GuardLogix 5570 and Compact GuardLogix 5370

Catalog Numbers 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS, 1756-L73EROMS, 1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMSK, 1769-L36ERMS, 1769-L33ERMOS, 1769-L36ERMOS, 1769-L37ERMOS, 1769-L37ERMS, 1769-L37ERMSK, 1769-L38ERMOS, 1769-L38ERMS, 1769-L38ERMSK

Allen-Bradley
by ROCKWELL AUTOMATION

Reference Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this presentation are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Table of Contents

Preface

About This Publication . . . 7
Summary of Changes . . . 7
Terminology . . . 7
Additional Resources . . . 8

Chapter 1

Safety Integrity Level (SIL) Concept

SIL 3 Certification . . . 9
Proof Tests . . . 9
GuardLogix Architecture for SIL 3 Applications . . . 10
GuardLogix System Components . . . 11
GuardLogix Certifications . . . 12
GuardLogix PFD and PFH Specifications . . . 13
Safety Integrity Level (SIL) Compliance Distribution and Weight . . . 14
System Reaction Time . . . 14
- Safety Task Reaction Time . . . 14
- Safety Task Period and Safety Task Watchdog . . . 14

Contact Information If Device Failure Occurs . . . 14

Chapter 2

GuardLogix Controller System

GuardLogix 5570 Controller Hardware . . . 15
- Primary Controller . . . 15
- Safety Partner . . . 15
- Chassis . . . 16
- Power Supplies . . . 16

Compact GuardLogix 5370 Hardware . . . 17
CIP Safety Protocol . . . 18
Safety I/O Devices . . . 18
Communication Bridges for GuardLogix 5570 Controllers . . . 19
- EtherNet/IP Network . . . 19
- DeviceNet Safety Network . . . 20
- ControlNet Network . . . 20

Programming Overview . . . 20

Chapter 3

CIP Safety I/O for the GuardLogix Control System

Overview . . . 21
Typical Safety Functions of CIP Safety I/O Devices . . . 21
- Diagnostics . . . 21
- Status Data . . . 21
- Status Indicators . . . 21
- On- or Off-delay Function . . . 21

Reaction Time . . . 22
Safety Considerations for CIP Safety I/O Devices . . . 22
- Ownership . . . 22
- Safety I/O Configuration Signature . . . 22

Safety I/O Device Replacement 23

Chapter 4

CIP Safety and the Safety Network Number

Routable CIP Safety Control System 25
Unique Node Reference 25
Safety Network Number 26
Considerations for Assigning the Safety Network Number (SNN). 28
Safety Network Number (SNN) for Safety Consumed Tags 28
Safety Network Number (SNN) for Out-of-box Devices 28
Safety Network Number (SNN) for Safety Device with a Different Configuration Owner 28
Safety Network Number (SNN) When Copying a Safety Project 28

Chapter 5

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

Differentiate between Standard and Safety 29
SIL 2 Safety Control in the Safety Task 29
SIL 2 Safety Logic 30
SIL 2 Safety Inputs 31
SIL 1 or SIL 2 Safety Control in Standard Tasks (only for GuardLogix 5570 Controllers) . 33
SIL 3 Safety–the Safety Task 33
Safety Task Limitations 33
Safety Task Execution Details 34
Use of Human Machine Interfaces 35
Precautions 35
Access to Safety-related Systems 35
Safety Programs 36
Safety Routines 36
Safety Tags 37
Standard Tags in Safety Routines (tag mapping) 38

Chapter 6

Safety Application Development

Safety Concept Assumptions 39
Basics of Application Development and Testing 40
Commissioning Lifecycle 40
Specification of the Control Function 41
Create the Project 41
Test the Application Program 42
Generate the Safety Task Signature 42
Project Verification Test 42
Confirm the Project 43
Safety Validation 43
Lock the GuardLogix Controller 44
Downloading the Safety Application Program 44
Uploading the Safety Application Program 45
Online Editing 45
Storing and Loading a Project from Nonvolatile Memory 45
Force Data 45

Inhibit a Device 46
Editing Your Safety Application 46
Performing Offline Edits 46
Performing Online Edits 47
Modification Impact Test 47

Chapter 7

Monitor Status and Handle Faults

Monitoring System Status 49
CONNECTION_STATUS Data 49
Input and Output Diagnostics 50
I/O Device Connection Status 50
De-energize to Trip System 50
Get System Value (GSV) and Set System Value (SSV) Instructions 50
GuardLogix System Faults 51
Nonrecoverable Controller Faults 51
Nonrecoverable Safety Faults 51
Recoverable Faults 51

Appendix A

Safety Instructions

. 53

Appendix B

Safety Add-On Instructions

Create and Use a Safety Add-On Instruction 58
Create Add-On Instruction Test Project 60
Create a Safety Add-On Instruction 60
Generate Instruction Signature 60
Download and Generate Safety Instruction Signature 60
SIL 3 Add-On Instruction Qualification Test 61
Confirm the Project 61
Safety Validate Add-On Instructions 61
Create Signature History Entry 61
Export and Import the Safety Add-On Instruction 61
Verify Safety Add-On Instruction Signatures 61
Test the Application Program 62
Project Verification Test 62
Safety Validate Project 62
Additional Resources 62

Appendix C

Reaction Times

System Reaction Time 65
Logix System Reaction Time 65
Simple Input-logic-output Chain 65
Logic Chain Using Produced/Consumed Safety Tags 66
Factors That Affect Logix Reaction-time Components 67
Access Guard I/O Input Module Delay Time Settings 68
Access Input and Output Safety Connection Reaction Time Limit 68
Configure the Safety Task Period and Watchdog 69

Access Produced/Consumed Tag Data 70

Checklists for GuardLogix Safety Applications

Appendix D
Checklist for GuardLogix Controller System 72
Checklist for Safety Inputs 73
Checklist for Safety Outputs 73
Checklist to Develop a Safety Application Program 74

GuardLogix Systems Safety Data

Appendix E
PFD Values 75
PFH Values 75

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

Appendix F
De-energize to Trip System 77
Use Connection Status Data to Initiate a Fault Programmatically 77

Use of 1794 FLEX I/O Modules and 1756 SIL 2 Inputs and Outputs with GuardLogix 5570 Controllers to Comply with EN 50156

Appendix G
SIL 2 Dual Channel Inputs (standard side of GuardLogix 5570 controllers) 83
SIL 2 Outputs With SIL 3 Guard I/O Output Modules 84
SIL 2 Outputs With 1756 or 1794 SIL 2 Output Modules 84
Safety Functions Within the GuardLogix 5570 Safety Task 85

Glossary 87

Index 91

About This Publication

This manual describes the GuardLogix® 5570 and Compact GuardLogix 5370 controller systems, which are type-approved and certified for use in safety applications as detailed in SIL 3 Certification on page 9.

Use this manual if you are responsible for the development, operation, or maintenance of a GuardLogix 5570 or Compact GuardLogix 5370 controller-based safety system that uses the Studio 5000 Logix Designer® application. You must read and understand the safety concepts and the requirements that are presented in this manual before operating a GuardLogix 5570 or Compact GuardLogix 5370 controller-based safety system.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this presentation are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Summary of Changes

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

Topic	Page
Updated the PFD Values and PFH Values for 1756-L7xS, 1756-L7SP, 1756-L72EROMS, 1756-L73EROMS, 1756-L73SXT, and 1756-L7SPXT controllers	75

Terminology

In this publication, the term 'GuardLogix controller' or 'GuardLogix system' applies to both GuardLogix 5570 and Compact GuardLogix 5370 controllers unless otherwise noted.

Abbreviation	Full Term	Definition
1oo2	One out of Two	Identifies the programmable electronic controller architecture.
CIP™	Common Industrial Protocol	An industrial communication protocol that is used by Logix 5000®-based automation systems on EtherNet/IP™, ControlNet®, and DeviceNet® communication networks.
CIP Safety™	Common Industrial Protocol – Safety Certified	SIL 3 -rated version of CIP™.
CL	Claim Limit	The maximum safety integrity level (SIL) that can be achieved.
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
EN	European Norm.	The official European Standard.
GSV	Get System Value	A ladder logic instruction that retrieves specified controller status information and places it in a destination tag.
PC	Personal computer	Computer that is used to interface with and control a Logix-based system via the Studio 5000® environment.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating.
SIL	Safety Integrity Level	A relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction.
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	A ladder logic instruction that sets controller system data.
--	Standard	Any object, task, tag, program, or component in your project that is not a safety-related item (that is, standard controller refers generically to a ControlLogix® or CompactLogix® controller).

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation. You can view or download publications at rok.auto/literature.

Resource	Description
ControlLogix Controllers Technical Data, publication 1756-TD001	Lists product specifications and certifications for GuardLogix 5570 controllers.
CompactLogix Controllers Technical Data, publication 1769-TD005	Lists product specifications and certifications for Compact GuardLogix 5370 controllers.
GuardLogix 5570 Controllers User Manual, publication 1756-UM022	Provides information on how to install, configure, program, and use GuardLogix 5570 controllers in Studio 5000 Logix Designer projects.
Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022	Provides information on how to install, configure, program, and use Compact GuardLogix 5370 controllers.
Armor GuardLogix Controllers Installation Instructions, publication 1756-IN060	Provides information on how to install, mount, and connect Armor™ GuardLogix® controllers to a network.
Armor Compact GuardLogix Controllers Installation Instructions, publication 1769-IN022	Provides information on how to install, mount, and connect Armor™ Compact GuardLogix controllers to a network.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety Application instruction set.
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.
Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001	Describes requirements for using ControlLogix controllers, and GuardLogix standard task, in SIL 2 safety control applications.
Logix Controllers Instructions Reference Manual, publication 1756-RM009	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.
ControlLogix System User Manual, publication 1756-UM001	Provides information on how to use ControlLogix controllers in non-safety 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 estimating the execution time and memory use for instructions.
Logix Import Export Reference Manual, publication 1756-RM084	Provides information on how to use the Logix Designer application 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, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

Safety Integrity Level (SIL) Concept

SIL 3 Certification

GuardLogix® 5570 and Compact GuardLogix 5370 controller systems are:

- Type-approved and certified for use in safety applications up to and including SIL 3 per IEC 61508
- Suitable for use in safety applications up to and including SIL CL3 per IEC 62061
- Suitable for use in safety applications up to and including Performance Level PLe (Category 4) per ISO 13849-1

SIL requirements are based on the standards current at the time of certification. In addition, the standard tasks within GuardLogix 5570 controllers can be used either for standard applications or SIL 2 safety applications as described in the Using ControlLogix® in SIL 2 Applications Reference Manual, publication 1756-RM001. In either case, do not use SIL 2 or standard tasks and variables to build up safety loops of a higher level. The safety task is the only task that is certified for SIL 3 applications. The standard task in a Compact GuardLogix 5370 controller cannot be used for SIL 2 safety applications.

Use the Studio 5000 Logix Designer® application to create programs for GuardLogix 5570 and Compact GuardLogix 5370 controllers.

The TÜV Rheinland has approved GuardLogix 5570 and Compact GuardLogix 5370 controller systems for use in safety-related applications up to SIL CL 3, in which the de-energized state is considered to be the safe state. All examples that are related to I/O included 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 the following: • 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: GuardLogix 5570 Controllers User Manual, publication 1756-UM022 or Compact GuardLogix Controllers User Manual, publication 1769-UM022

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

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 test intervals can be once a year, once every 15 years, or whatever time frame is appropriate.

GuardLogix 5570 and Compact GuardLogix 5370 controllers have a proof test interval of up to 20 years. Other components of the system, such as safety I/O devices, sensors, and actuators can have shorter proof test intervals. Include the controller in the functional verification tests of the other components in the safety system.

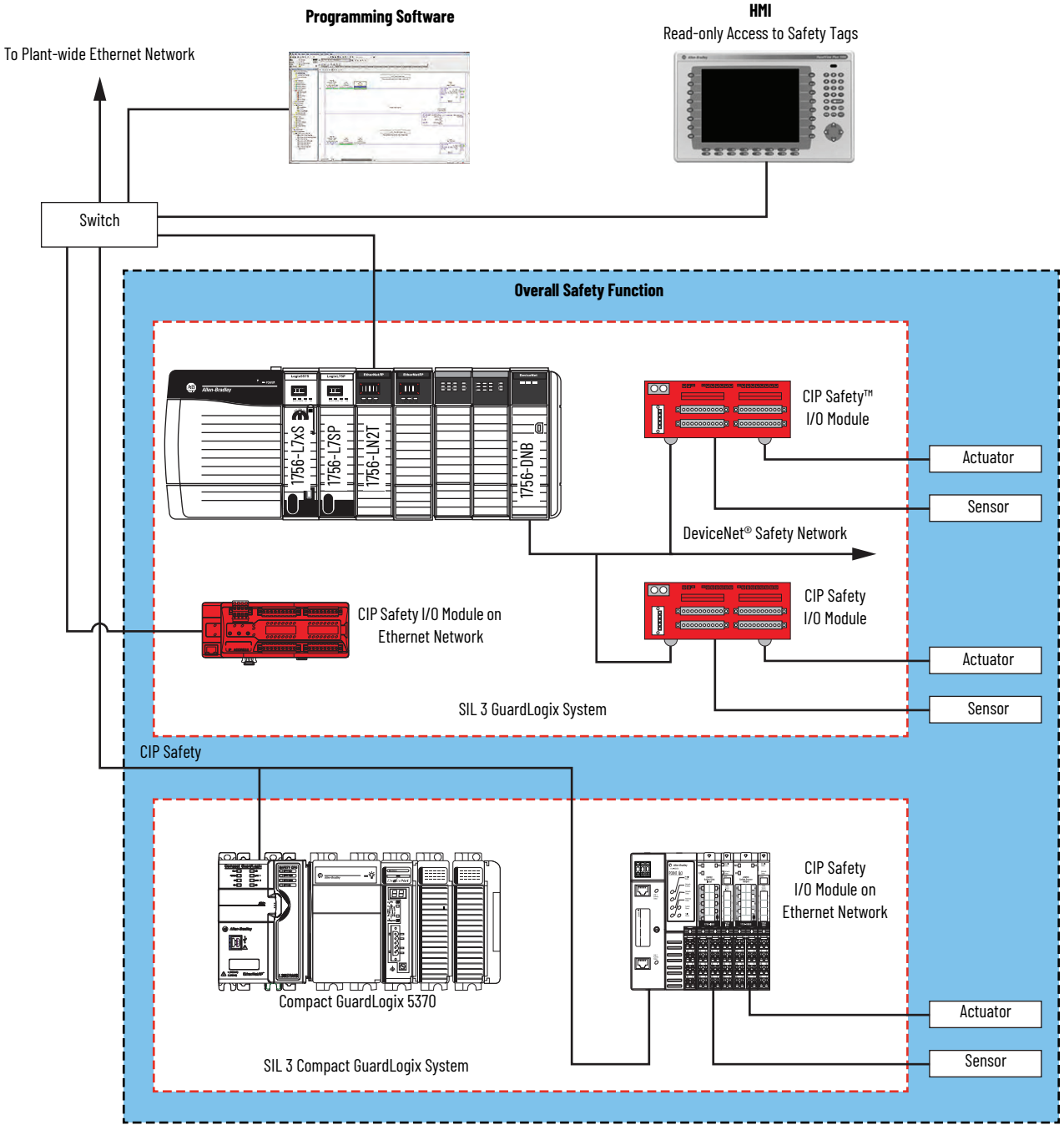
IMPORTANT	Your specific application determines the time frame for the proof test interval. It mainly pertains to safety I/O devices and field instrumentation.

GuardLogix Architecture for SIL 3 Applications

This figure shows a typical SIL function, including the following:

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

Figure 1 - Typical SIL Function



GuardLogix System Components

The tables in this section list non-SIL 3-certified components that can be used with SIL 3 GuardLogix systems. For the most current list of GuardLogix controller and CIP Safety I/O devices certified series and firmware revisions, see the safety certificates at rok.auto/certifications.

Firmware revisions are available from the Rockwell Automation® Product Compatibility and Download Center (PCDC) support website at rok.auto/pcdc.

Table 1 - Components Suitable for Use with 1756 GuardLogix Controller Safety Systems

Device Type	Cat. No.	Description	Series(2)	Revision(2)	Related Documentation(3)	
					Installation Instructions	User Manual
Chassis	1756-A4 1756-A7 1756-A10 1756-A13 1756-A17	4-slot chassis 7-slot chassis 10-slot chassis 13-slot chassis 17-slot chassis	B	N/A	1756-IN621	N/A
	1756-A4LXT 1756-A5XT 1756-A7XT 1756-A7LXT 1756-A10XT	4-slot XT chassis 5-slot XT chassis 7-slot XT chassis 7-slot XT chassis 10-slot XT chassis	B	N/A		
Power supply	1756-PA72	Power supply, AC	C	N/A	1756-IN619	N/A
	1756-PB72(1)	Power supply, DC	C			
	1756-PA75	Power supply, AC	B			
	1756-PB75	Power supply, DC	B			
	1756-PAXT	XT power supply, AC	B			
	1756-PBXT	XT power supply, DC	B			
Communication modules	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	EtherNet/IP bridge	A A A C B	3.006 2.005 2.005 10.007 10.007	ENET-IN002	ENET-UM001
	1756-EN2TXT 1756-EN2TRXT	XT EtherNet/IP™ bridge (copper)	C C	5.007 10.006		
	1734-AENT	POINT I/O™ Ethernet adapter	B	5.012	1734-IN590	1734-UM011
	1734-AENTR	POINT I/O Two Port Ethernet Adapter	B	5.012	1734-IN040	
	1756-DNB	DeviceNet bridge	A	6.002	DNET-IN001	DNET-UM004
	1756-CN2	ControlNet® bridge	A	12.001	CNET-IN005	CNET-UM001
	1756-CN2R	ControlNet bridge, redundant media	A	12.001		
	1756-CN2RXT	XT ControlNet bridge, redundant media	B	20.020		
Programming software	9324-*xxxx*	Studio 5000® environment for GuardLogix 5570 controllers	N/A	21.00.00	N/A	Consult online help.
Memory cards	1784-CF128	128 MB CompactFlash Card for GuardLogix 5560 controllers	N/A	N/A	N/A	N/A
	1784-SD1	1 GB Secure Digital (SD) Card for GuardLogix 5570 controllers				
	1784-SD2	2 GB Secure Digital (SD) Card for GuardLogix 5570 controllers				

(1) An Armor™ GuardLogix® controller system has this power supply inside its IP67-rated housing.
(2) This version or later.
(3) These publications are available from Rockwell Automation at rok.auto/literature.

You can fill slots of a SIL 3 system chassis unused by the GuardLogix SIL 3 system with other ControlLogix (1756) modules that are certified to the Low Voltage and EMC Directives.

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

Table 2 - Components Suitable for Use with Compact GuardLogix 5370 Safety Systems

Device Type	Cat. No.	Description	Series(2)	Revision(2)	Related Documentation(3)	
					Installation Instructions	User Manual
Power supply	1769-PA2	Power supply, AC	A	N/A	1769-IN028	N/A
	1769-PB2(1)	Power supply, DC	A			
	1769-PA4	Power supply, AC	A			
	1769-PB4	Power supply, DC	A			
Communication modules	1734-AENT	POINT I/O Ethernet Adapter	B	5.012	1734-IN590	1734-UM014
	1734-AENTR	POINT I/O Two Port Ethernet Adapter	B	5.012	1734-IN040	
Programming software	9324-*xxxx*	Studio 5000® environment	N/A	28.00.00	N/A	Consult online help.
Memory cards	1784-SD1	1 GB Secure Digital (SD) Card	N/A			
	1784-SD2	2 GB Secure Digital (SD) Card				

(1) An Armor™ Compact GuardLogix controller system has this power supply inside its IP67-rated housing.
(2) This version or later.
(3) These publications are available from Rockwell Automation at rok.auto/literature.

Expansion slots of a SIL 3 system bus that are not used by the Compact GuardLogix 5370 SIL 3 system can be populated with 1769 Compact I/O™ expansion modules that are certified to the Low Voltage and EMC Directives.

GuardLogix Certifications

These publications list the product specifications and the agency certifications for which the products are approved:

- ControlLogix Controllers Technical Data, publication 1756-TD001
- CompactLogix™ Controllers Technical Data, publication 1769-TD005

If a product has achieved agency certification, it is marked as such on the product labeling.

See the Product Certifications website, rok.auto/certifications for Declarations of Conformity, Certificates, and other certification details.

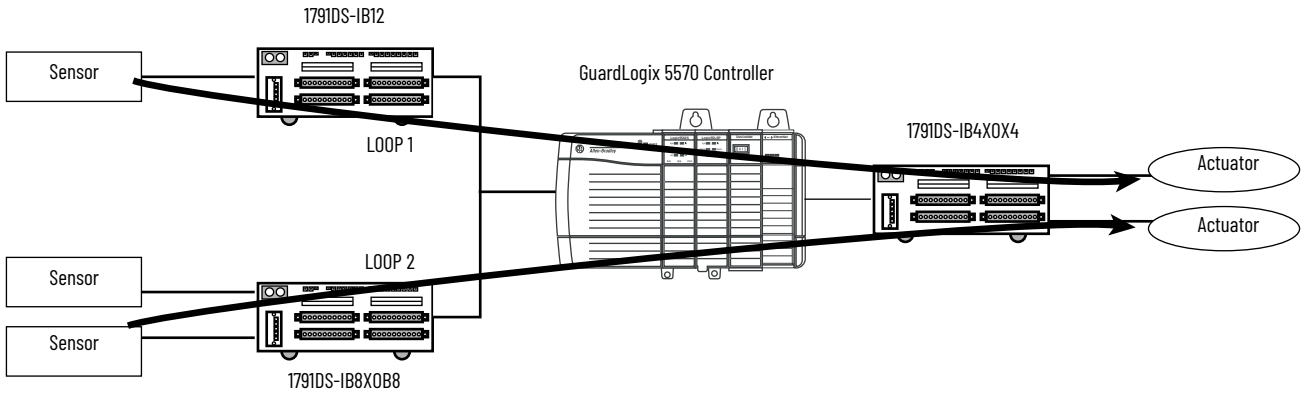
GuardLogix PFD and PFH Specifications

Safety-related systems can be classified as operating in either a Low Demand mode, or in a High Demand/Continuous mode. IEC 61508 quantifies this classification by stating that the frequency of demands for operation of the safety system is no greater than once per year in the Low Demand mode, or greater than once per year in High Demand/Continuous mode.

The Safety Integrity Level (SIL) value for a Low Demand safety-related system is directly related to order-of-magnitude ranges of its average probability of failure to satisfactorily perform its safety function on demand or, simply, probability of failure on demand (PFD). The SIL value for a High Demand/Continuous mode safety-related system is directly related to the probability of a dangerous failure occurring per hour (PFH).

PFD and PFH values are associated with each of the three primary elements that constitute a safety-related system (the sensors, the logic element, and the actuators). Within the logic element, you also have input, processor, and output elements.

Figure 2 - PFH Example



To determine the logic element PFH for each safety loop in the simple example system that is shown in the PFH Example, sum the PFH values for each component in the loop. This table provides a simplified example of PFH value calculations for each safety loop that is shown in Figure 2.

Table 3 - PFH Equations by Safety Loop

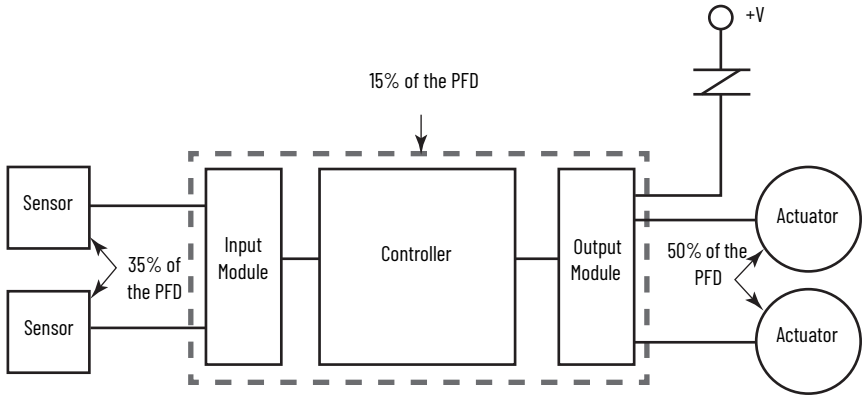
For This Loop	Sum the PFH Values of These Components
Total PFH for loop 1 =	Sensor PFH + 1791DS-IB12 + GuardLogix controller + 1791DS-IB4XOX4 + Actuator PFH
Total PFH for loop 2 =	Sensor PFH + 1791DS-IB8XOB8 + GuardLogix controller + 1791DS-IB4XOX4 + Actuator PFH

When you calculate PFH values, you must consider the specific requirements of your application, including proof test and diagnostic test intervals.

Safety Integrity Level (SIL) Compliance Distribution and Weight

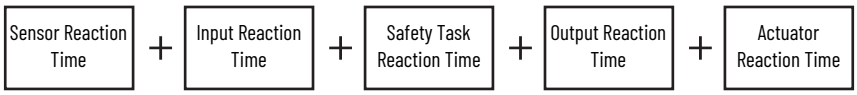
The GuardLogix controller and I/O system can conservatively be assumed to contribute 15% of the reliability burden. A SIL 3 system can incorporate multiple inputs for critical sensors and input devices, as well as dual outputs connected in series to dual actuators dependent on SIL assessments for the safety-related system.

Figure 3 - Reliability Burden



System Reaction Time

The system reaction time is the amount of time from a safety-related event as an input to the system until the system sets corresponding outputs to their safe state. Faults within the system can also affect the reaction time of the system. The system reaction time is the sum of the following reaction times.



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

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. It is less than or equal to the sum of the safety task period and the safety task watchdog.

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 safety-task processing time exceeds the safety-task watchdog time, a nonrecoverable safety fault occurs in the controller and outputs transition to the safe state (off) automatically.

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 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 task signature is created.

Contact Information If Device Failure Occurs

If you experience a failure with any SIL 3-certified device, contact your local Allen-Bradley distributor to initiate the following actions:

- You can return the device to Rockwell Automation so the failure is appropriately logged for the catalog number that is affected and a record is made of the failure.
- You can request a failure analysis (if necessary) to try to determine the cause of the failure.

GuardLogix Controller System

For a brief list of components suitable for use in Safety Integrity Level (SIL) 3 applications, see Table 1 on page 11. For more detailed and current information, see rok.auto/certifications.

See Additional Resources on page 8 to find additional installation information for the following controllers:

- GuardLogix® 5570
- Compact GuardLogix 5370
- Armor™ GuardLogix®
- Armor™ Compact GuardLogix

GuardLogix 5570 Controller Hardware

The GuardLogix controller consists of a primary controller (ControlLogix® 557xS) and a safety partner (ControlLogix 557SP). These two modules work in a 1oo2 architecture to create the SIL 3-capable controller. They are described in the following sections.

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

For details on status indicator operation, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

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.

For a list of GuardLogix safety controller catalog numbers, see Table 1 on page 11. For a list of standard ControlLogix components suitable for safety applications, see Table 2 on page 12.

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, a safety partner must be installed in the slot immediately to the right of the primary controller. The safety partner is a co-processor that provides redundancy 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 nonrecoverable controller fault. For information on how to respond to this situation, see article 63983 in the Rockwell Automation Knowledgebase.

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

Chassis

The chassis provides the physical connections between modules and the 1756 GuardLogix system. Any failure, though unlikely, is 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.

GuardLogix-XT™ controllers must use a ControlLogix-XT™ chassis to achieve the extreme environment rating.

Power Supplies

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

GuardLogix-XT controllers must use a ControlLogix-XT power supply to achieve the extreme environment rating.

Compact GuardLogix 5370 Hardware

Compact GuardLogix 5370 controllers (1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMSK, 1769-L36ERMS, 1769-L37ERMS, 1769-L37ERMSK, 1769-L38ERMS, 1769-L38ERMSK) combine the primary and safety partner controllers in a single controller hardware package to form a SIL 3 capable controller.

The Armor Compact GuardLogix controllers (1769-L33ERMOS, 1769-L36ERMOS, 1769-L37ERMOS, and 1769-L38ERMOS) combine a Compact GuardLogix controller with a power supply in an IP67-rated housing for mounting on a machine.

The controllers support this functionality:

- Two EtherNet/IP™ ports support CIP Safety™ protocol
- One USB port
- Support for 1769 Compact I/O™ local expansion modules (Compact GuardLogix 5370 controllers only)
- Control of distributed EtherNet/IP safety I/O modules
- Support for Integrated Motion on EtherNet/IP networks
- Use of 1784-SD1 or 1784-SD2 Secure Digital (SD) card for nonvolatile memory
- An internal energy storage solution instead of a battery

Cat. No.	Local Expansion Modules Supported, max	Number of Motion Axes
1769-L30ERMS	8	4
1769-L33ERMS 1769-I33ERMSK	16	8
1769-L33ERMOS	—	8
1769-L36ERMS	30	16
1769-L36ERMOS 1769-L37ERMOS(1)	—	16
1769-L37ERMS 1769-L37ERMSK	30	16
1769-L38ERMOS	—	16
1769-L38ERMS 1769-L38ERMSK	30	16

(1) Available at firmware revision 30.

The Compact GuardLogix 5370 controller is powered by one of these power supplies:

- 1769-PA2
- 1769-PB2
- 1769-PA4
- 1769-PB4

A 1769-ECx end cap is required to terminate the end of the last bank in the control system.

The Armor Compact GuardLogix controllers do not use an external power supply. A power supply is included inside the controller housing.

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.

For details on status indicator operation, refer to the Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022.

CIP Safety Protocol

Safety-related communication between GuardLogix controllers takes place via produced and consumed safety tags. These safety tags use the CIP Safety protocol, which is designed to preserve data integrity during communication.

Compact GuardLogix 5370 controllers support CIP Safety protocol only over EtherNet/IP networks.

For more information on safety tags, see Chapter 5, Characteristics of Safety Tags, the Safety Task, and Safety Programs.

Safety I/O Devices

For information on CIP Safety I/O devices for use with GuardLogix controllers, see Chapter 3.

Communication Bridges for GuardLogix 5570 Controllers

Table 4 lists the communication interface modules available in GuardLogix 5570 systems to facilitate communication over EtherNet/IP, DeviceNet®, and ControlNet® networks via the CIP Safety protocol.

Table 4 - Communication Interface Modules by System

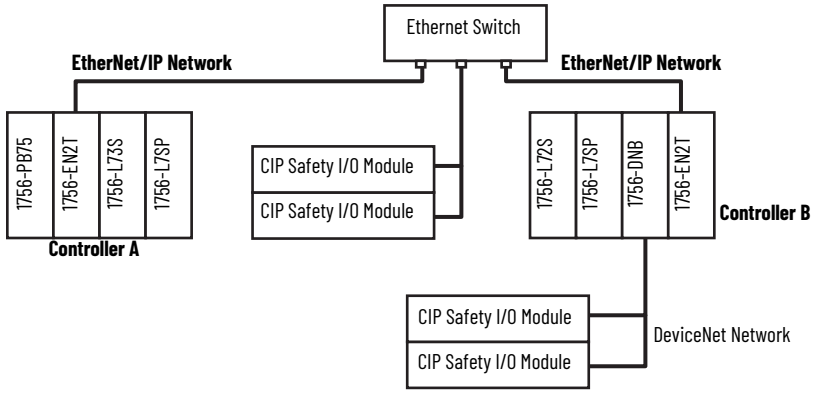
GuardLogix System	Communication Modules
1756	• 1756-ENBT, 1756-EN2T(R), 1756-EN2F, or 1756-EN3TR EtherNet/IP bridge • 1756-DNB DeviceNet bridge • 1756-CN2 ControlNet bridge • 1756-CN2R Redundant ControlNet bridge
1756 XT	• 1756-EN2TXT, 1756-EN2TRXT EtherNet/IP bridge XT (copper) • 1756-CN2RXT Redundant XT ControlNet bridge
1768	• 1768-CNB • 1768-CNBR

IMPORTANT Due to the design of the CIP Safety control system, CIP Safety bridge devices, like the bridges that are listed in Table 4, are not required to be SIL 3-certified.

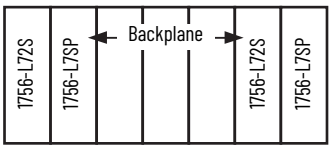
EtherNet/IP Network

Peer-to-peer safety communication between GuardLogix controllers is possible via the EtherNet/IP network by using EtherNet/IP bridges. An EtherNet/IP bridge lets the GuardLogix controller control and exchange safety data with CIP Safety I/O devices on an EtherNet/IP network.

Figure 4 - Peer-to-peer Communication via EtherNet/IP Bridges and the EtherNet/IP Network



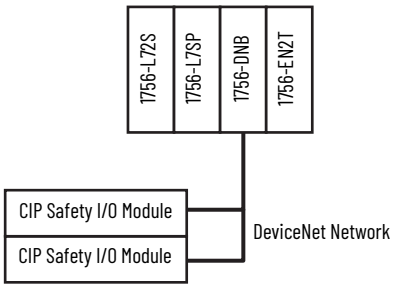
Peer-to-peer safety communication between two GuardLogix controllers in the same chassis is also possible via the backplane.



DeviceNet Safety Network

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

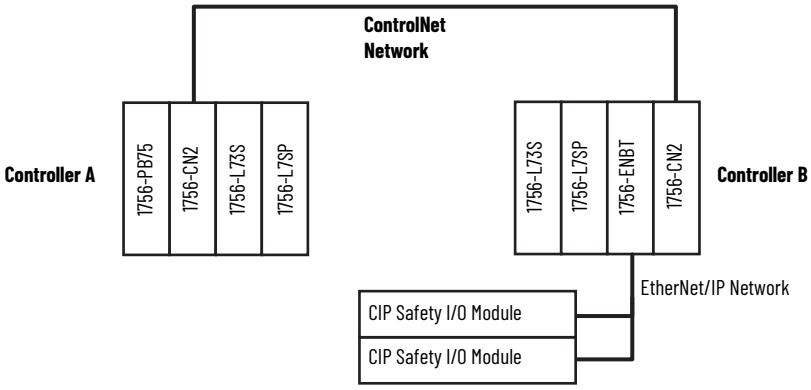
Figure 5 - Communication via a DeviceNet Bridge



ControlNet Network

ControlNet bridges let the GuardLogix controller produce and consume safety tags over ControlNet networks to other GuardLogix controllers or remote CIP Safety I/O networks.

Figure 6 - Communication via a ControlNet Bridge



Programming Overview

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

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

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

Authorized personnel can change a safety program, but only by using one of the processes that are described in Editing Your Safety Application on page 46.

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.

CIP Safety I/O for the GuardLogix Control System

Overview

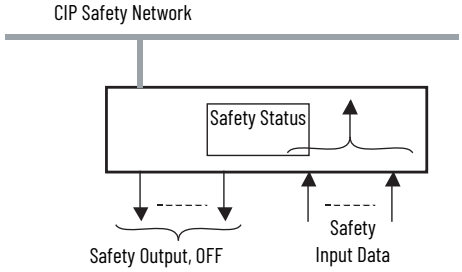
Before you operate a GuardLogix® safety system with CIP Safety I/O devices, you must first read, understand, and follow all safety information in the publications for those products.

CIP Safety I/O devices can be connected to safety input and output devices, like sensors and actuators, that let these devices be monitored and controlled by the GuardLogix controller. 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 CIP Safety I/O Devices

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

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



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

Diagnostics

CIP 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, CIP Safety I/O devices support status data to monitor device and I/O circuit health. See your device product documentation for specific capabilities.

Status Indicators

The CIP Safety I/O devices include status indicators. For details on status indicator operation, refer to the product documentation for your specific device.

On- or Off-delay Function

Some CIP 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 the pulse test from safety devices that affect the input logic level.

See Appendix C 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, refer to the product documentation for your specific CIP Safety I/O device.

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

Safety Considerations for CIP 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

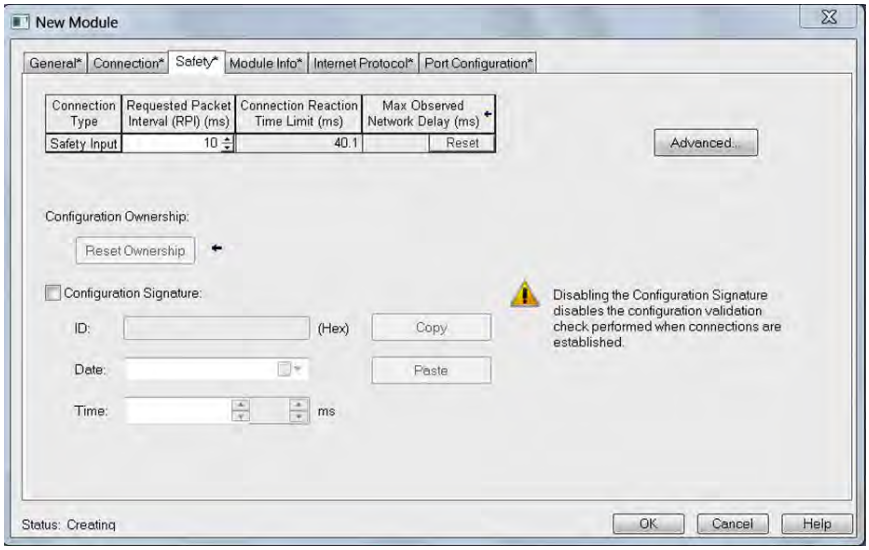
Each CIP Safety I/O device in a GuardLogix system is owned by one GuardLogix controller. Multiple GuardLogix controllers and multiple CIP Safety I/O devices can be used without restrictions in chassis or on networks as needed. When a controller owns an I/O device, it stores the device's configuration data, as defined by the user. This configuration controls how the devices operate in the system.

From a control standpoint, safety output devices can be controlled by only one controller. Each safety input device is also owned by a single controller; however, safety input data can be shared (consumed) by multiple GuardLogix controllers.

Safety I/O Configuration Signature

The configuration signature defines the device's configuration so it can be read and monitored. The configuration signature is used to uniquely identify a device's configuration. 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 CIP safety connection between the controller and I/O module is broken.

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.



Safety I/O Device Replacement

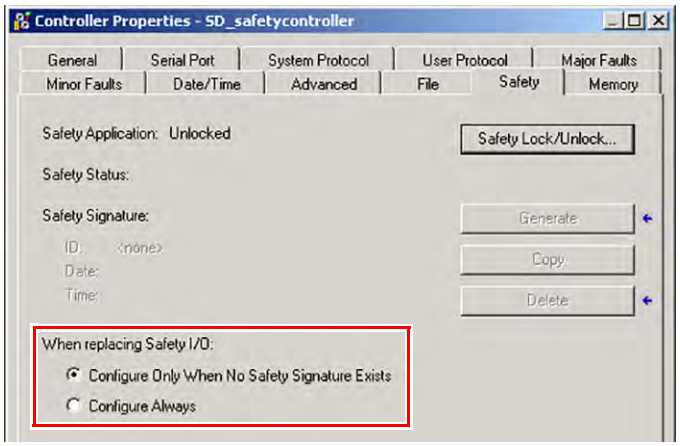
The replacement of safety devices requires that the replacement device be configured properly and that the replacement device's operation be user-verified.

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 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 automatically configure a safety device only when the safety task does not have a safety task signature, and the replacement device is in an out-of-box condition, meaning that a safety network number does not exist in the safety device.

If the safety task has a safety task signature, the GuardLogix controller only automatically configures the replacement CIP Safety I/O device if the following is 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 SNN when a safety signature exists, a manual action (typically SET) is required to download the proper SNN, after which the remainder of the configuration is automatically downloaded.

For detailed information, see the 'Replace a Safety I/O Device' procedure in the Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022 or GuardLogix 5570 Controllers User Manual, publication 1756-UM022.

Configure Always

The GuardLogix controller always attempts to automatically configure a replacement CIP Safety I/O device if the device is in an out-of-box condition, meaning that a safety network number does not exist in the replacement safety device, and the node number and I/O device keying matches the controller's configuration.

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

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

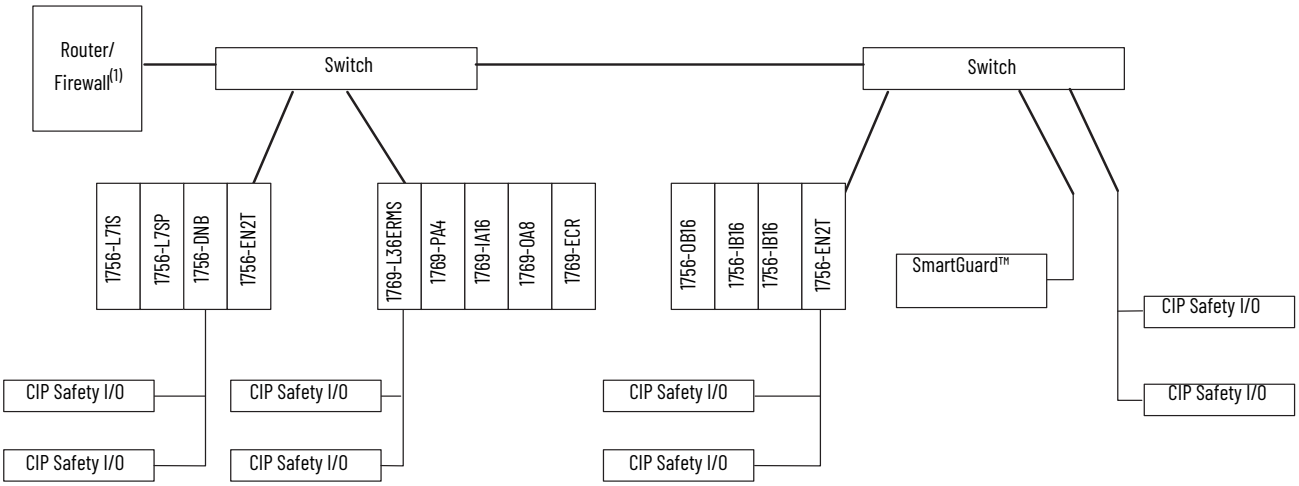
ATTENTION: Do not place any devices in the out-of-box condition on any CIP Safety network when the Configure Always feature is enabled, except while following the device replacement procedure in the GuardLogix 5570 Controllers User Manual, publication 1756-UM022 or Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022.

CIP Safety and the Safety Network Number

Routable CIP Safety Control System

To understand the safety requirements of a CIP Safety™ control system, including the safety network number (SNN), you must first understand how communication is routable in CIP™ control systems. The CIP Safety control system represents a set of interconnected CIP Safety devices. The routable system represents the extent of potential mis-routing of packets from an originator to a target within the CIP Safety control system. The system is isolated such that there are no other connections into the system. For example, the system in Figure 8 cannot be interconnected to another CIP Safety system through a larger, plant-wide Ethernet backbone. Therefore, the system in Figure 8 illustrates the extent of a routable CIP Safety system.

Figure 8 - CIP Safety System Example



(1) The router or firewall is configured to limit traffic.

Unique Node Reference

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

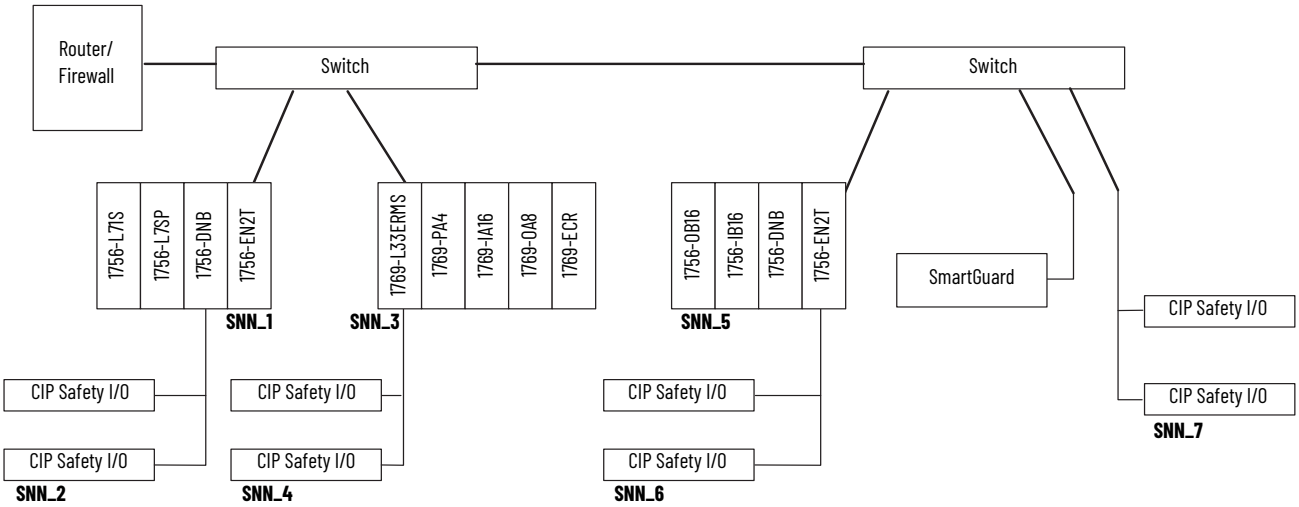
To help prevent errors in non-certified bridges, switches, or routers from becoming dangerous, each end node within a routable CIP Safety control system must have a unique node reference. The unique node reference is a combination of a safety network number (SNN) and the node address of the node.

Safety Network Number

The safety network number (SNN) is assigned automatically by the software or manually by you. Each CIP Safety network that contains safety I/O nodes must have at least one unique SNN. Each chassis that contains one or more safety devices must have at least one unique SNN. Safety network numbers that are assigned to each safety network or network subnet must be unique.

Multiple SNNs can be assigned to a CIP Safety subnet or a chassis that contains multiple safety devices.

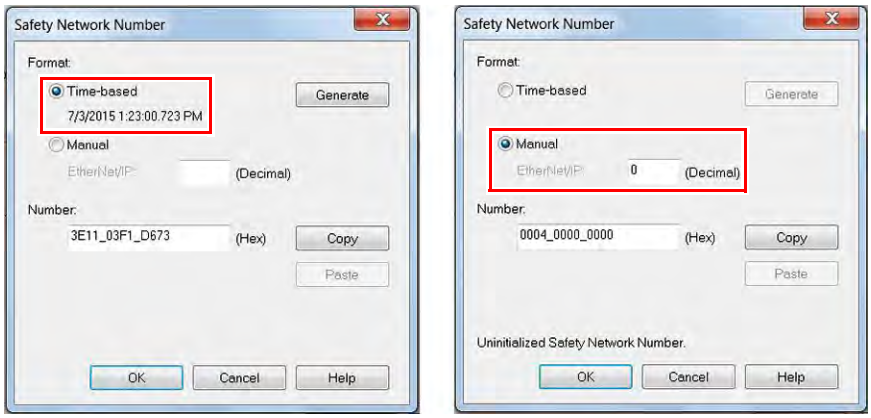
Figure 9 - CIP Safety Example with More Than One SNN



Each CIP Safety device must be configured with an SNN. Any device that originates a safety connection to another safety device must be configured with the SNN of the target device. If the CIP Safety system is in the start-up process before the functional safety testing of the system, the originating device can be used to set the unique node reference into the device.

The SNN used by the system is a 6-byte hexadecimal number. The SNN can be set and viewed in one of two formats: time-based or manual. When the time-based format is selected, the SNN represents a localized date and time. When the manual format is selected, the SNN represents a network type and must have a decimal value from 1...9999.

Figure 10 - SNN Formats



The assignment of a time-based SNN is automatic when you create a GuardLogix® safety controller project and add new CIP Safety I/O devices.

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

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

IMPORTANT	If you assign an SNN manually, make sure that system expansion does not result in duplication of SNN and node address combinations. A warning appears if your project contains duplicate SNN and node address combinations. You can still verify the project, but we recommend that you resolve the duplicate combinations.

Considerations for Assigning the Safety Network Number (SNN)

The assignment of the SNN is dependent upon factors, which include the configuration of the controller or CIP Safety I/O device.

Safety Network Number (SNN) for Safety Consumed Tags

When a safety controller that contains produced safety tags is added to the I/O Configuration tree, the SNN of the producing controller must be entered. The SNN can be copied from the producing controller's project and pasted into the new controller being added to the I/O Configuration tree.

See the following for information on how to copy and paste an SNN.

- GuardLogix® 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

Safety Network Number (SNN) 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 more information, see Safety I/O Device Replacement on page 23.

Safety Network Number (SNN) for Safety Device with a Different Configuration Owner

When a CIP Safety I/O device is owned by another GuardLogix controller (controller B), and then is added to another GuardLogix project (controller A project), the Logix Designer application assigns the SNN based on the current project. Because the current project (controller A project) is not the true configuration owner, you need to copy the original SNN (controller B project) into the configuration in controller A's project. This is easy to do with standard copy and paste commands. The result is that the CIP Safety I/O device produces data to two GuardLogix controllers simultaneously. You can do copy and paste for a maximum of 16 controllers.

See the following for information on how to change, copy, and paste safety network numbers.

- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

Safety Network Number (SNN) When Copying a Safety Project

ATTENTION: If a safety project is copied for use in another project with different hardware or in another physical location, and the new project is within the same routable CIP Safety system, every SNN must be changed in the second system. SNN values must not be repeated.
See the following for information on how to change the SNN.

- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

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

Differentiate between Standard and Safety

Because it is a Logix-series 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 controllers provide the same functionality as other controllers. What differentiates GuardLogix controllers from standard controllers is that they provide a 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. You can implement both SIL 2 and SIL 3 levels of safety control with the safety task of the GuardLogix controller.

SIL 2 Safety Control in the Safety Task

You can perform SIL 2 safety control by using the GuardLogix controller's safety task.

Because GuardLogix 5570 controllers are part of the ControlLogix® series of processors, you can perform SIL 2 safety control with a GuardLogix 5570 controller by using standard tasks or the safety task. This capability provides unique and versatile safety-control options, as most applications have a higher percentage of SIL 2 safety functions than SIL 3 safety functions.

IMPORTANT	Compact GuardLogix 5370 controllers do not support SIL 2 applications in the standard task. SIL 2 applications are supported only in the safety task of a Compact GuardLogix 5370 controller.

The GuardLogix safety task can be used to provide SIL 2 and SIL 3 safety functions. If SIL 3 safety functions must be performed simultaneously with SIL 2 safety functions, you must fulfill the requirements that are defined in the SIL 3 Safety-the Safety Task, Safety Programs, and Safety Routines sections of this chapter, as well as the SIL 2 requirements that are listed in this section.

SIL 2 Safety Logic

From a GuardLogix safety control perspective, the biggest difference between SIL 2 and SIL 3 safety-rated devices is that SIL 2 is generally single-channel, while SIL 3 is typically dual-channel. When you use Guard I/O™ safety-rated modules that are required in the safety task, SIL 2 safety inputs can be single channel, which can reduce complexity and the number of modules that are necessary.

It is up to the safety system designer to implement all safety functions properly. Consideration must be given to the following:

- Field device selection (properly select, identify, and mitigate all device faults)
- Consider safety demand requirements (low IEC 61511 or high ISO 13849)
- Consider test intervals (diagnostics and proof testing that is needed to satisfy application requirements)
- Identify and justify with proper documentation any fault exclusions that are used

IMPORTANT	If a combination of SIL 2 and SIL 3 safety functions are used simultaneously within the safety task, you must prevent SIL 2 input signals from directly controlling SIL 3 safety functions. Use specific safety-task programs or routines to separate SIL 2 and SIL 3 safety functions.

Within the safety task, the Logix Designer application includes a set of safety-related ladder-logic instructions. GuardLogix controllers also feature application-specific SIL 3-rated safety instructions. All of these logic instructions can be used in CAT. 1...4 and SIL 1...3 safety functions.

For SIL 2-only safety, a safety task signature is not required. However, if any SIL 3 safety functions are used within the safety task, a safety task signature is required.

For SIL 2 applications, we recommend that you safety-lock the safety task once testing is completed. Locking the safety task enables more security features. You can also use FactoryTalk® Security and Logix Designer routine source protection to limit access to safety-related logic.

For more information on how to generate a safety task signature and safety-locking the safety task, see the following.

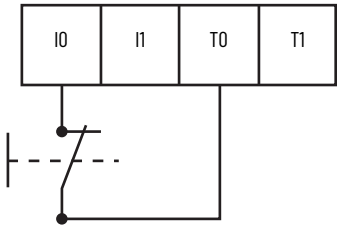
- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

SIL 2 Safety Inputs

CompactBlock™ Guard I/O™ (1791-series), ArmorBlock® Guard I/O™ (1732-series), and POINT Guard I/O™ (1734-series) safety input modules support single-channel SIL 2 safety input circuits. Because these modules are also rated for SIL 3 operation, mixing SIL 2 and SIL 3 circuits on the same module is allowed, provided you follow these guidelines.

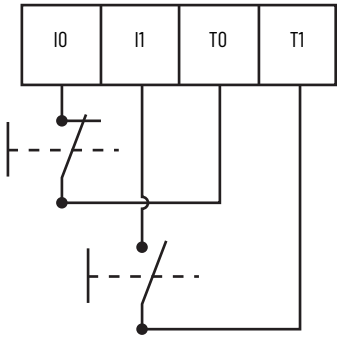
These two wiring examples show how to wire SIL 2 safety circuits to Guard I/O™ safety input modules. These examples use onboard test sources (TO...Tx) that are resident on all 1791 and 1732 safety input modules.

Figure 11 - Input Wiring



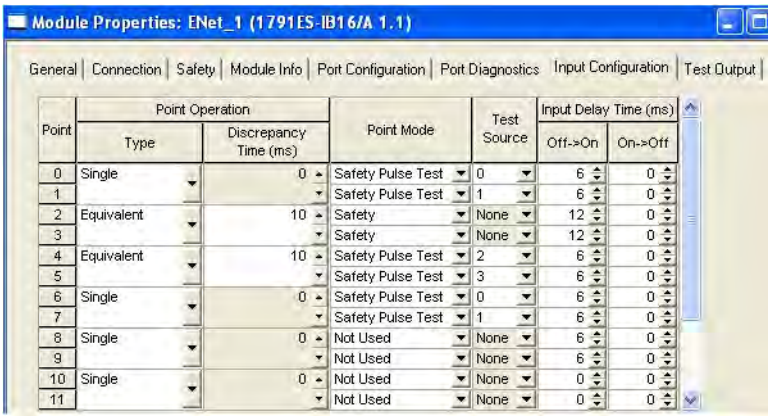
Guard I/O modules group inputs in pairs to facilitate Cat. 3, Cat. 4, and SIL 3 safety functions. For use in Cat. 1, Cat. 2, and SIL 2 safety functions, module inputs should still be used in pairs as illustrated. Two SIL 2 safety functions are shown wired to inputs I0 and I1 using test sources T0 and T1, respectively.

Figure 12 - Input Wiring in Pairs



For Cat. 1, Cat. 2, and SIL 2 safety functions, the Guard I/O safety modules need specific configurations within the GuardLogix project. In this example, inputs 0, 1, 6, 7, 8, 9, 10, and 11 are part of a Cat. 1, 2 or SIL 2 safety function because they are configured as SINGLE. Inputs 2, 3, 4, and 5 are part of a Cat. 3, Cat. 4, or SIL 3 safety function because they are configured as EQUIVALENT.

Figure 13 - Input Configuration



Field	Value
Type	Single
Discrepancy Time	N/A
Point Mode	Safety Pulse Test
Test Source	Set values based on how the field device is physically wired to the module. To make sure the test source is properly enabled, open and view settings on the Test Output tab.
Input Delay Time	User input based on field device characteristics.

IMPORTANT The onboard pulse test outputs (TO...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.

IMPORTANT If you use GuardLogix Safety Application Instructions to detect discrepancy faults of dual channel devices, be sure to configure your safety input modules as single, not equivalent or complementary. If configured for equivalent or complementary, discrepancy faults at the safety instruction are masked by the input module.

These instructions provide all dual-channel functionality necessary for PLd (Cat. 3) or PLe (Cat. 4) safety functions. Either the instruction or the module can provide the discrepancy checking typically required for SIL 3 safety functions.

See the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095.

SIL 1 or SIL 2 Safety Control in Standard Tasks (only for GuardLogix 5570 Controllers)

Because of the quality and number of diagnostics that are built into the ControlLogix® series of controllers, you can perform SIL 1 or SIL 2 safety functions from within standard tasks. This is also true for GuardLogix 5570 controllers.

To perform SIL 1 or SIL 2 safety control within a GuardLogix 5570 controller standard task, you must abide by requirements that are defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

SIL 3 Safety–the Safety Task

Creation of a GuardLogix project automatically creates a single 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 a single safety task.
- Within the safety task, you can use multiple safety programs that are composed of multiple safety routines.
- You cannot schedule or execute standard routines from within the safety task.

The safety task is a periodic, timed task with a user-selectable task priority and watchdog. In most cases, it is the controller's top priority and the user-defined program watchdog must be set to accommodate fluctuations in the execution of the safety task.

Safety Task Limitations

You specify both the safety task period and the safety task watchdog. The safety task period is the period at which the safety task executes. 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, page 65.

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 is triggered while it is still executing from the previous trigger.

For more information, see Chapter 7, Monitor Status and Handle Faults.

Safety Task Execution Details

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

- For GuardLogix 5570 controllers, the safety task does not begin to execute until the primary controller and safety partner have established their control partnership and the coordinated system time (CST) is synchronized. However, standard tasks begin to execute as soon as the controller transitions to Run mode. The free running clock (FRC) is the source of the diagnostic clock.

  For Compact GuardLogix 5370 controllers, the safety partner performs time polling with the primary controller to establish safety synchronized time (SST). SST status on the partner must be synchronized before partnership begins to form. Only when partnership is formed does the safety task begin to execute.
- Although the configurable range of the requested packet interval (RPI) for safety inputs and safety-consumed tags is 6...500 ms, safety input tags and safety-consumed tags are updated only at the beginning of safety task execution. This means that even though the I/O RPI can be faster than the safety task period, the data does not change during safety task execution. The data is read only once at the beginning of the safety task execution.
- Safety input values are frozen at the start of safety task execution. As a result, timer-related instructions, such as TON and TOF, are not updated during a single 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, but is similar to PLC or SLC™ behavior.

- For standard tags that are mapped to safety tags, the standard tag values are copied into safety memory at the start of the safety task and do not change during safety task execution.
- Safety output tag (output and produced) values are updated at the conclusion of safety task execution.
- The safety task responds to mode changes (for example, Run to Program or Program to Run) at timed intervals. As a result, the safety task can take multiple task periods, but always less than two, to make a mode transition.

IMPORTANT	While safety-unlocked and without a safety task 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, add 2 ms to the safety watchdog time. When the controller is safety-locked or a safety task signature exists, the situation that is described in this note cannot occur.

IMPORTANT	The safety task signature is required to operate in a SIL 3 safety function.

Use of Human Machine Interfaces

Follow these precautions and guidelines for using Human Machine Interfaces (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 Figure 1 on page 10.

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

Access to Safety-related Systems

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

Reading 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.

Changing 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 who 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 variable must be sent twice to two different tags; that is, both values must not be written to with one command.
  b. Safety-related code that executes in the controller, must check both tags for equivalency and make sure they are within range (boundary checks).
  c. Both new variables must be read back and displayed on the HMI device.
  d. Trained operators must visually check that both variables are the same and are the correct value.
  e. 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 validation procedure.

- Sufficiently document all safety-related changes that are made via the HMI, including the following:
  - Authorization
  - Impact analysis
  - Execution
  - Test information
  - Revision information
- Changes to the safety-related system must comply with IEC 61511 standard on process safety, section 11.7.1 Operator Interface requirements.
- Changes to the safety-related system must comply with IEC 62061 for machine safety.
- The developer must follow the same sound development techniques and procedures that are used for other application software development, including the verification and testing 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 must be secured and maintained for SIL-level compliance after the system has been validated and tested.

Safety Programs

A safety program has all of 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 all of the attributes of standard routines, except that they can exist only in safety programs. One safety routine can be designated as the main routine. Another safety routine can be designated as the fault routine. Only safety-certified instructions are used in safety routines.

For a listing of safety instructions, see Appendix A.

ATTENTION: To preserve SIL 3, you must verify that your safety logic does not attempt to read or write standard tags.

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 all of the attributes of standard tags with the addition of mechanisms to provide SIL 3 data integrity.

Valid Data Types for Safety Tags

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

The 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. Controller-scoped safety tags can be read by either standard or safety logic or other communication devices, but can be written by only safety logic or another GuardLogix safety controller. Program-scoped safety tags are accessible only by local safety routines. These are routines that reside within the safety program.

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

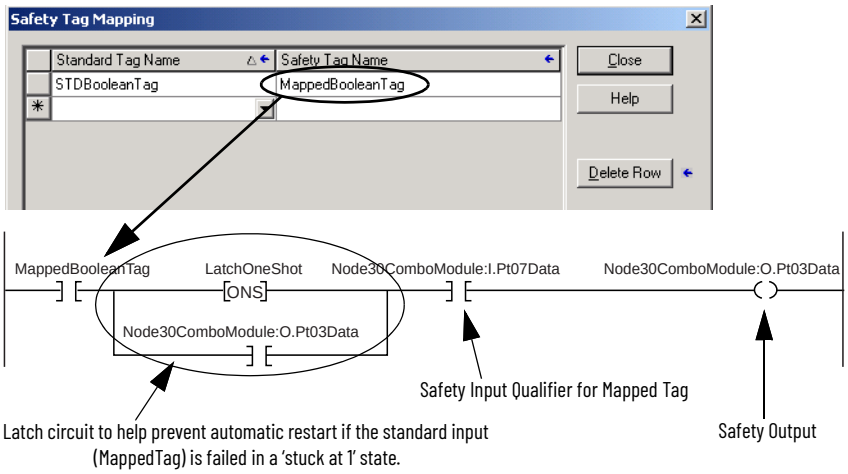
IMPORTANT	Any controller-scoped safety tag is readable by any standard routine, but the update rate is based on the execution of the safety task. Thus, safety tags are updated at the safety task periodic rate, which differs from standard tag behavior.

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 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 14 - Qualify Standard Data with Safety Data



Safety Application Development

Safety Concept Assumptions

The safety concept assumes the following:

- If you are responsible for creating, operating, and maintaining 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. Programming errors can be detected by strict adherence to specifications, programming and naming rules.
- You perform a critical analysis of the application and use all possible measures to detect a failure.
- You confirm all application downloads via a manual check of the safety task signature.
- You perform a complete functional test of the entire system before the operational startup of a safety-related system.

Table 5 - Controller Modes

Controller Mode	Safety Task Status	Safety[1] (up to and including)	Comments (A valid program has been downloaded to the controller.)
Program	Unlocked No signature		• I/O connections established. • Safety Task logic is not being scanned.
Run	Unlocked No signature	(Only for development purposes)	• Forcing allowed. • Online editing allowed. • Safety memory is isolated, but is unprotected (read/write). • Safety Task logic is being scanned. Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.
Run	Locked No signature	PLd/Cat. 3 Control reliable SIL CL2	• Safety I/O forces are not allowed. (They must be removed to safety lock the controller.) • Online editing is not allowed. • Safety memory is protected (read-only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs.
Run	Unlocked With signature	Ple/Cat. 4 Control reliable SIL CL3	• Safety I/O forces are not allowed. (They must be removed to generate a safety task signature.) • Online editing is not allowed. • Safety memory is protected (read-only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs. • Safety task signature is unprotected and can be deleted by anyone who has access to the controller.
Run	Locked With signature	Ple/Cat. 4 Control reliable SIL CL3	• Safety I/O forces are not allowed. (They must be removed to generate a safety task signature.) • Online editing is not allowed. • Safety memory is protected (read-only). • Safety task logic is scanned. • Primary and partner controllers process logic, cross-compare logic outputs. Logic outputs are written to safety outputs. • Safety task signature is protected. Users must enter the unlock password to unlock the controller before they can delete the safety task signature.

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

Basics of Application Development and Testing

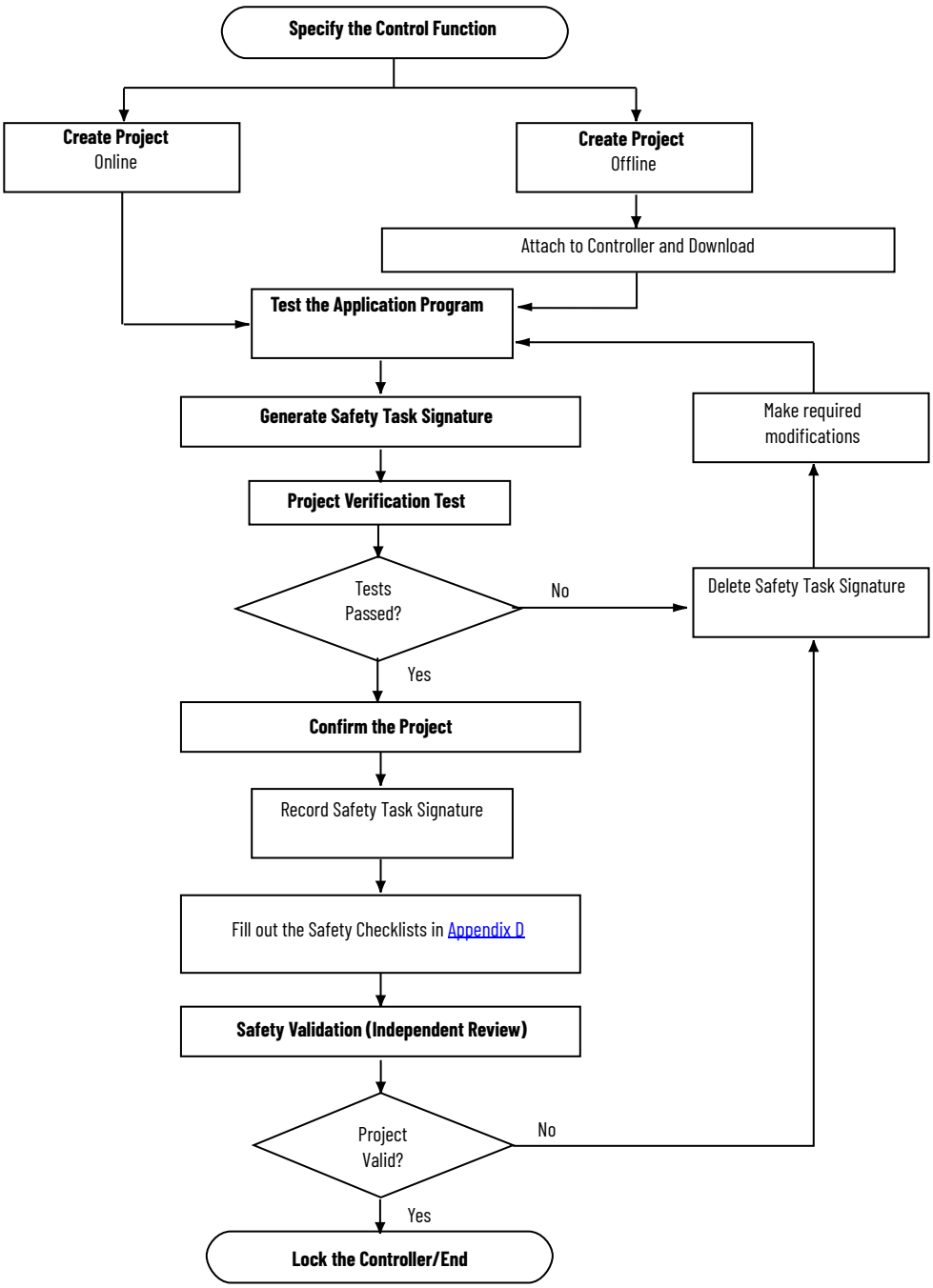
We recommend that the application program for the intended SIL CL3 system is developed by the system integrator or a user who is trained and experienced in safety applications. The developer must follow good design practices:

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

Commissioning Lifecycle

The flowchart below shows the steps that are required for commissioning a GuardLogix® system. The items in bold text are explained in the following sections.

Figure 15 - Commission the System



Specification of the Control Function

You must create a specification for your control function. Use this specification to verify that program logic correctly and fully addresses your application's functional and safety control requirements. 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 print out
- 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 required for SIL levels
  - Discrepancy monitoring and visualization, including your diagnostic logic
- Actuators
  - Position and activation in standard operation (normally OFF)
  - 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

The application program is clearly identified by one of the following:

- Name
- Date
- Revision
- Any other user 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 Verification test.

Generate the Safety Task Signature

The safety task signature is required to operate in a SIL 3 safety function. It uniquely identifies each project, including its logic, data, and configuration. The safety task signature is composed of an ID (identification number), date, and time.

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

- The 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 application program testing is complete, you must generate the safety task signature. The programming software automatically uploads the safety task signature after it is generated.

IMPORTANT	To verify the integrity of every download, you must manually record the safety task signature after initial creation and check after every download to make sure that it matches the original.

You can delete the safety task signature only when the GuardLogix® controller is safety-unlocked and, if online, the keyswitch is in the REM or PROG position.

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

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

Project Verification Test

To check your application program for adherence to the specification, you must generate a suitable set of test cases covering 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 manually manipulating sensors and actuators.

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

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

To perform a project verification 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. From a controller perspective, this means toggling the I/O point going into the controller, not necessarily the actual activators. Be sure to test all shutdown functions, because these functions are not typically exercised during normal operation.

Also, a project verification test is valid only for the specific application tested. If the controller is moved to another application, you must also perform startup and project verification testing on the controller in the context of its new application program.

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, Safety Add-On Instructions for information on creating and using safety Add-on Instructions in SIL 3 applications.

The steps below illustrate one method for confirming the project.

1. With the controller in Program mode, save the project.
2. Answer Yes to the Upload Tag Values prompt.
3. With the Logix Designer application offline, save the project with a new name, such as Offlineprojectname.ACD, where 'projectname' is the name of your project.

   This 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 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 Logix Designer Program Compare utility to perform these comparisons:
   - Compare all of the properties of the GuardLogix controller and CIP Safety™ I/O devices.
   - Compare all of the properties of the safety task, safety programs and safety routines.
   - Compare all of the logic in the safety routines.

Safety Validation

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

Lock the GuardLogix Controller

The GuardLogix controller system can be safety-locked to help protect safety control components from modification. However, safety-locking the controller is not a requirement for SIL 3 applications. The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety tags, safety Add-OnOn Instructions, safety I/O, and safety task signature. However, safety-locking alone does not satisfy 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:

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

IMPORTANT	If a safety task signature exists and the controller is safety-locked, only projects with a matching safety task 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 may 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, refer to the GuardLogix 5570 Controllers User Manual, publication 1756-UM022, or the Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022.

Downloading the Safety Application Program

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

IMPORTANT	To verify the integrity of every download, you must manually record the safety task signature after initial creation and check the safety task signature after every download to make sure that it matches the original.

Downloads to a safety-locked GuardLogix controller are allowed only if the safety task signature, the hardware series, and the operating system version of the offline project all match those contained in the target GuardLogix controller and the controller's safety task status is OK.

IMPORTANT	If the safety task 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 task signature. As a result, you must revalidate the application.

ATTENTION: The USB port is intended for only temporary local programming purposes and not intended for permanent connection.

Uploading the Safety Application Program

If the GuardLogix controller contains a safety task signature, the safety task signature is uploaded with the project. This means that any changes made to offline safety data are overwritten as a result of the upload.

Online Editing

If there is no safety task signature and the controller is safety-unlocked, you can perform online edits to your safety routines.

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

Pending edits cannot exist when the controller is safety-locked or when there is a safety task signature. Online edits can exist when the controller is safety-locked. However, they cannot be assembled or canceled.

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

See page 46 for more information about edits to your application program.

Storing and Loading a Project from Nonvolatile Memory

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 for nonvolatile memory.

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 nonvolatile memory only under these conditions:

- If the controller type specified by the project that is stored in nonvolatile memory matches your controller type
- If the major and minor revisions of the project in nonvolatile memory match the major and minor revisions of your controller
- If your controller is not in Run mode

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

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

Force Data

All data 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 task signature exists. However, forces must be uninstalled, not just disabled, on all safety tags before the safety project can be safety-locked or a safety task signature can be generated. You cannot force safety tags while the project is safety-locked or when a safety task signature exists.

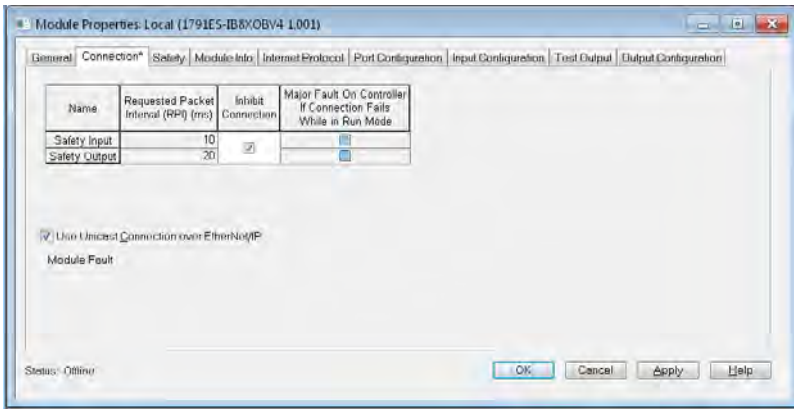
You can install and uninstall forces on standard tags regardless of the safety-locked or -unlocked state.

Inhibit a Device

You cannot inhibit or uninhibit CIP Safety I/O devices or producer controllers if the application program is safety-locked or a safety task signature exists.

Follow these steps to inhibit a specific safety I/O device.

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



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

Editing Your Safety Application

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

- Only authorized, specially trained personnel can make program edits. These personnel should use all supervisory methods available, for example, using the controller keyswitch and software password protections.
- When authorized, specially-trained personnel make program edits, they assume the central safety responsibility while the changes are in progress. These personnel must also maintain safe application operation.
- When editing 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 task 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 resuming operation.

The flowchart on page 48 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 resuming operation. The flowchart on page 48 illustrates the process for online editing.

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

Online edits are affected by the safety-lock and safety task signature features of the GuardLogix controller.

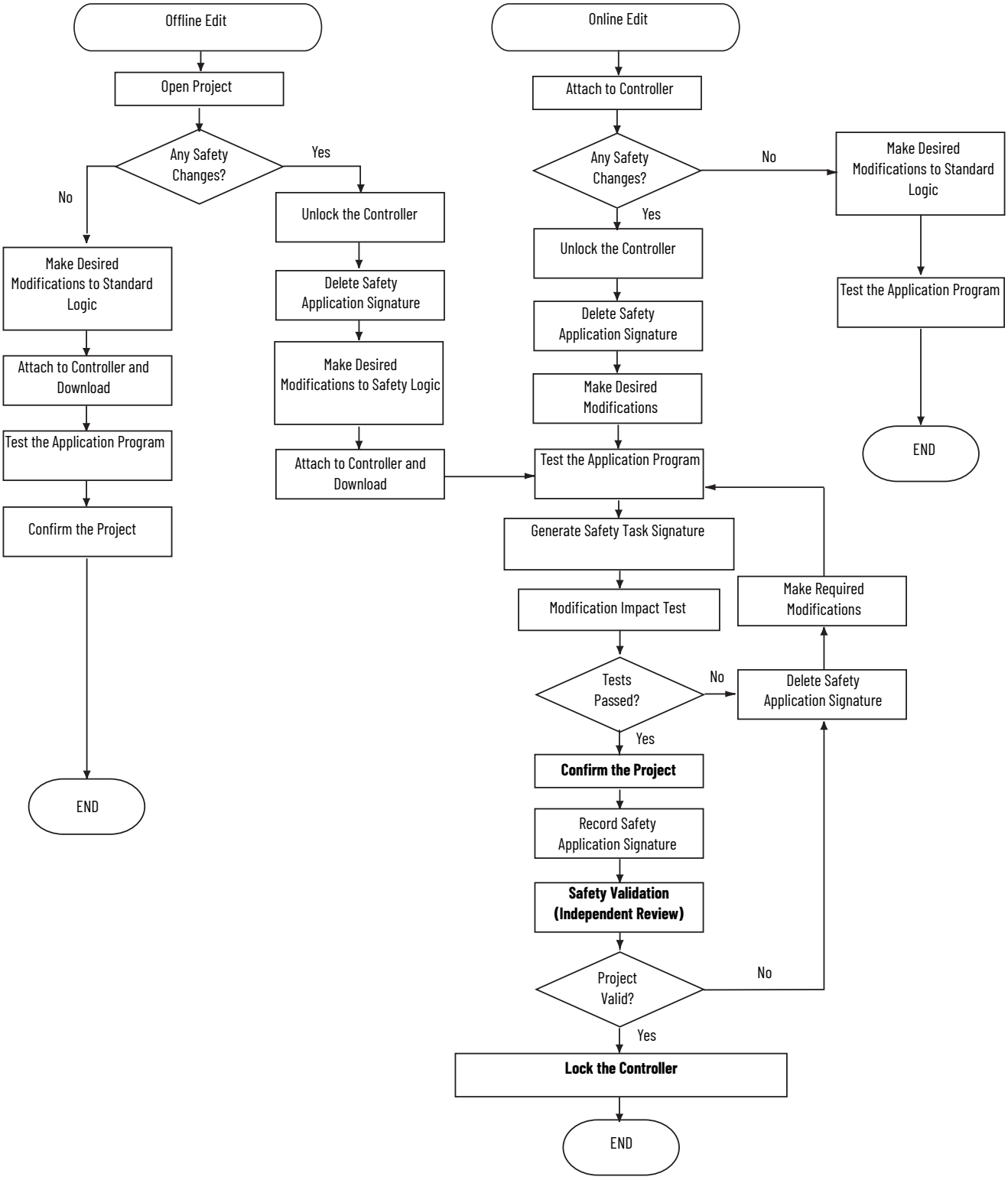
See Generate the Safety Task Signature on page 42 and Lock the GuardLogix Controller on page 44 for more information.

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

Modification Impact Test

Any modification, enhancement, or adaptation of your validated software must be planned and analyzed for any impact to the functional safety system. All appropriate phases of the software safety lifecycle must be implemented as indicated by the impact analysis. At a minimum, functional testing of all impacted software must be implemented. All modifications to your software specifications must be documented. Test results must also be documented. For detailed information, see IEC 61508-3, Section 7.8 Software Modification.

Figure 16 - Online and Offline Edit Process



Monitor Status and Handle Faults

The GuardLogix® architecture provides you with many ways of detecting and reacting to faults in the system. The first way that you can handle faults is to make sure you have completed the checklists for your application (see Appendix D).

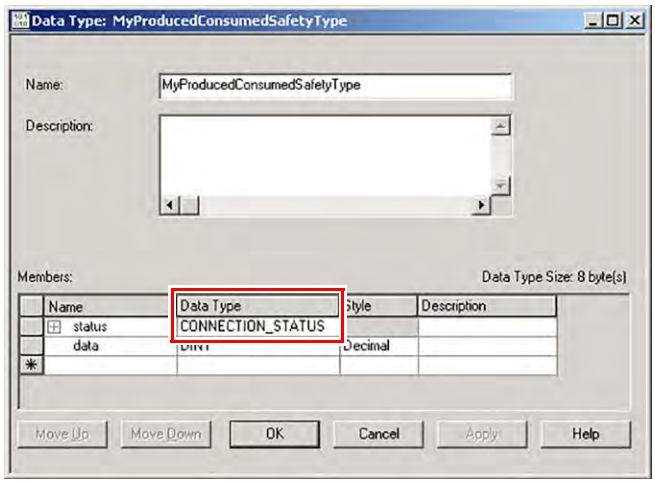
Monitoring System Status

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 17 - Data Type Dialog Box



The first two bits of the CONNECTION_STATUS data type contain a device's RunMode and ConnectionFaulted status bits.

Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Idle	0 = Valid	The connection is active and the producing device is in the Idle state. The safety data is reset to zero.
0 = Idle	1 = Faulted	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero.
1	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. If you must detect a device fault to be sure that the system maintains SIL 3, 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 make sure the system restarts properly.

I/O Device Connection Status

The CIP Safety™ protocol provides status for each I/O device in the safety system. If an input connection failure is detected, the operating system sets all device inputs to their de-energized (safety) state, and the associated input status to faulted. If an output connection failure is detected, the operating system sets the associated output status to faulted. The output device de-energizes the outputs.

IMPORTANT	You are responsible for providing application logic to latch these I/O failures and to make sure 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 zero (safe state). Faults associated to a specific input channel result in that specific channel being set to zero; for example, a pulse test fault that is specific to channel 0 results in channel 0 input data being set to the safe state (0). 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 (0).

For information on how to use GuardLogix safety application instructions, see Appendix F of this manual and the GuardLogix Safety Application Instructions Safety 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. Safety object attributes written by the standard task 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 following.

- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

For general information on using GSV and SSV instructions, refer to the Logix Controllers Instructions Reference Manual, publication 1756-RM009.

GuardLogix System Faults

Faults in the GuardLogix system fall into these three categories:

- Nonrecoverable controller faults
- Nonrecoverable safety faults
- Recoverable faults

For information on handling faults, see the following:

- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

Nonrecoverable Controller Faults

A nonrecoverable controller fault occurs if the controller's internal diagnostics fail. Partnership is lost when a nonrecoverable controller fault occurs in either the primary controller or the safety partner, causing the other to generate a nonrecoverable watchdog timeout fault. Standard task and safety task execution stops, and Safety I/O transitions to the safe state.

Recovery from a nonrecoverable controller fault requires a download of the application program.

Nonrecoverable Safety Faults

In the event of a non-recoverable safety fault, the controller logs the fault to the controller-scoped fault handler and shuts down the safety task, including Safety I/O and safety logic.

To recover from a nonrecoverable safety fault, safety memory is reinitialized either from the safety task signature (happens automatically when you clear the fault) or, if no safety task signature exists, via an explicit download of the safety project.

You can override the safety fault by clearing the fault log entry through the controller-scoped safety fault handler. This allows standard tasks to keep running.

ATTENTION: Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that doing so maintains SIL 3.

Recoverable Faults

Controller faults that are caused by user programming errors in a safety program trigger the controller to process the logic contained in the project's safety program fault handler. The safety program fault handler provides the application with the opportunity to resolve the fault condition and then recover.

ATTENTION: You must provide proof to your certifying agency that automatic recovery from recoverable faults maintains SIL 3.

When a safety program fault handler does not exist or the fault is not recovered by it, the controller processes the logic in the controller-scoped fault handler, terminating safety program logic execution and leaving safety I/O connections active, but idle.

IMPORTANT When the execution of safety program logic is terminated due to a recoverable fault that is not handled by the safety program fault handler, the safety I/O connections are closed and reopened to reinitialize safety connections.

If user logic is terminated as a result of a recoverable fault that is not recovered, 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.

When you use safety I/O for standard applications, safety I/O is commanded to the safe state if user logic is terminated as a result of a recoverable fault that is not recovered.

If a recoverable safety fault is overridden in the controller-scoped fault handler, only standard tasks keep running. If the fault is not overridden, the standard tasks are also shut down.

ATTENTION: Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that the action maintains SIL 3.

Safety Instructions

For the latest information on certified instructions, see our safety certificates and revision release list at rok.auto/certifications.

Table 6 and Table 7 list the safety application instructions that are certified for use in SIL 3 applications.

Table 6 - 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 a single 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 Bidirectional 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 7 - 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.

Table 7 - Metal-Form Safety-Application Instructions (Continued)

Mnemonic	Name	Purpose
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 manually drive a valve during maintenance operations.

For more information on RSLogix 5000® instructions, see Appendix.

Table 8 - RSLogix 5000, Version 14 and Later, Safety Application Instruction Descriptions

Mnemonic	Name	Purpose
ENPEN	Enable Pendant	Monitors two safety inputs to control a single output and has a 3-s inputs-inconsistent timeout value.
ESTOP	E-stop	Monitors two safety inputs to control a single output and has a 500-ms inputs-inconsistent timeout value.
RIN	Redundant Input	Monitors two safety inputs to control a single 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 a single 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 a single output.
LC	Light Curtain	Monitors two safety inputs from a light curtain to control a single output.

Routines in the safety task can use these ladder-logic safety instructions.

Table 9 - Ladder Logic Safety Instructions

Type	Mnemonic	Name	Purpose
Array (File)	FAL	File Arithmetic and Logic	Perform copy, arithmetic, logic, and function operations on data that is stored in an array.
	FLL	File Fill	Fill the element of an array with the Source Value, while leaving the source value unchanged.
	FSC	File Search and Compare	Compare the value in an array, element by element.
	SIZE	Size In Elements	Find the size of a dimension of an array.
Bit	XIC	Examine If Closed	Enable outputs when a bit is set.
	XIO	Examine If Open	Enable outputs when a bit is cleared.
	OTE	Output Energize	Set a bit.
	OTL	Output Latch	Set a bit (retentive).
	OTU	Output Unlatch	Clear bit (retentive).
	ONS	One Shot	Triggers an event to occur one time.
	OSR	One Shot Rising	Triggers an event to occur one time on the false-to-true (rising) edge of change-of-state.
	OSF	One Shot Falling	Triggers an event to occur one time on the true-to-false (falling) edge of change-of-state.
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.

Table 9 - Ladder Logic Safety Instructions (Continued)

Type	Mnemonic	Name	Purpose
Compare	CMP[1]	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.
	COP[2]	Copy	Copy 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	Jump over a section of logic that does not always need to be executed (skips to referenced label instruction).
	LBL	Label	Labels an instruction so that it can be referenced by a JMP instruction.
	JSR	Jump to Subroutine	Jump to a separate routine.
	RET	Return	Return the results of a subroutine.
	SBR	Subroutine	Pass data to a subroutine.
	TND	Temporary End	Mark a temporary end that halts routine execution.
	MCR	Master Control Reset	Disable every rung in a section of logic.
	AFI	Always False Instruction	Disable a rung.
	NOP	No Operation	Insert a placeholder in the logic.
	EVENT	Trigger Event Task	Trigger one execution of an event task.[4]
Math/ Compute	ADD	Add	Add two values.
	CPT	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[3]	Get System Value	Get controller status information.
	SSV[3]	Set System Value	Set controller status information.

(1) Advanced operands like SIN, COS, and TAN are not supported in safety routines.
(2) The length operand must be a constant when the COP instruction is used in a safety routine. The length of the source and the destination must be the same.
(3) For special considerations when using the GSV and SSV instructions, see the GuardLogix® 5570 Controllers User Manual, publication 1756-UM022 or the Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022.
(4) The event instruction triggers a scan of the standard task.

IMPORTANT If you use Motion Direct Commands with a Kinetix® 5500 or K5700 servo drive or a PowerFlex® 527 drive, see the following publications 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 these 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.
Logix Controllers Instructions Reference Manual, publication 1756-RM009	Provides information on the Logix 5000® instruction set that includes general, motion, and process instructions.

Safety Add-On Instructions

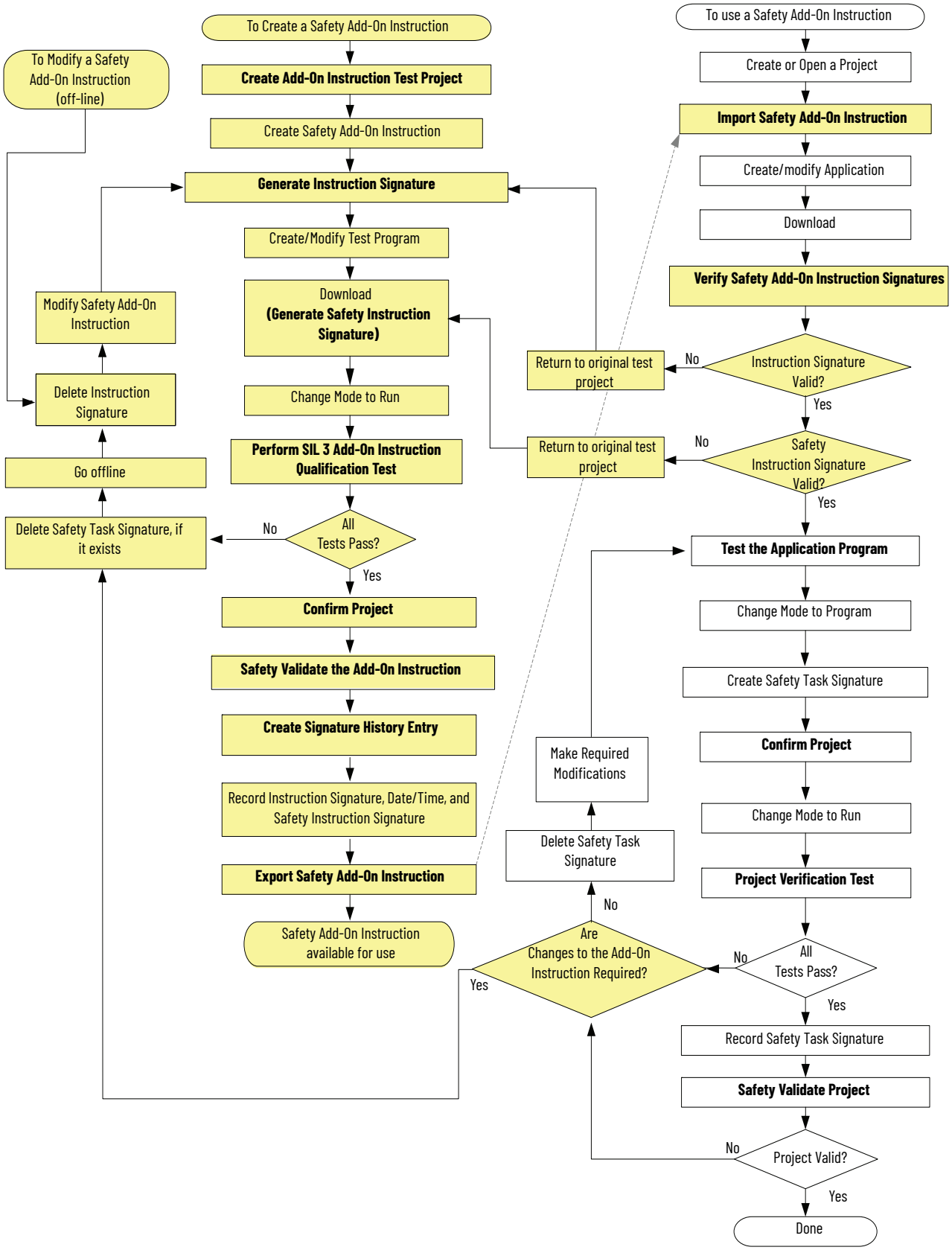
With the Logix Designer application, you can create safety Add-On Instructions. Safety Add-On Instructions let you encapsulate commonly used safety logic into a single instruction, which makes it modular and easier to reuse.

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

Create and Use a Safety Add-On Instruction

This figure shows the steps that are required to create a safety Add-On Instruction and then use that instruction in a SIL 3 safety application program. The shaded items are steps unique to Add-On Instructions. The items in bold text are explained in the pages following the flowchart.

Figure 18 - Flowchart for Creating and Using Safety Add-On Instructions



Create 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 41.

Create a Safety Add-On Instruction

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

Generate Instruction Signature

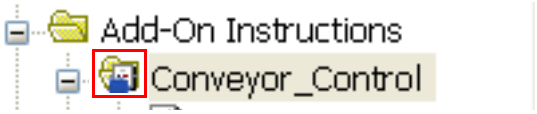
The instruction signature lets you quickly determine if the instruction has been modified. Each Add-On Instruction can have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and can sometimes be required for regulated industries.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



IMPORTANT	If you plan to protect your Add-On Instruction by using the source protection feature in the Logix Designer application, you must enable source protection before you generate the instruction signature.

Download and Generate Safety Instruction Signature

When a sealed safety Add-On Instruction is downloaded for the first time, a SIL 3 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 3 Add-On Instruction Qualification Test

Safety Add-On Instruction SIL 3 tests must be performed in a separate, dedicated application to make sure 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.

Development of all safety Add-On Instructions must meet IEC 61508 - 'Requirements for software module testing', which provides detailed requirements for unit testing.

Confirm the Project

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

See Confirm the Project on page 43 for a description of one method to confirm a project.

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 is required for IEC 61508 SIL 3.

Create Signature History Entry

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

The Signature Listing report in the 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 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 project.
- You cannot import a safety Add-On Instruction into a safety project that has been safety-locked or one that has a safety task 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 Types are not available, you may need to remove the signature.

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 Verification Test

Perform an engineering test of the application, including the safety system.

See Project Verification Test on page 42 for more information on requirements.

Safety Validate Project

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

Additional Resources

For more information on Add-On Instructions, refer to these publications.

Resource	Description
Logix5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on how to plan, create, use, import, and export Add-On Instructions in RSLogix 5000® applications.
Import/Export Project Components Programming Manual, publication 1756-PM019	Contains detailed information on how to import and export project components.

Notes:

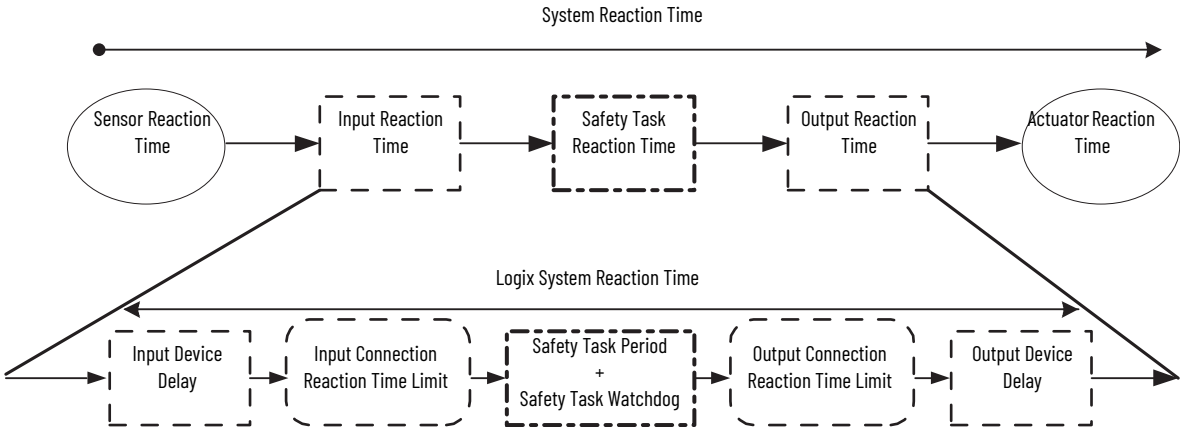
Reaction Times

System Reaction Time

To determine the system reaction time 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 19 - System Reaction Time

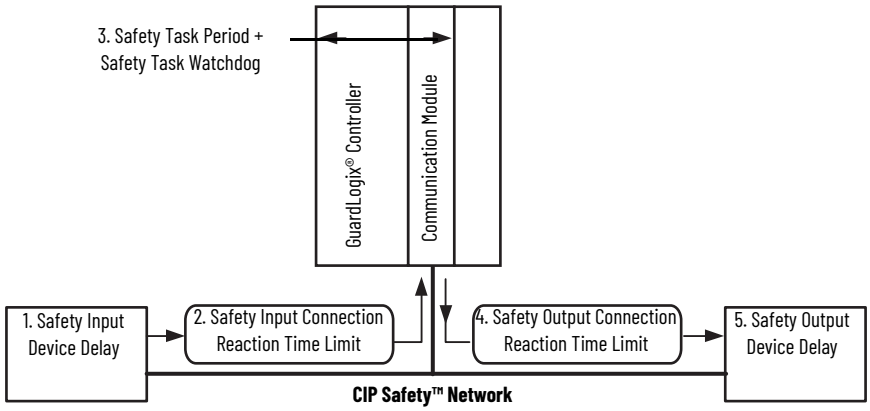


Logix System Reaction Time

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

Figure 20 - Logix System Worst-case Reaction Time for Simple Input to Logic to Output



The Logix System Reaction Time for any simple input to logic to output chain consists of these five components:

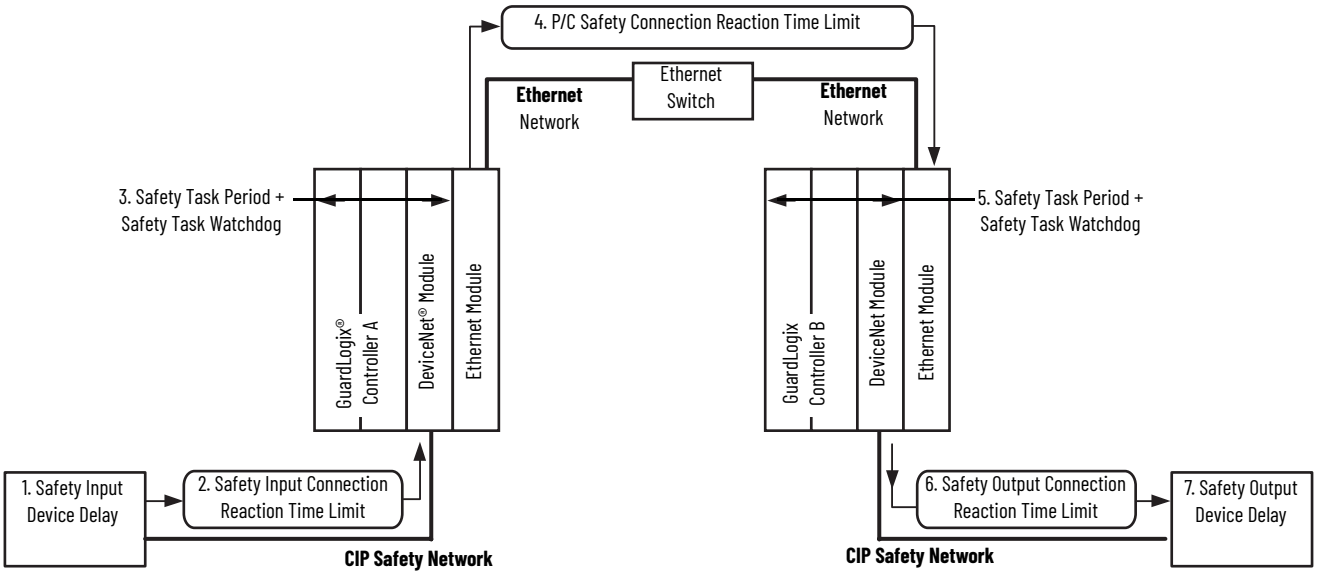
1. Safety input device reaction time (plus input delay time, if applicable)
2. Safety Input Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety input device connection RPI.)
3. Safety Task Period plus Safety Task Watchdog time

4. Safety Output Connection Reaction Time Limit
   (Read from the Module Properties dialog box in the Logix Designer application, this value is a multiple of the safety task period.)
5. Safety output device reaction time

To aid you in determining the reaction time of your particular control loop, a Microsoft® Excel® spreadsheet is available in the Tools folder of the Studio 5000® environment DVD.

Logic Chain Using Produced/Consumed Safety Tags

Figure 21 - 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
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

To aid you in determining the reaction time of your particular control loop, a Microsoft Excel spreadsheet is available in the Tools folder of the Studio 5000 environment DVD.

Factors That Affect Logix Reaction-time Components

The Logix Reaction Time components that are described in the previous sections can be influenced by a number of factors.

Table 11 - Factors Affecting Logix System Reaction Time

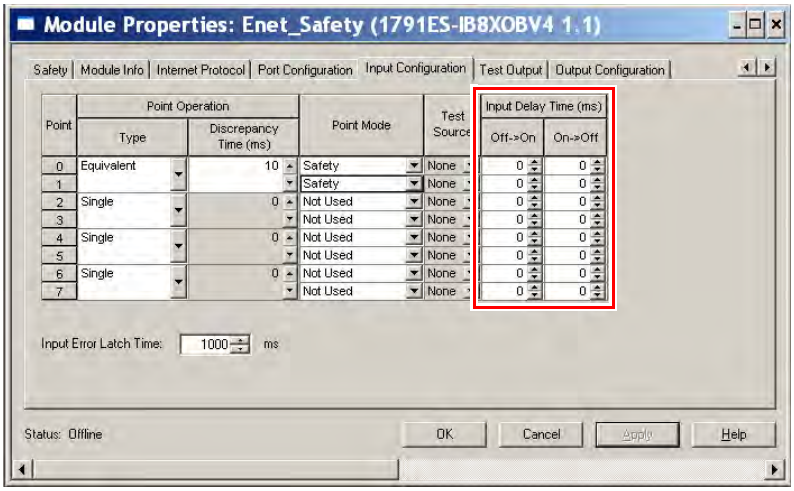
These Reaction Time Components	Are Influenced by the Following Factors
Input device delay	Input device reaction time
	On-Off and Off-On delay settings for each input channel, if applicable
Safety Input Connection Reaction Time Limit	Input device settings for: • Requested Packet Interval (RPI) • Timeout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

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

Access Guard I/O Input Module Delay Time Settings

To configure input module delay time in the 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.



Access Input and Output Safety Connection Reaction Time Limit

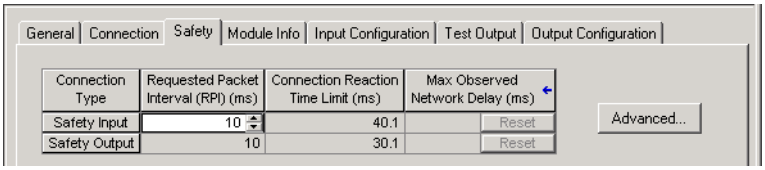
The Connection Reaction Time Limit (CRTL) is defined by these three values:

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 essentially 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.

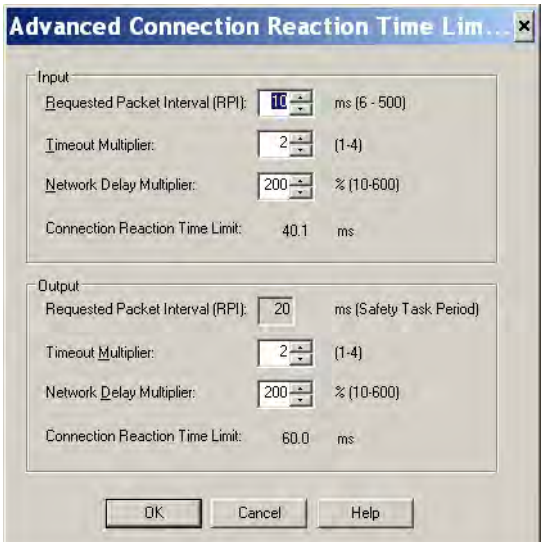
If you adjust these values, then you can adjust the Connection Reaction Time Limit. If a valid packet is not received within the CRTL, the safety connection times out, and the input and output data is placed in the safe state (OFF).

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.



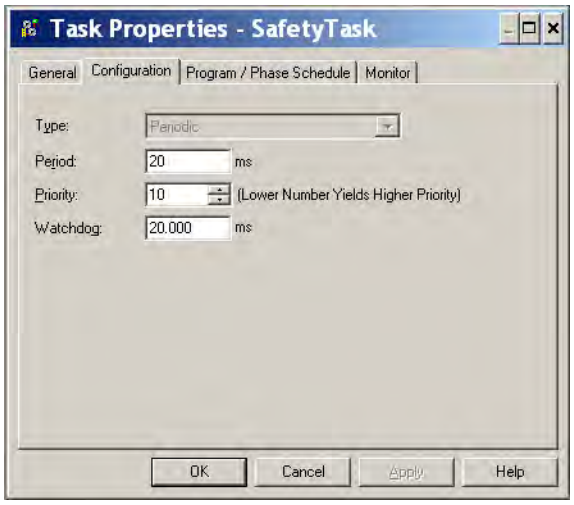
3. Click Advanced to open the Advanced Connection Reaction Time Limit dialog box.



Configure the Safety Task Period and Watchdog

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

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

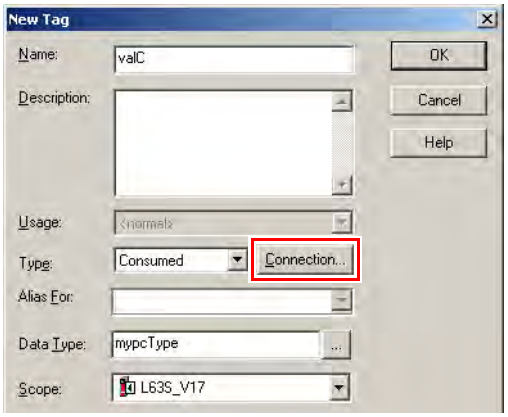


The priority of the safety task is not a safety concern, as the safety task watchdog monitors if the task is interrupted by higher priority task.

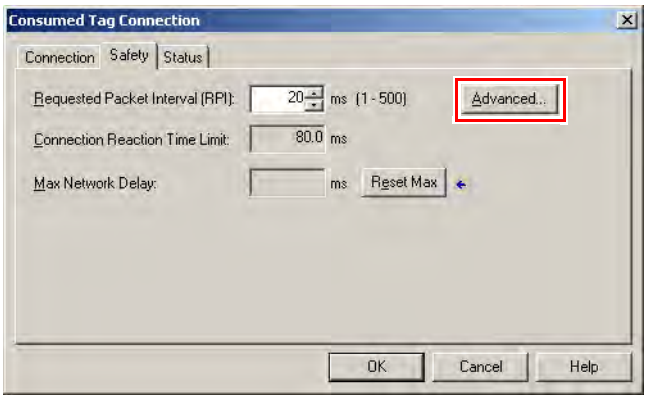
Access Produced/Consumed Tag Data

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

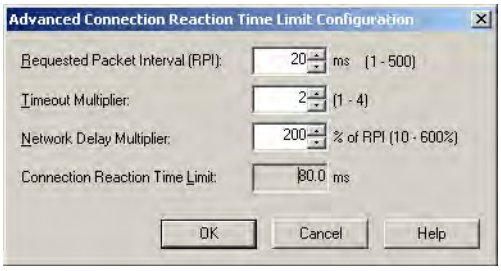
1. In the configuration tree, right-click Controller Tags and choose Edit tags.
2. In the Tag Editor, right-click the name of the tag and choose Edit Properties.
3. Click Connection.



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.

- GuardLogix 5570 Controllers User Manual, publication 1756-UM022
- Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022

Checklists for GuardLogix Safety Applications

The checklists in this appendix are required to plan, program, and start up a SIL 3-certified GuardLogix® application. They can be used as planning guides and during project verification testing. If used as planning guides, the checklists can be saved as a record of the plan.

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

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

Checklist for GuardLogix Controller System

Company	
Site	
Safety Function Definition	

Number	System Requirements	Fulfilled		Comment
		Yes	No	
1	Are you using only the SIL 3-certified components, with the corresponding firmware release, as listed at https://www.rockwellautomation.com/global/certification/safety.page	☐	☐	
2	Have you calculated the system's safety response time for each safety chain?	☐	☐	
3	Does the system's response time 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 tolerance time?	☐	☐	
5	Have probability (PFD/PFH) values been calculated per the system's configuration?	☐	☐	
6	Have you performed all appropriate project verification 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 CIP Safety™ device configured with the correct SNN?	☐	☐	
10	Have you generated a safety task signature?	☐	☐	
11	Have you uploaded and recorded the safety task signature for future comparison?	☐	☐	
12	After a download, have you verified that the safety task signature in the controller matches the recorded safety task 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 pages 73 and 73?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Checklist for Safety Inputs

For programming or startup, an individual checklist can be completed for every SIL input channel in a 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.

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 verification 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 PLe/Cat. 4 per ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the sensor and input are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on how to wire your CIP Safety™ I/O device, refer to the product documentation for your specific device.

Checklist for Safety Outputs

For programming or startup, an individual requirement checklist must be completed for every SIL output channel in a 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.

Company	
Site	
Safety Function Definition	
SIL Output Channels	

Number	Output Device Requirements	Fulfilled		Comment
		Yes	No	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed project verification 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 PLe/Cat. 4 per ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the output and the actuator are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on how to wire your safety I/O device, refer to the product documentation for your specific device.

Checklist to Develop a Safety Application Program

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

Company	
Site	
Project Definition	

Number	Application Program Requirements	Fulfilled		Comment
		Yes	No	
1	Are you using version 21 or later[1] of Logix Designer application, the GuardLogix system programming tool?	☐	☐	
2	Were the programming guidelines in Chapter 6 followed during creation of the safety application program?	☐	☐	
3	Does the safety application program contain only relay ladder logic?	☐	☐	
4	Does the safety application program contain only those instructions that are listed in Appendix A as suitable for safety application programming?	☐	☐	
5	Does the safety application program clearly differentiate between safety and standard tags?	☐	☐	
6	Are only safety tags used for safety routines?	☐	☐	
7	Have you verified that safety routines do not attempt to read from or write to standard tags?	☐	☐	
8	Have you verified that no safety tags are aliased to standard tags and vice versa?	☐	☐	
9	Is each safety output tag correctly configured and connected to a physical output channel?	☐	☐	
10	Have you verified that all mapped tags have been conditioned in safety application logic?	☐	☐	
11	Have you defined the process parameters that are monitored by fault routines?	☐	☐	
12	Have you sealed any safety Add-On Instructions with an instruction signature and recorded the safety instruction signature?	☐	☐	
13	Has the program been reviewed by an independent safety reviewer (if necessary)?	☐	☐	
14	Has the review been documented and signed?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) The Studio 5000 Logix Designer® application version 28 or later supports Compact GuardLogix 5370 controllers.

GuardLogix Systems Safety Data

The following examples show probability of a dangerous failure on demand (PFD) and average frequency of a dangerous failure per hour (PFH) values for GuardLogix® 1oo2 SIL 3 systems.

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.

Data for Rockwell Automation® machine safety products is now available in the form of a library file to be used with the Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA). The library file is available for download at https://www.rockwellautomation.com/en-us/capabilities/industrial-safety-solutions/machine-safety.html.

Mission time for GuardLogix controllers is 20 years.

PFD Values

Table 12 - Calculated PFD Values by Proof Test Interval

Cat. No.	Description	Calculated PFD			
		2 Years (17,520 hours)	5 Years (43,800 hours)	10 Years (87,600 hours)	20 Years (175,200 hours)
1756-L7xS, 1756-L7SP, 1756-L72EROMS, and 1756-L73EROMS	GuardLogix and Armor™ GuardLogix® 5570 controllers	5.4E-06	1.5E-05	3.4E-05	8.4E-05
1756-L73SXT and 1756-L7SPXT	GuardLogix 5570 XT controller	5.4E-06	1.5E-05	3.4E-05	8.4E-05
1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMSK, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS, 1769-L37ERMS, 1769-L37ERMSK, 1769-L38ERMOS, 1769-L38ERMS, 1769-L38ERMSK	Compact GuardLogix and Armor™ Compact GuardLogix 5370 controllers	9.4E-06	2.4E-05	5.2E-05	1.2E-04

PFH Values

This table data applies to proof test intervals up to and including 20 years.

Table 13 - PFH Calculation

Cat. No.	Description	PFH (1/Hour)
1756-L7xS, 1756-L7SP, 1756-L72EROMS, and 1756-L73EROMS	GuardLogix and Armor GuardLogix 5570 controllers	1.1E-09
1756-L73SXT and 1756-L7SPXT	GuardLogix 5570 XT controller	1.1E-09
1769-L30ERMS, 1769-L33ERMS, 1769-L33ERMSK, 1769-L33ERMOS, 1769-L36ERMS, 1769-L36ERMOS, 1769-L37ERMOS, 1769-L37ERMS, 1769-L37ERMSK, 1769-L38ERMOS, 1769-L38ERMS, 1769-L38ERMSK	Compact GuardLogix and Armor Compact GuardLogix 5370 controllers	1.5E-09

Notes:

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

De-energize to Trip System

When using instructions from RSLogix 5000® software, version 14, safety application instructions, all inputs and outputs are set to zero when a fault is detected. As a result, any inputs that are monitored by one of the diverse input instructions (Diverse Inputs or Two-hand Run Station) should have normally-closed inputs that are conditioned by logic similar to the logic in Rung 4 of Ladder Logic Example 2 and Ladder Logic Example 3 on pages 80 and 81. The exact logic that is required is both application and input-device dependent. However, the logic must create a safe state of 1 for the normally-closed input of the diverse input instructions.

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 78 to determine which rungs of logic are required for different application situations. Ladder Logic Example 1 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 Logic Example 2. 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 to determine which rungs of application logic in Ladder Logic Example 3 on page 81 are required.

Figure 22 - Input Fault Latch and Reset Flowchart

Figure 23 - Ladder Logic Example 1

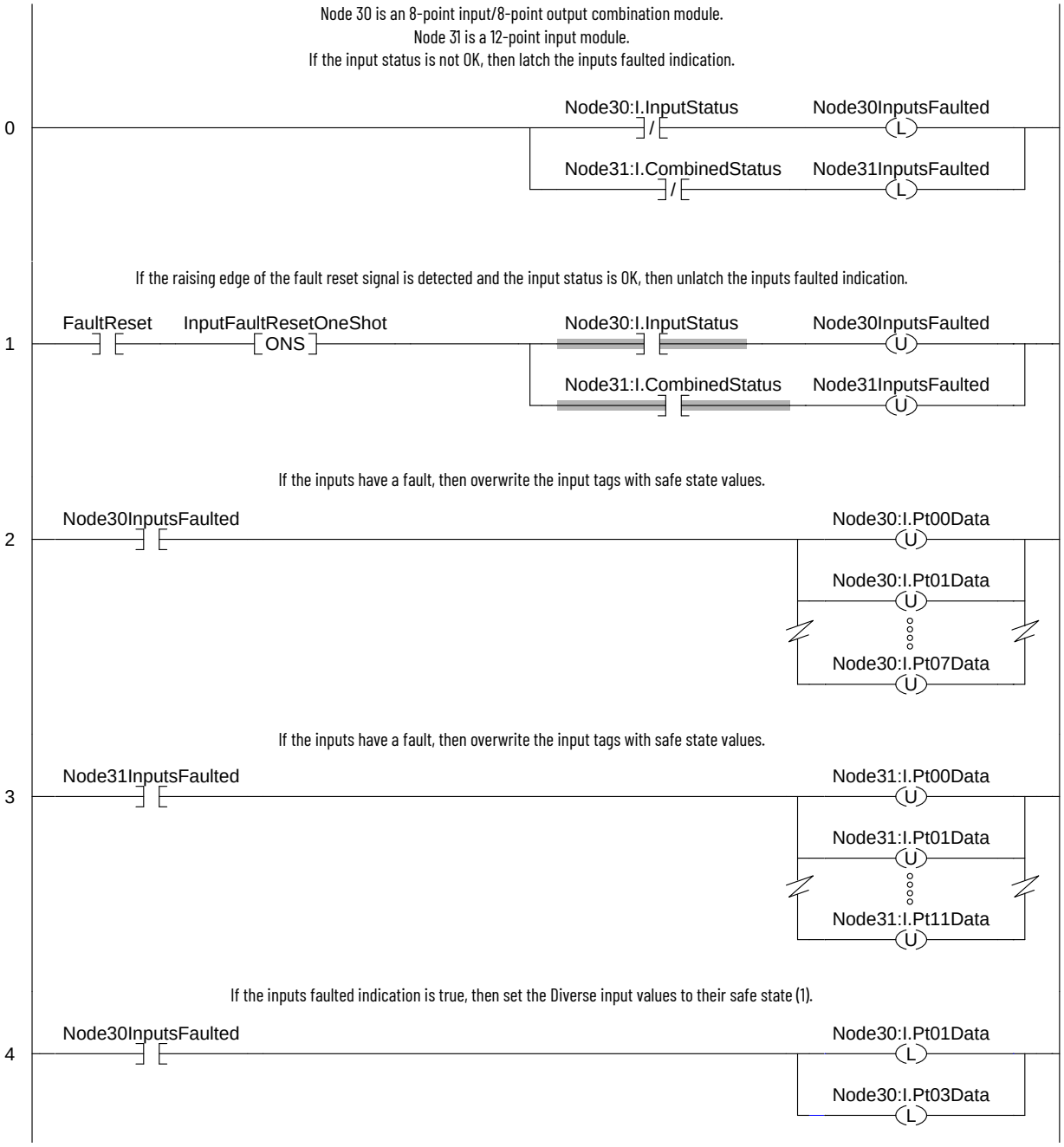


Figure 24 - Ladder Logic Example 2

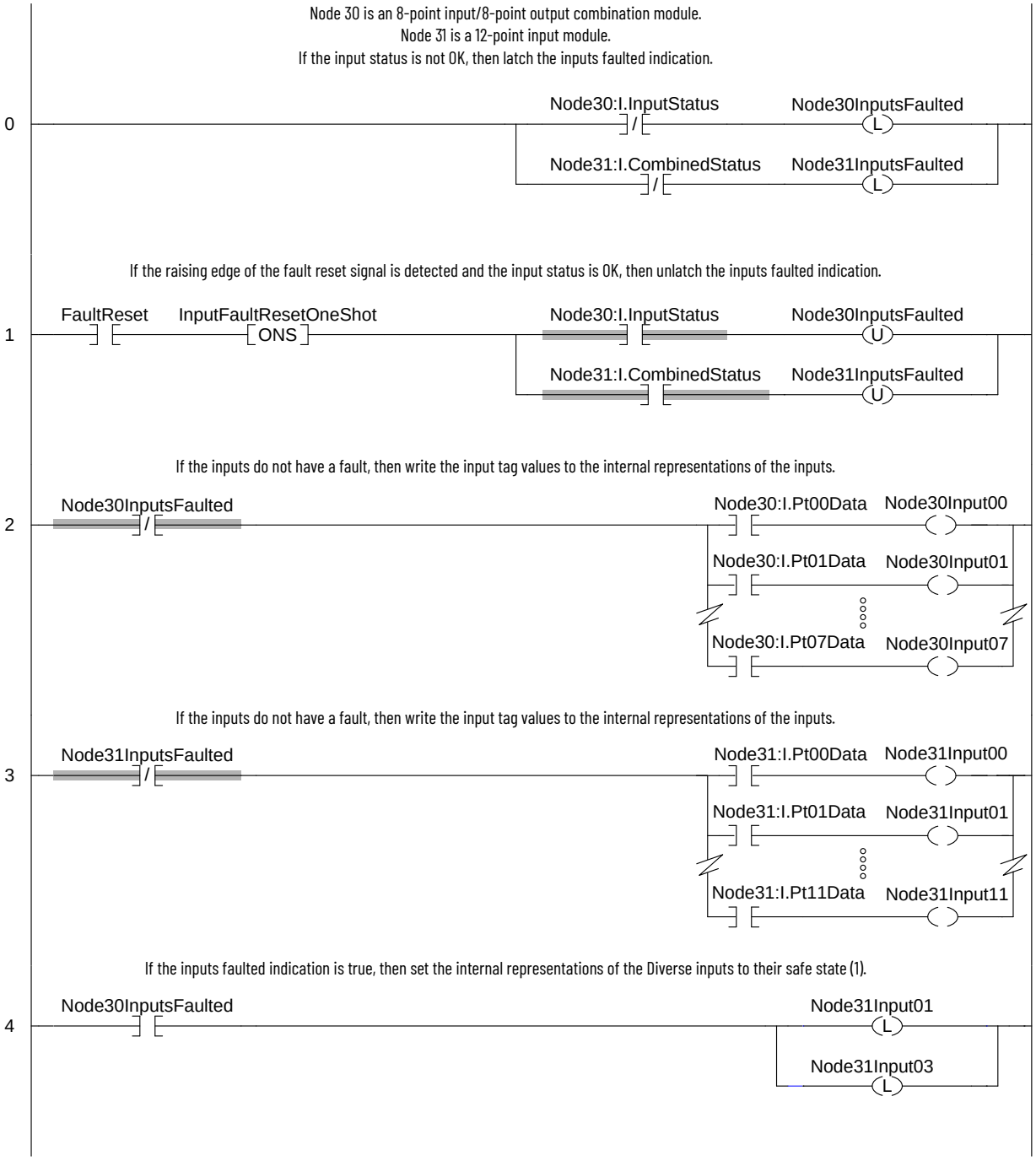


Figure 25 - Output Fault Latch and Reset Flowchart

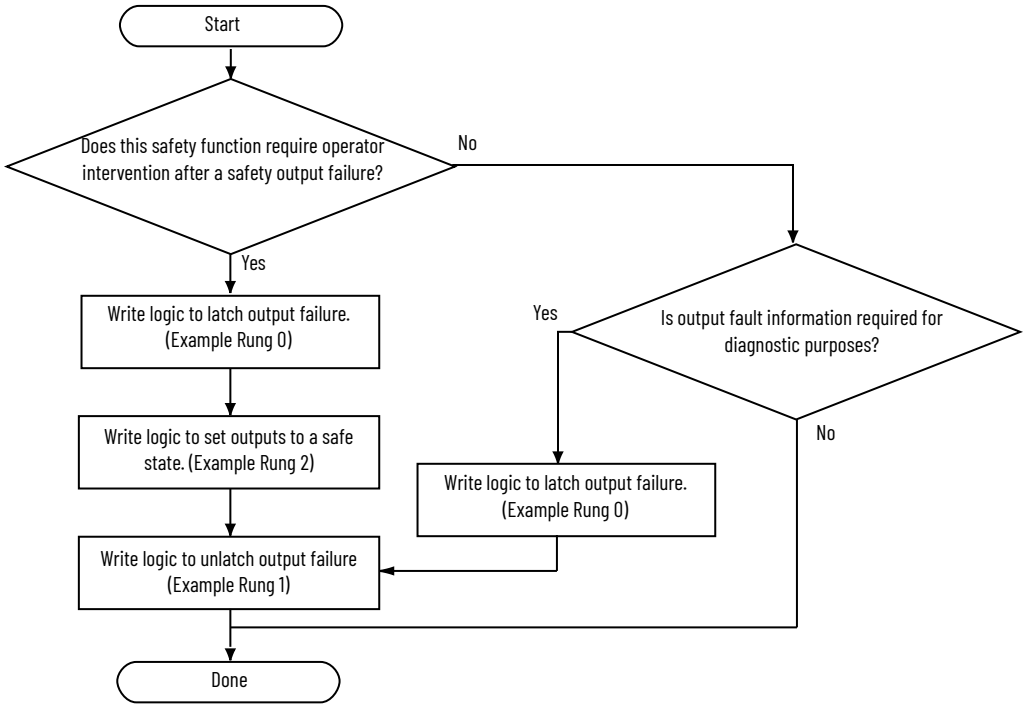
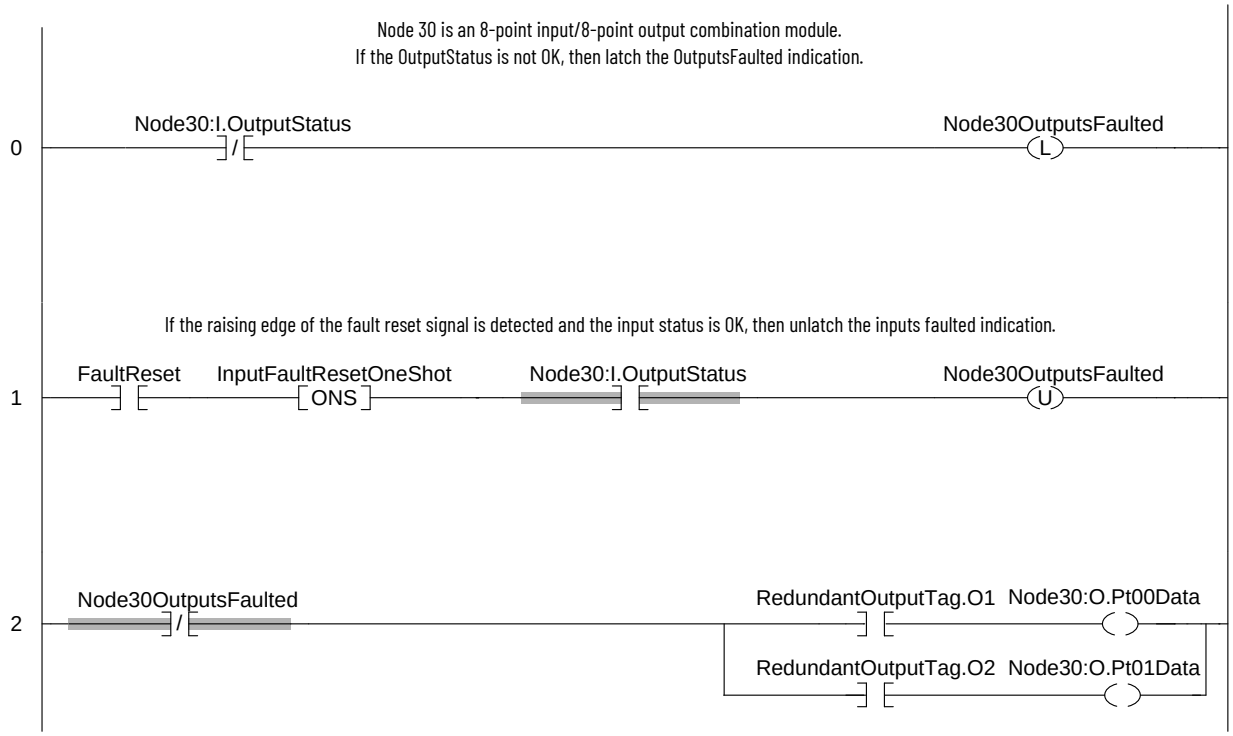


Figure 26 - Ladder Logic Example 3



Notes:

Use of 1794 FLEX I/O Modules and 1756 SIL 2 Inputs and Outputs with GuardLogix 5570 Controllers to Comply with EN 50156

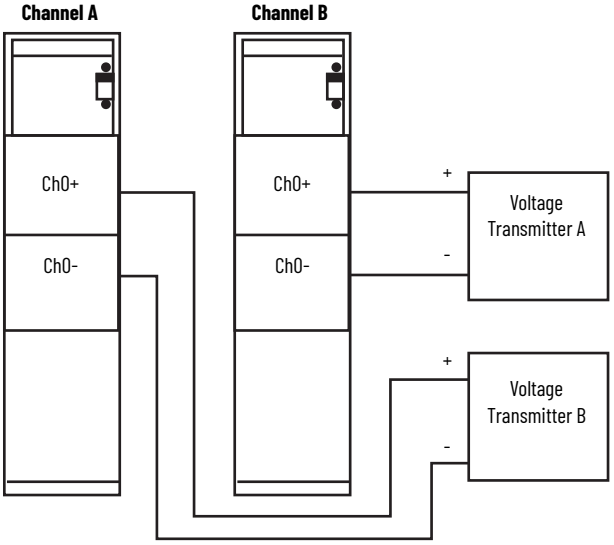
Dual channel configuration is required for compliance in certain safety-related applications, including burner-related safety functions. These examples provide guidelines for satisfying EN50156 SIL 2 dual channel requirements with 1- and 2-year proof test intervals.

The information in this appendix is applicable only to GuardLogix® 5570 controller systems.

SIL 2 Dual Channel Inputs (standard side of GuardLogix 5570 controllers)

You must implement clear and easily identifiable separation between both input channels and adhere to all existing SIL 2 requirements as defined in Using ControlLogix® in SIL 2 Applications, publication 1756-RM001.

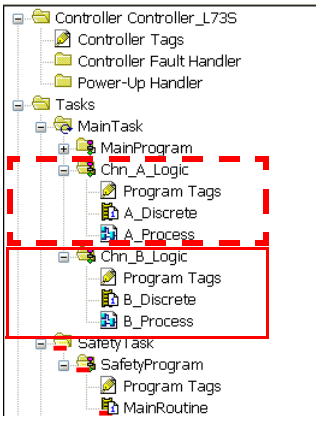
Figure 27 - SIL 2 Dual Channel Inputs Example F



SIL 2 Input Data

Always keep channel A and channel B input data separate. This example illustrates one method to separate channel A and channel B data in your application.

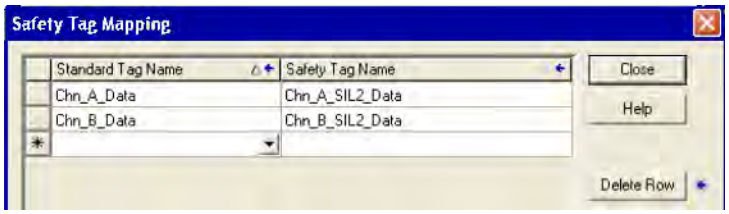
Follow all rules for 1756 I/O modules and 1794 FLEX™ I/O modules as defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.



IMPORTANT Do not perform safety-specific functions within these routines. Safety evaluation must be handled within the 1756 GuardLogix safety task.

Transfer SIL 2 Data Into the Safety Task

To transfer channel A and channel B SIL 2 safety data into the GuardLogix safety task, use the safety-tag mapping functionality in the Logix Designer application. The tag names that are used here are for example purposes. Implement and follow naming conventions that are appropriate for your application.



To use the safety-tag mapping feature, select Map Safety Tags from the Logic menu in the Logix Designer application.

SIL 2 Outputs With SIL 3 Guard I/O Output Modules

Follow these guidelines for SIL 2 outputs:

- Guard I/O™ output modules that are used for SIL 2 safety outputs must be configured for dual channel operation.
- The following Guard I/O output modules are approved for use in SIL 2 applications.
  - 1732DS-IB8XOBV4
  - 1791ES-IB8XOBV4
  - 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  - 1791DS-IB4XOW4
  - 1791DS-IB8XOB8
  - 1734-OB8S
- The following output modules are approved for use in SIL 2 applications that use a single channel safety output.
  - 1734-OB8S
  - 1732ES-IB12XOB4
  - 1732ES-IB8XOB8

SIL 2 Outputs With 1756 or 1794 SIL 2 Output Modules

When using these SIL 2-rated output modules, you are required to configure your SIL 2 safety outputs as GuardLogix-produced safety tags to comply with the dual channel requirements of EN 50156.

Create produced safety tags with the SIL 2 outputs that your application requires. GuardLogix produced/consumed safety tags require the first member to be allocated for diagnostics. The first member of a produced/consumed safety connection must be a data type called CONNECTION_STATUS. This example shows a SIL 2 tag with two INT and two BOOL members. Use these SIL 2 safety tags to control the 1756 or 1794 SIL 2 outputs directly.

Name	Alias For	Base Tag	Data Type	Class	Description	External Access	Constant	Style
SIL2_Outputs			SIL_2_Produced	Safety		Read/Write	☐	
SIL2_Outputs.Connection_Status			CONNECTION_STA	Safety		Read/Write		
SIL2_Outputs.SIL2_TempA			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_TempB			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_Valve1			BOOL	Safety		Read/Write		Binary
SIL2_Outputs.SIL2_Valve2			BOOL	Safety		Read/Write		Binary

In this example, a consumer for the produced tag is not shown. The connection status shows a fault if you don't configure a consumer. However, in this type of configuration, you are not required to monitor the connection status of the produced tag so the fault is not a concern.

Follow all rules for 1756 I/O modules and 1794 FLEX™ I/O modules as defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

Safety Functions Within the GuardLogix 5570 Safety Task

Follow these guidelines for using SIL 2 and SIL 3 safety functions within the safety task:

- All available safety application instructions can be used.
- SIL CL3 safety input modules (that is, Guard I/O modules) can be used with single-channel configuration for SIL 2 safety functions.
- Use of the safety task signature and safety-locking the application is recommended. The safety task signature is required to operate in a SIL 3 safety function.

IMPORTANT You must not use SIL 2 data to control a SIL 3 output directly.

Notes:

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

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 can test, untest, or cancel the edits.

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

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

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

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.

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 re-downloaded.

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, and the hardware and firmware must be compatible for partnership to be established.

pending edit 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.

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

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.

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) When communicating over a network, this value is the maximum amount of time between subsequent production of input data.

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.

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 3 safety instruction signature for use in safety-related functions.

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

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

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

safety network number (SNN) Uniquely identifies a network across all networks in the safety system. The end user is responsible is 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.

safety program A safety program has all the 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 routine A safety routine has all the 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 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 the attributes of a standard tag except that the GuardLogix® controller provides mechanisms that are certified to 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 the 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 task signature A value, which is calculated by the firmware, 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.

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 activator Reaction Times and the Controller Reaction Time.

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.

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

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

Numerics

1734-AENT 11, 19
1756-A10 11
1756-A10XT 11
1756-A13 11
1756-A17 11
1756-A4 11
1756-A5XT 11
1756-A7 11
1756-A7XT 11
1756-CN2 11, 19
1756-CN2R 11, 19
1756-CN2RXT 11, 19
1756-DNB 11, 19
1756-EN2F 11, 19
1756-EN2T 11, 19
1756-EN2TR 19
1756-EN2TXT 11, 19
1756-EN3TR 19
1756-ENBT 11, 19
1756-PB72 11
1756-PB75 11
1768-CNB 19
1768-CNBR 19
1768-ENBT 19
1784-CF128 11
1784-SD1 11, 12
1784-SD2 11, 12

A

Add-On Instruction
certify 57
instruction signature 60
safety instruction signature 60
agency certifications 12
application development basics 40
application program
changing 46
See program

B

burner-related safety functions 83

C

Category 4 9
certifications 12
changing your application program 46
chassis
catalog numbers 11
hardware overview 16
checklist
GuardLogix controller system 20
program development 74
SIL 3 inputs 73
SIL 3 outputs 73
CIP Safety protocol
definition 87
overview 18
routable system 25
commissioning life cycle 40
communication modules
catalog numbers 11, 12
hardware overview 19
configuration signature 22
connection status 49
CONNECTION_STATUS
data type 49
control and information protocol
definition 7
control function
specification 41
ControlNet bridge module
hardware overview 19

D

DeviceNet Safety
communication overview 20
DeviceNet scanner interface module
hardware overview 19
diagnostic coverage
definition 7

E

EN50156 83
EtherNet/IP
communication overview 19
EtherNet/IP communication interface module
hardware overview 19
European norm.
definition 7

F

faults
nonrecoverable controller faults 51
nonrecoverable safety faults 51
overriding 51
recoverable 51, 87
firmware revisions 11
forcing 45

G

get system value (GSV)
definition 7
GSV instructions 50

H

hard faults
recovery 51
human-to-machine interfaces
use and application 35 - 36

I

I/O modules
replacement 23 - 24
IEC 61508
Safety Integrity Level 3 (SIL 3) certification 9, 61
inhibiting a module 46
instruction signature 60
definition 87
interface
HMI use and application 35 - 36
ISO 13849-1 9

L

ladder logic safety instructions 54
Logix components
SIL 3-certified 11
Logix system reaction time
calculating 65

M

mapping tags 38
memory card 11, 12

N

nonrecoverable controller faults 51, 87
nonrecoverable safety faults 51, 87
restarting the safety task 51

O

offline edits 46
online
definition 87
online editing 45, 47
output delay time 22
overlap
definition 87
ownership 22

P

partnership
definition 87
peer-to-peer communication 19
pending edits 45
Performance Level
definition 7
period task
definition 87
PLe 9
power supplies 11, 12
hardware overview 16
primary controller
definition 87
hardware overview 15
probability of failure on demand (PFD) 13
definition 7
probability of failure per hour (PFH) 13
definition 7
program
checklist 74
download 44
editing life cycle 48
indentification 41
offline editing 46
online editing 47
upload 45
verification 42
project
confirmation 43
project verification test 42, 62
proof tests 9

Q

qualifying standard data 38

R

reaction time
calculating for system 65
safety task 14
system 14, 89
recoverable faults 51, 87
reliability burden 14
requested packet interval
definition 87
range 34

S

safety application instructions
definition 88
safety certifications and compliances 12
safety concept
assumptions 39
safety consumed tags
safety network number 28
safety functions
CIP Safety I/O 21
Safety Output 22
safety instruction signature 60
definition 88
Safety Integrity Level (SIL)
compliance distribution and weight 14
function example 11
policy 9 - 14
Safety Integrity Level (SIL) 3 certification
Logix components 11
TÜV Rheinland 9
user responsibilities 9
Safety Integrity Level 3 (SIL 3) certification 9, 61

safety network number 26
definition 88
manual assignment 26
out-of-box modules 28
safety consumed tags 28
safety partner
definition 88
hardware overview 15
location 15
safety program 36
definition 88
safety routine 36
definition 88
safety tags 37
definition 88
valid data types 37
safety task
definition 88
execution 34
overview 33
priority 69
reaction time 14, 88
watchdog time 69
safety task period 14
definition 88
limitations 33
overview 14
safety task signature
definition 88
deleting 42
restricted operations 42
safety task watchdog 14
definition 88
modifying 14
overview 14
setting 14
timeout 33
safety-locking 44
default 44
passwords 44
restricted operations 44
Secure Digital (SD) card 11, 12
set system variable (SSV) instruction 50
signature history 61
SIL 2
EN50156 83
software
changing your application program 46
Studio 5000 environment 11, 12
system reaction time 14
calculating 65

T

tags
produced/consumed safety data 37
Safety I/O 37
see also safety tags
timeout multiplier 67
definition 89

U

unique node reference
defined 25

W

watchdog time 69

X

XT-components 11

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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

Allen-Bradley, Armor, ArmorBlock, CompactBlock, Compact I/O, CompactLogix, ControlLogix, ControlLogix-XT, expanding human possibility, FactoryTalk, FLEX, Guard I/O, GuardLogix, GuardLogix-XT, Kinetix, Logix5000, POINT Guard I/O, POINT I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLogix 5000, SLC, SmartGuard, Studio 5000, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

CIP, CIP Safety, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

Microsoft and Excel are trademarks of Microsoft Corporation.

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

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

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44) (1908) 838-800

Publication 1756-RM099H-EN-P - October 2024
Supersedes Publication 1756-RM099G-EN-P - May 2018

Copyright © 2024 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.