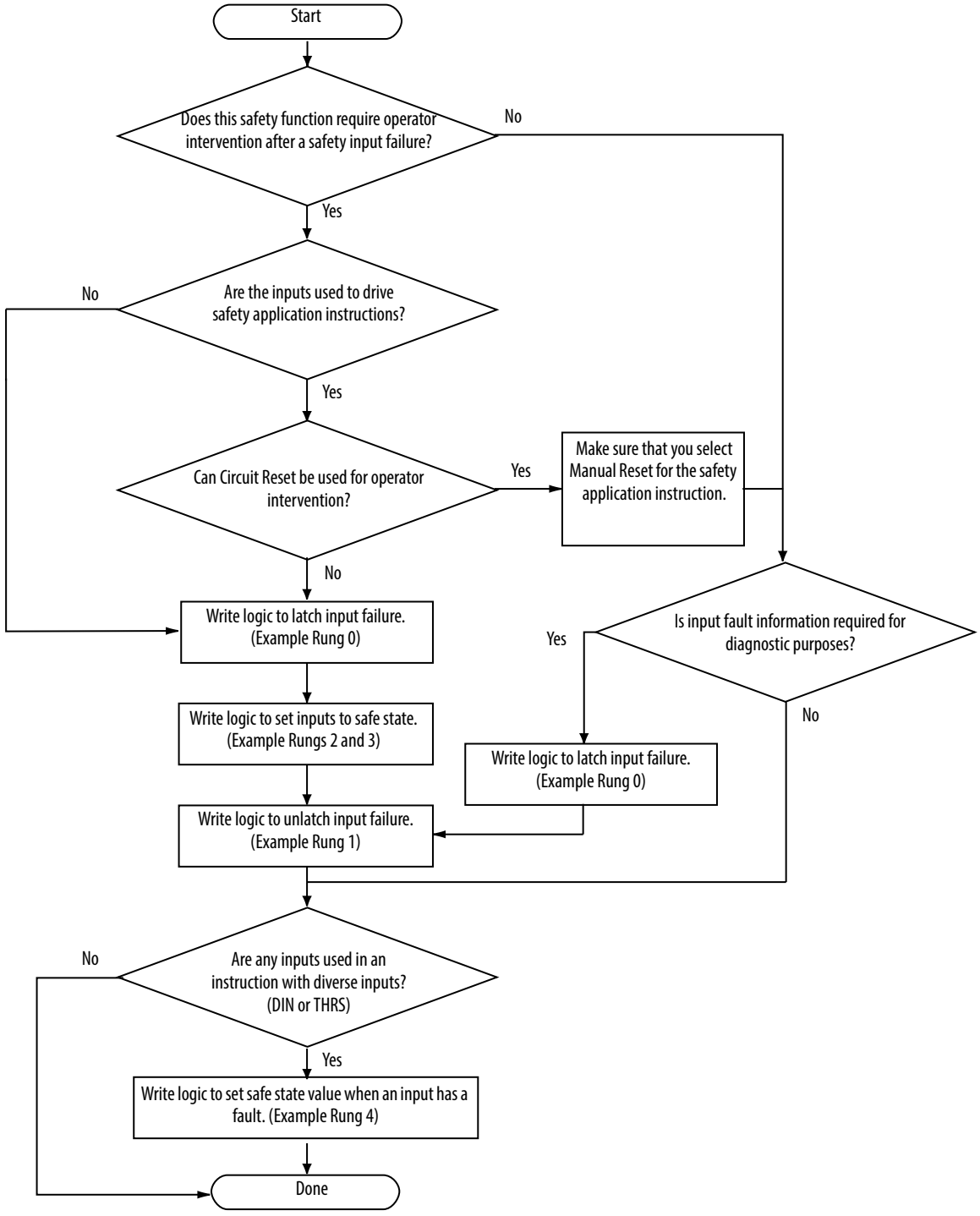


Figure 28 - Ladder Diagram Example 1

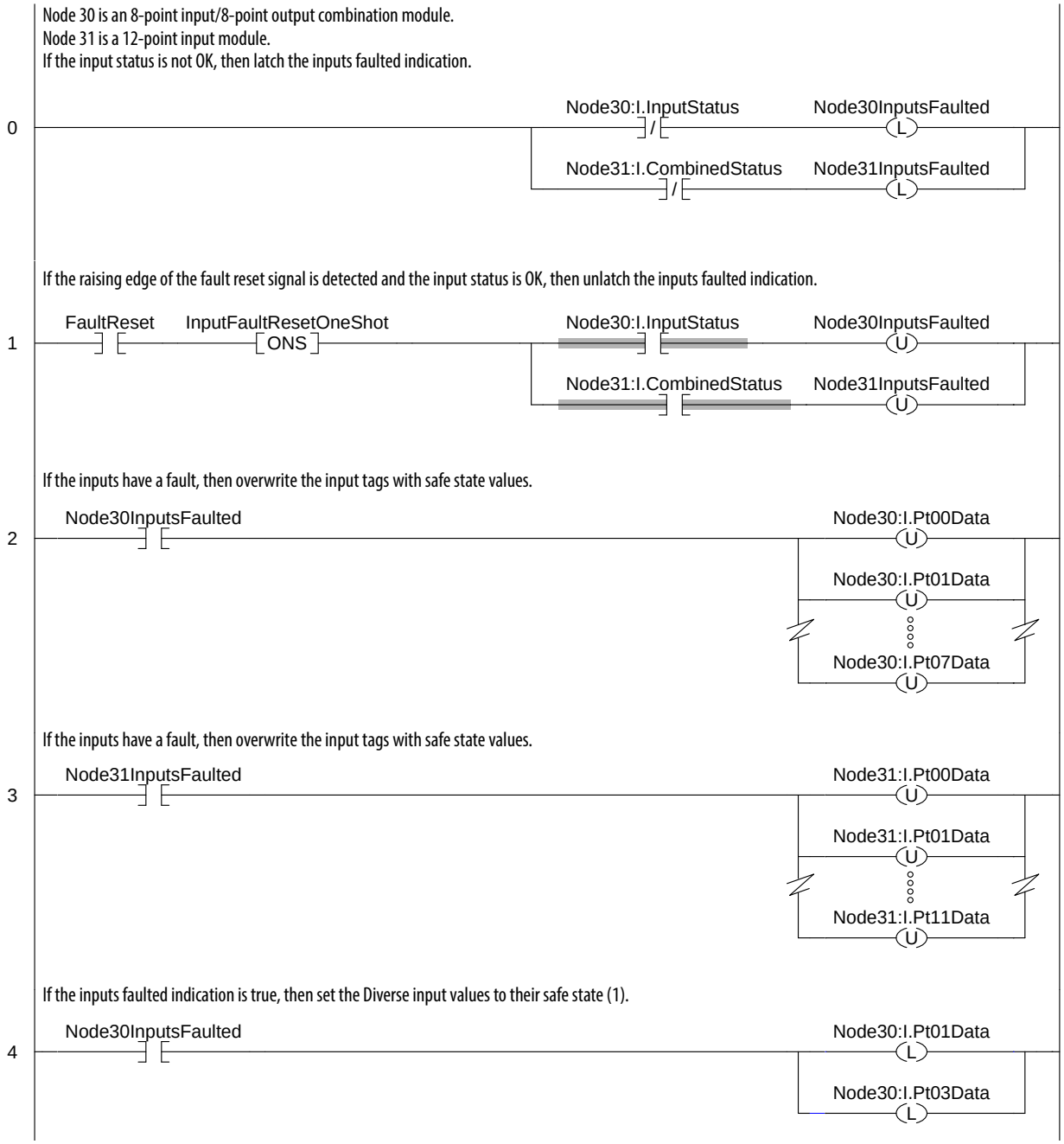


Figure 29 - Ladder Diagram Example 2

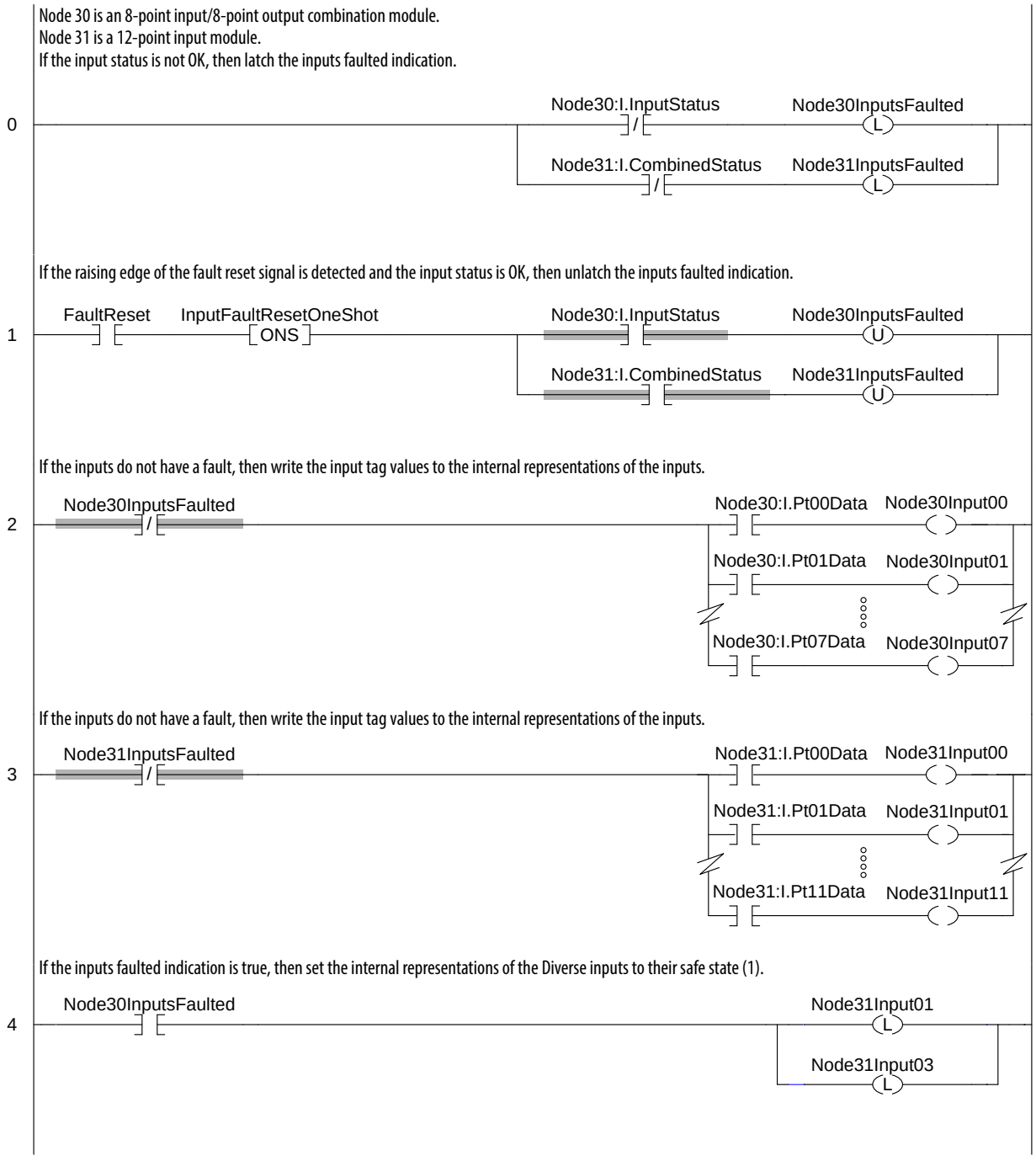


Figure 30 - Output Fault Latch and Reset Flowchart

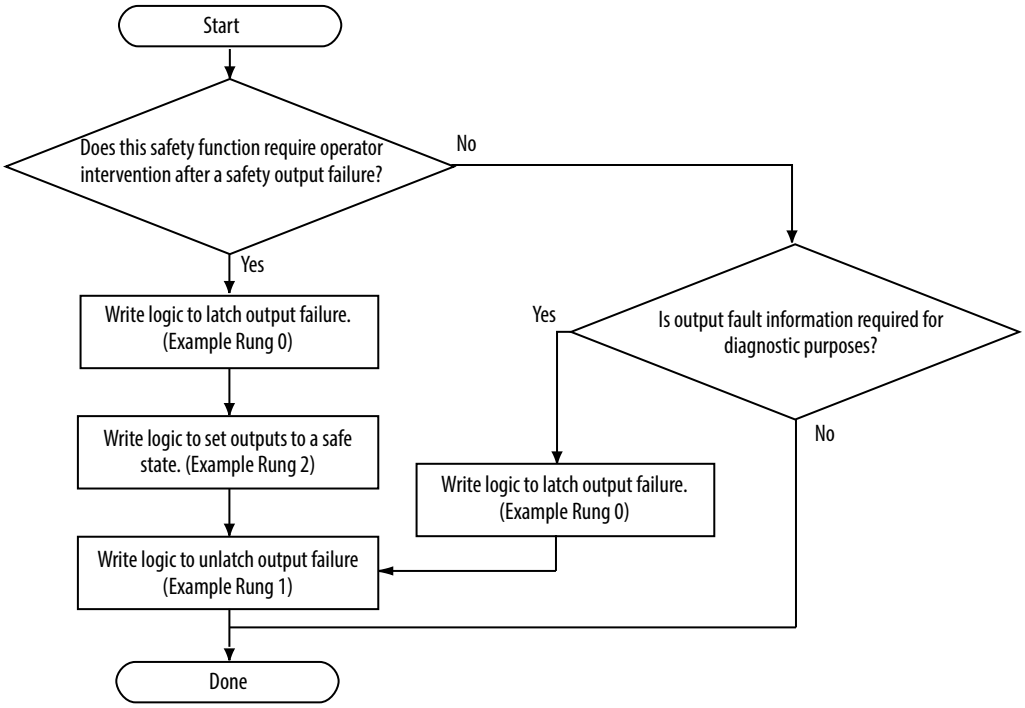
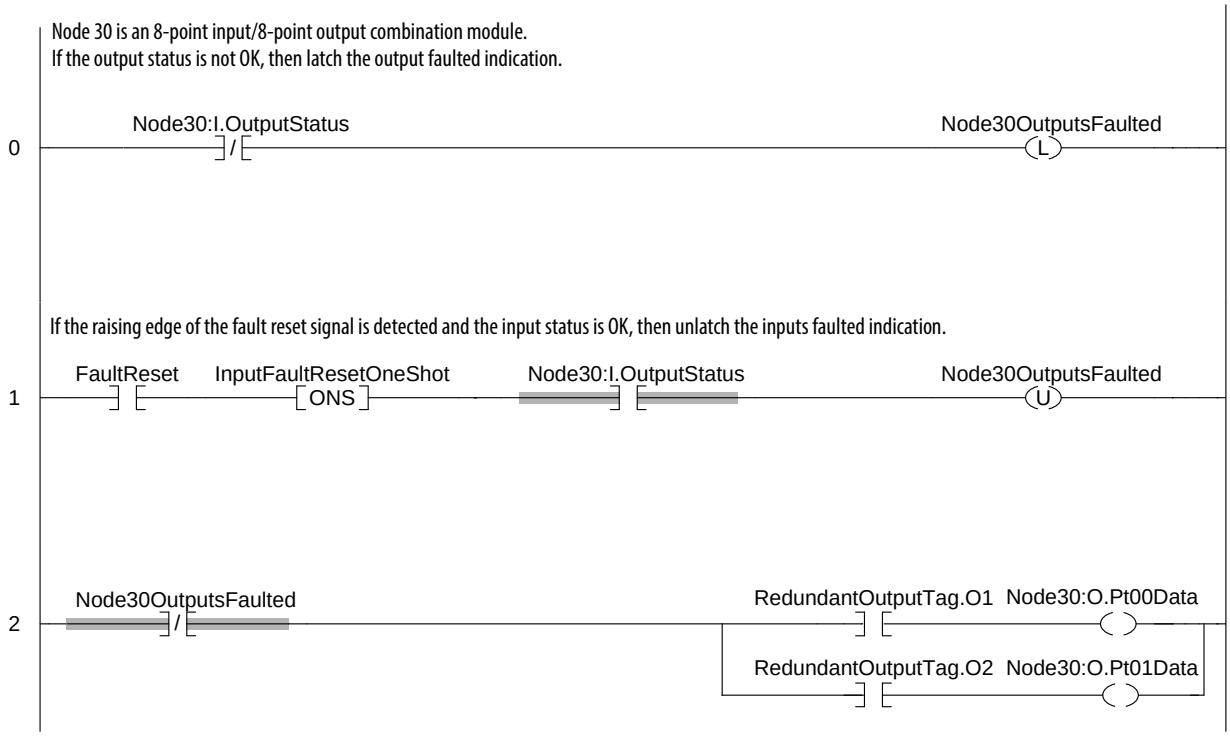


Figure 31 - Ladder Diagram Example 3



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. 1oo1 is a single-channel system.

1oo2 (one-out-of-two) Identifies the programmable electronic controller architecture. 1oo2 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 Logix5000-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.

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.

Probability of dangerous failure per hour (PFH) The average frequency of a dangerous failure per hour.

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 2 or 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 69 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 A value, which the firmware calculates, that uniquely represents the logic and configuration of the safety system. It is used to verify the integrity of the safety application program during downloads to the controller.

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.

SIL claim limit (SILCL) Maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity. (from IEC 62061)

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 a 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.

Notes:

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Rockwell Automation Support

Use the following resources to access support information.

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

Documentation Feedback

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

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

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

Publication 1756-RM012B-EN-P - April 2018
Supersedes Publication 1756-RM012A-EN-P – February 2018