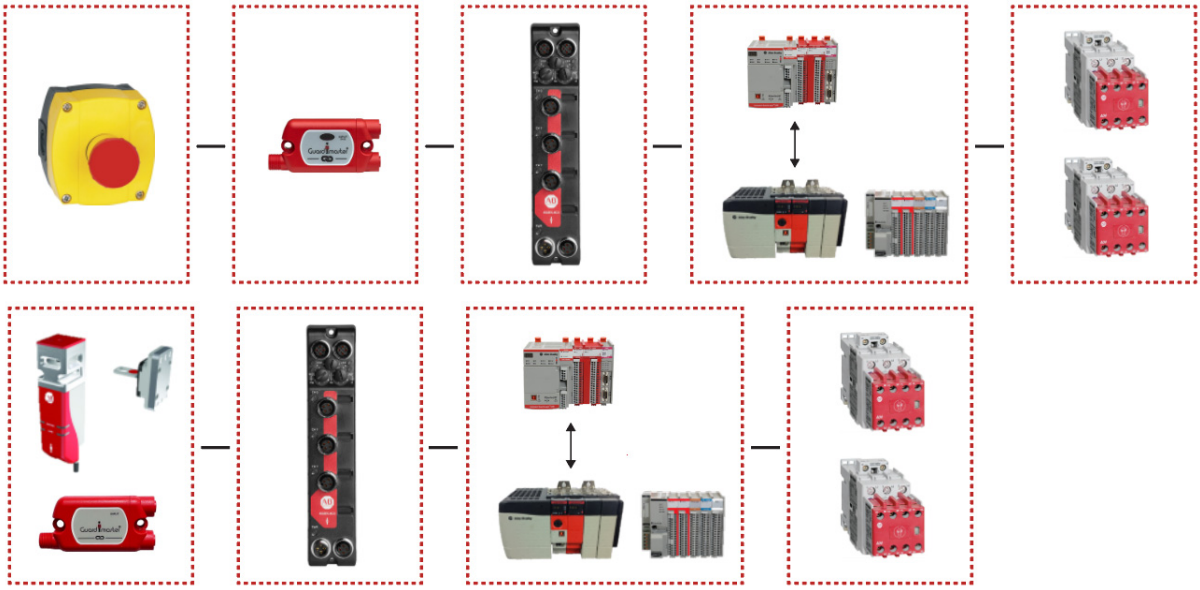
Application Technique

Original Instructions

GuardLink Emergency Stop and Door Monitoring Via GuardLogix Safety Controller Safety Function

Products: 800F E-stop, 440G-MZ Interlocking Switch, 440S GuardLink Taps, 432ES-IG3 GuardLink Interface, GuardLogix 5580 or Compact GuardLogix 5380 Controller, Compact 5000 I/O Safety Modules, 100S-C Contactors

Safety Rating: Cat. 3, PLd to ISO 13849-1:2023



Topic	Page
Important User Information	2
General Safety Information	3
Introduction	4
Use Sample Project Files	4
Safety Function Realization: Risk Assessment	5
Safety Functions	5
Safety Function Requirements	6
Bill of Materials	7
Setup and Wiring	8
Configuration	10
Programming	14
Calculation of the Performance Level	20
Verification and Validation Plan	22
Additional Resources	23

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

General Safety Information

Contact Rockwell Automation to learn more about our safety risk assessment services.

IMPORTANT This application example is for advanced users and assumes that you are trained and experienced in safety system requirements.

ATTENTION: Perform a risk assessment to make sure that all task and hazard combinations have been identified and addressed. The risk assessment can require additional circuitry to help reduce the risk to a tolerable level. Safety circuits must consider safety distance calculations, which are not part of the scope of this document.

Safety Distance Calculations

ATTENTION: While safety distance or access time calculations are beyond the scope of this document, compliant safety circuits must often consider a safety distance or access time calculation.

Non-separating safeguards provide no physical barrier to help prevent access to a hazard. Publications that offer guidance for calculating compliant safety distances for safety systems that use non-separating safeguards, such as light curtains, scanners, two-hand controls, or safety mats, include the following:

- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

Separating safeguards monitor a movable, physical barrier that guards access to a hazard. Publications that offer guidance for calculating compliant access times for safety systems that use separating safeguards, such as gates with limit switches or interlocks (including SensaGuard™ switches), include the following:

- EN ISO 14119:2013 (Safety of Machinery – Interlocking devices associated with guards - Principles for design and selection)
- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

In addition, consult relevant national or local safety standards to verify compliance.

Introduction

This safety function application technique explains how to wire, configure, and program an 800F E-stop and 440G-MZ safety interlock switch with the 432ES-IG3 GuardLink® interface to a Compact GuardLogix® controller and Compact 5000™ I/O safety modules. This application technique describes two safety functions:

1. If the E-stop is pressed or a fault is detected in the safety function, the GuardLogix controller de-energizes a redundant pair of 100S-C contactors.
2. If the interlock switch is open or unlocked, or a fault is detected in the safety function, the GuardLogix controller de-energizes a redundant pair of 100S-C contactors.

The 432ES-IG3 GuardLink interface guard locking output is not safety rated. The process control system (PCS) controls the locking of the 440G-MZ safety interlock switch with a standard output that helps prevent the access gate from being opened. The process control system can limit the triggering of the interlock switch safety function to times that are least disruptive to the guarded process. Any details about how the PCS is programmed or configured to perform its tasks is beyond the scope of this document.

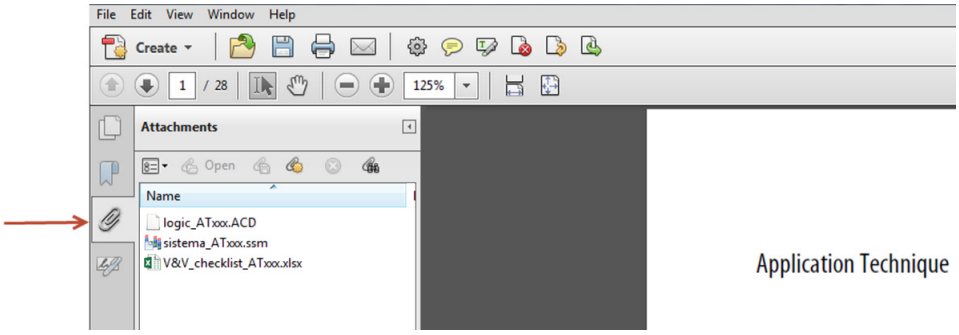
This example uses a Compact GuardLogix 5069-L3100ERMS2 controller, but you can substitute a GuardLogix controller that supports the safety rating that is demonstrated in this safety function application technique. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) calculations that are shown later in this document must be recalculated if different products are used.

Use Sample Project Files

Sample project files (ACD, SISTEMA, and Verification and Validation checklist) are attached to this document to help you implement this safety function.

To access these files, follow these steps.

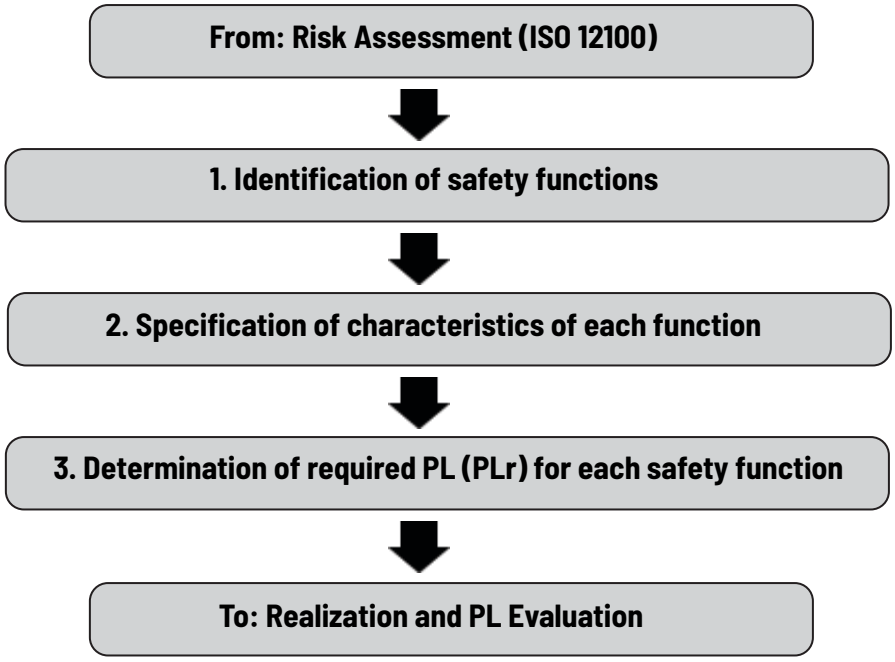
1. If you are viewing the PDF file in a browser and do see not the Attachments link, download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link.
3. Right-click and save the desired file.



4. Open the file in the appropriate application.

Safety Function Realization: Risk Assessment

The Performance Level required (PLr) is the result of a risk assessment and refers to the amount of the risk reduction to be conducted by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. In this application, the Performance Level required by the risk assessment is category 3, Performance Level d (cat. 3, PLd), for each safety function. A safety system that achieves cat. 3, PLd, or higher, can be considered control reliable. Each safety product has its own rating and can be combined to create a safety function that meets or exceeds the PLr.



Safety Functions

This application technique includes three Safety Functions:

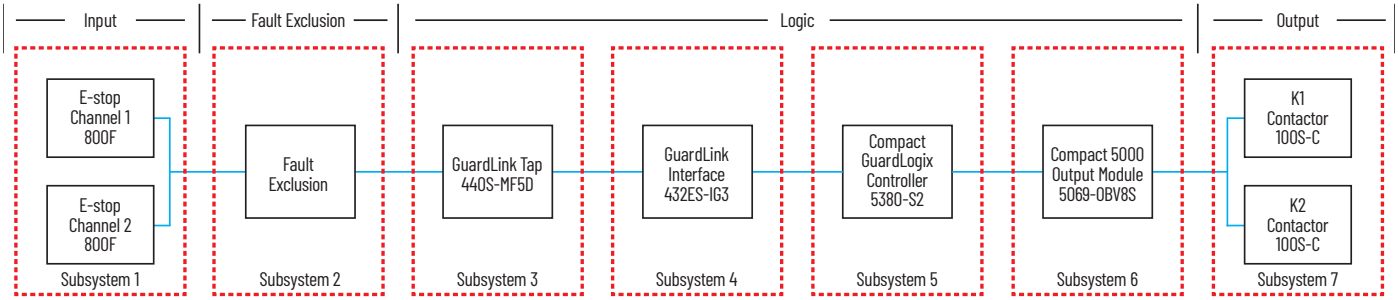
1. Safety-related stop function initiated by an emergency stop.
2. Safety-related stop function initiated by a safeguard.
3. Prevention of an unexpected startup.

In this example, safety functions 2 and 3 are analyzed as one safety function.

Safety Function Requirements

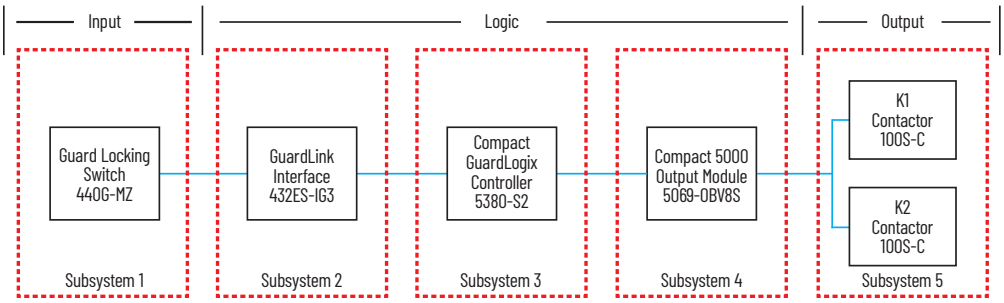
Safety-related Stop Function Initiated by an Emergency Stop

The emergency stop (E-stop) function is complementary to other safeguards on the machine. When the E-stop is pressed, the safety system de-energizes the two safety contactors, which removes power from the motor that generates hazardous motion. Power removal causes the hazardous motion to coast uncontrolled to a stop (category 0 stop). Hazardous motion cannot be restarted until the E-stop is released and the Reset button on the HMI is pressed and released. The contactor coils energize and close their N.O. safety contacts. After the safety contactors are energized, pressing the HMI Start button starts the motor. A detected fault in the safety system opens the two safety contactors to create a category 0 stop.



Safety-related Stop Function Initiated by a Safeguard

A fence guards a production process where workers need access to the machines for inspection, operational, or maintenance purposes. An access gate that a safety interlock monitors is provided for these purposes. The safety system de-energizes the motor that drives a hazard in the access area whenever the access gate is unlocked or opened. The safety system helps prevent the motor from being re-energized before the gate is closed and the Reset button is pressed and released. If the gate is opened at the wrong time, de-energizing the motor causes downtime and loss of product.



IMPORTANT ISO 14119:2013 8.4 has general requirements for the release of a guard locking device when guard locking is used for risk reduction. The 432ES-IG3 GuardLink interface guard door locking is suitable for protecting the process and carries no safety rating for risk reduction.

The process control system (PCS) keeps the access gate locked at times when de-energizing the motor would cause disruption. Access is requested by making an unlock request. The PCS then unlocks the gate at a time when de-energizing the motor would be non-disruptive to the process. Once the gate is unlocked or opened, the motor is de-energized and prevented from restarting while the gate is open. The PCS can only resume the process after the operator has:

1. Exited the hazardous area and closed the gate.
2. Canceled the unlock request.
3. Pressed and released the reset button.

The safety functions in this application technique each meet or exceed the requirements for category 3, Performance Level d (cat. 3, PLd), per ISO 13849-1 and control reliable operation per ANSI B11.19.

Considerations for Safety Distance and Stopping Performance

Based on the selection of a 440G-MZ safety interlock switch, the risk assessment determines if a safety distance calculation is required. Typically, a safety distance calculation is required if a non-separating sensor subsystem (such as a light curtain) is selected for the safety function. Since the locking function is not safety rated, a safety distance calculation should be considered. If a safety distance calculation is required for this safety function, the following documents can be referenced:

- Machinery SafeBook 5 – Safety related control systems for machinery, publication SAFEBK-RM002
- Safety Function: Light Curtain Products: Light Curtain GuardLogix® Controller, publication SAFETY-AT191
- GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012

Bill of Materials

This application technique uses these products.

Cat. No.	Description	Quantity
432ES-IG3	432ES GuardLink EtherNet/IP™ interface, 3-channel safety input	1
440S-MF5D	5-pin EMSS (Electromechanical Safety Switch) GuardLink-enabled tap	1
440S-PF5D	5-pin GuardLink passive tap (for use with GuardLink-embedded devices)	1
440G-MZS20UNRJ	Guard locking switch - Power to Release, 6 in. (150 mm) pigtail, M12 male 5-pin QD	1
800F-1YMD51	800F enclosed E-stop station, twist-to-release yellow plastic, M12 male 5-pin QD	1
1585D-M4TBJM-5	Ethernet Cable Cat5e, 100 Mbit/s, 4 Conductors, M12, Straight Male, Standard, RJ45, Straight Male	1
889D-F4AC-5	Cordset: Quick disconnect 16.4 ft (5 m) cable, yellow, M12 female (4-pin), no connector	1
889D-F4NEDM-1	Patchcord: M12, straight socket, 4-pin, red, straight plug, 3.3 ft (1 m), 18 AWG	2
889D-F5NCDM-1	Patchcord: M12, straight socket, 5-pin, red, straight plug, 3.3 ft (1 m), 22 AWG	1
898D-418U-DM2	GuardLink terminator	1
5069-IB8S	Compact 5000 I/O 8-channel 24V DC safety input module	1
5069-OBV8S	Compact 5000 I/O 8-channel 24V DC safety configurable output module	1
5069-RTB18-SCREW	5069 Compact I/O™ 18 pins screw-type terminal block	2
100S-C09EJ23C	100S-C safety contactor, 9 A, 24V DC electronic coil	2
1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 120/240V AC input	1

Choose one of the following safety-controller hardware groups.

Controller	Cat. No.	Description	Quantity
GuardLogix 5580 [1]	1756-L81ES	GuardLogix processor, 3 MB standard memory, 1.5 MB safety memory	1
	1756-L82ES	GuardLogix processor, 5 MB standard memory, 2.5 MB safety memory	
	1756-L83ES	GuardLogix processor, 10 MB standard memory, 5 MB safety memory	
	1756-L84ES	GuardLogix processor, 20 MB standard memory, 6 MB safety memory	
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A7	Seven-slot ControlLogix® chassis	1
	5069-AENTR	5069 Compact I/O slim EtherNet/IP adapter	1
Compact GuardLogix 5380 - SIL 2	5069-L306ERS2	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory	1
	5069-L306ERMS2		
	5069-L310ERMS	Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory	
	5069-L310ERMS2		
	5069-L320ERS2	Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory	
	5069-L320ERMS2		
	5069-L330ERS2	Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory	
	5069-L330ERMS2		
	5069-L340ERS2	Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory	
	5069-L340ERMS2		
	5069-L350ERS2	Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory	
	5069-L350ERMS2		
	5069-L380ERS2	Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory	
	5069-L380ERMS2		
	5069-L3100ERS2	Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	
	5069-L3100ERMS2		
Compact GuardLogix 5380 - SIL 3	5069-L306ERMS3	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory	1
	5069-L310ERMS3	Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory	
	5069-L320ERMS3	Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory	
	5069-L330ERMS3	Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory	
	5069-L340ERMS3	Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory	
	5069-L350ERMS3	Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory	
	5069-L380ERMS3	Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory	
	5069-L3100ERMS3	Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	

[1] If your PLr is SIL 3/PLe, use a GuardLogix 5580 controller with a safety partner, Cat. No. 1756-L8SP.

Setup and Wiring

For detailed information on how to install and wire the products in this application technique, refer to the publications that are listed in the Additional Resources on page 23.

System Overview

With the process running, the operator presses the E-stop. When the E-stop is pressed, the 440S GuardLink tap brings GuardLink channel 0 of the 432ES-IG3 GuardLink interface status low (0).

With the process running and the gate closed and locked, when the operator makes an unlock request, the process control system (PCS) determines when access would be non-disruptive. The 432ES-IG3 sends the standard rated unlock signal to the 440G-MZ guard locking switch. When the gate is unlocked, the GuardLink-enabled 440G-MZ safety interlock switch brings GuardLink channel 0 of the 432ES-IG3 GuardLink interface status low (0).

The safety controller monitors the GuardLink Channel 0 Status input. When the channel status transitions low (0), the safety task responds by removing the safety output enable. A certified function block called Configurable Redundant Output (CROUT) controls redundant 100S-C

safety contactors and monitors mechanically linked feedback to provide diagnostic coverage. The CROUT turns off 5069-OBV8S safety module outputs that de-energize a pair of safety contactors (K1 and K2). The contactors control hazardous energy using redundant-series wiring. Power to the hazard is removed only if one of the contactors operates properly. A feedback circuit is wired through mechanically linked, normally closed contacts and back to an input on the 5069-IB8S module to monitor both contactors for proper operation. Wiring feedback to a safety input is not required for functional safety but is an industry best practice.

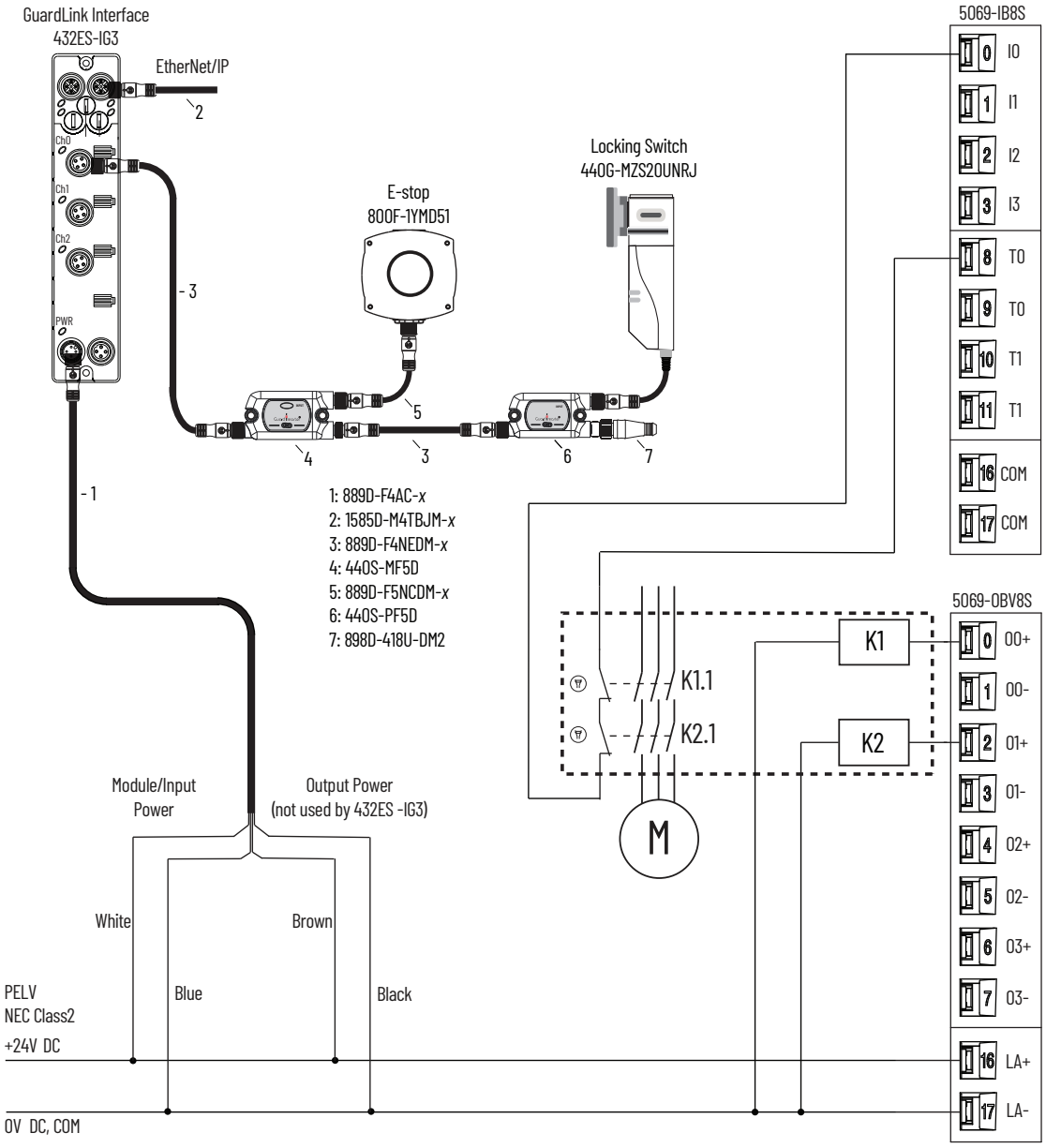
If the PCS has not already stopped the motor, it now coasts to a stop.

When the operator has completed the work tasks, and no one remains in the guarded area, the gate is closed. The operator removes the unlock request. The PCS sends the gate lock command to the guard locking switch via the GuardLink interface.

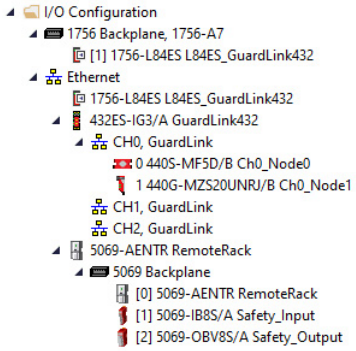
GuardLink channel 0 status transitions to high (1) when the E-stop is in the run ready position, the gate closed and locked, and no input faults are detected. The Reset button is pressed and released and if no system faults are detected, the safety controller energizes the K1 and K2 contactors.

The system uses a reset signal mapped from standard logic for the reset of faults and safety outputs.

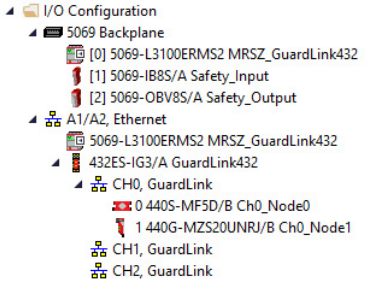
Electrical Schematic



Network Architecture



GuardLogix 5580 Controller with remote Guard I/O (1)



GuardLogix 5380 Controller with local Guard I/O ™

(1) When using a GuardLogix 5580 controller, slot 2 is reserved for the safety partner, which is required for SIL 3/PLe applications.

Configuration

The GuardLogix controller is configured by using the Studio 5000 Logix Designer® application, version 34 or later. You must create a project and add the appropriate safety I/O modules. The integrated Ethernet/IP port on the GuardLogix controller is used, so no Ethernet module is required. A detailed description of each step is beyond the scope of this document. Knowledge of the Logix Designer application is assumed.

For a Studio 5000 Logix Designer project file that you can import into your own project, see the attached ACD file. For instructions on how to access the attachments, see Use Sample Project Files on page 4. The attached ACD file includes a GuardLogix 5380 controller, but if you choose a 5580 controller, you can change the controller in the Logix Designer program.

Minimum Version	Product
Logix Designer 34	GuardLink Interface: 432ES-IG3
FactoryTalk® Linx 6.30	

Create a Project with a GuardLogix Controller

If you are not using the attached ACD file, follow these steps to create a project. For instructions on how to access the attachments, see Use Sample Project Files on page 4.

Configure the GuardLogix Controller

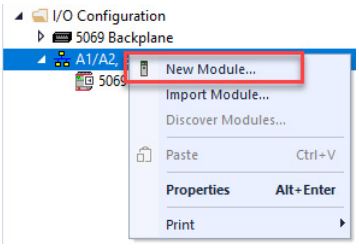
1. In the Logix Designer application, create a project with a GuardLogix controller.

IMPORTANT If you use a GuardLogix 5580 controller, you must configure the safety level of the controller on the Safety tab of the Module Properties dialog box. The default setting is SIL 2, PLd. For SIL 3, PLe operation, you must have a 1756-L8SP Safety Partner installed to the right of the primary controller.

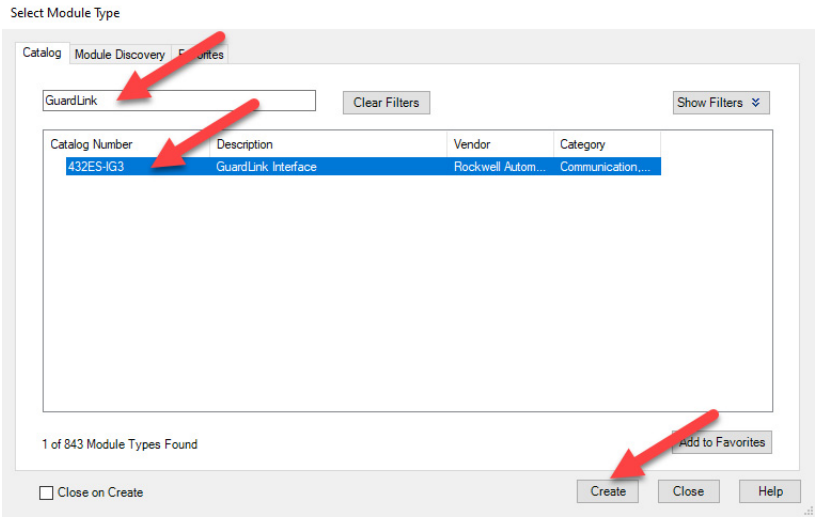
2. Set the IP address for the controller or any Ethernet communication modules, if used.
3. Add 5069-IB8S safety input modules to project.
   - Configure Input 0 to be Safety Pulse Test from Test Source 0.
4. Add 5069-OB8VS safety output modules to project.
   - Configure Outputs 0 and 1 to be Dual and Safety Pulse Test.
5. Configure the modules properly for your application.
   See the Additional Resources on page 23 for information on your I/O modules.

Configure the 432E-IG3 GuardLink Interface

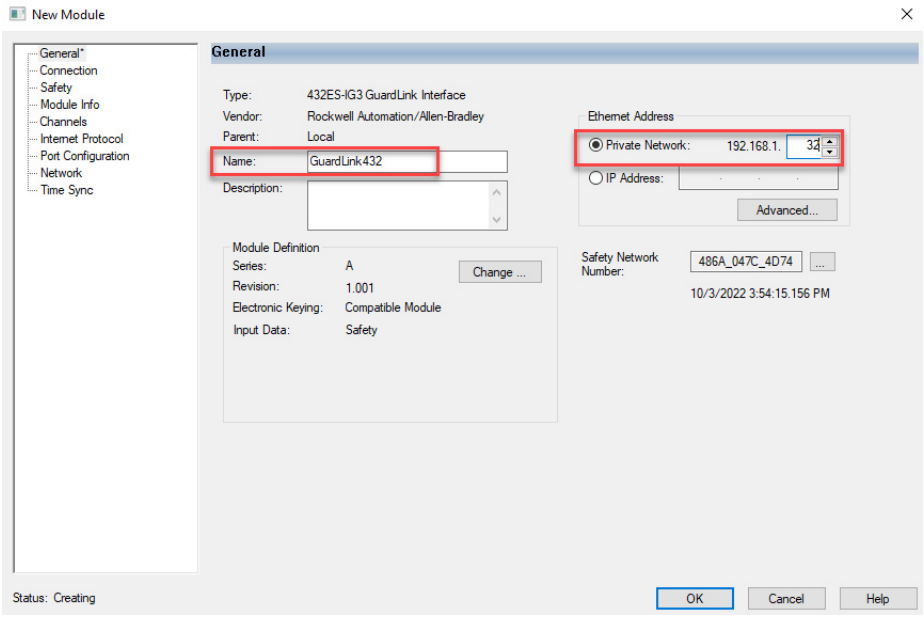
1. To add the GuardLink Interface to the project, in the I/O Configuration, right-click the Ethernet network and choose New Module.



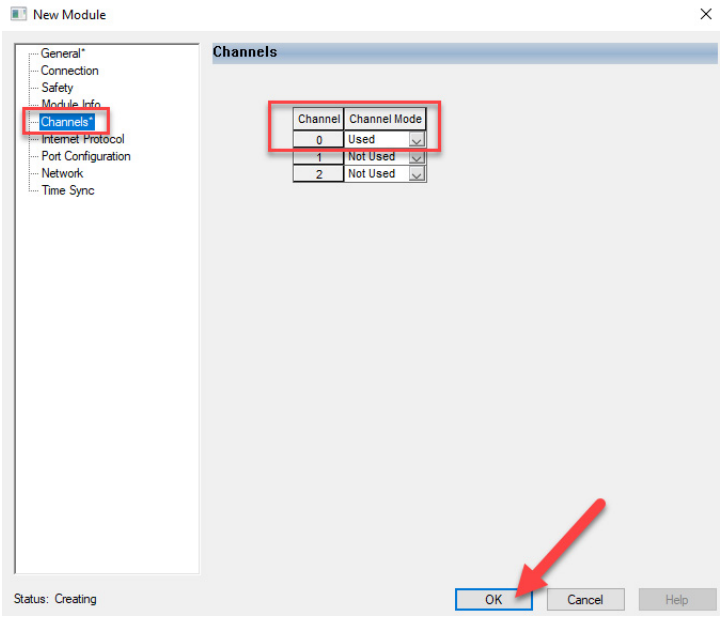
2. In the Select Module Type dialog box, do the following:
   a. Locate the GuardLink Interface by typing GuardLink in the search field.
   b. Select the GuardLink Interface.
   c. Click Create.



3. In the New Module dialog box, General Tab, do the following:
   a. Name the module (the example uses GuardLink432).
   b. Enter the IP address (the example uses 192.168.1.32).

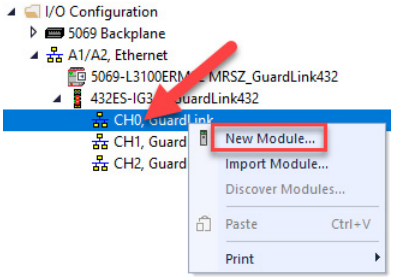


4. Click Channels
   a. Set Channel 0 to Used
   b. Click OK.

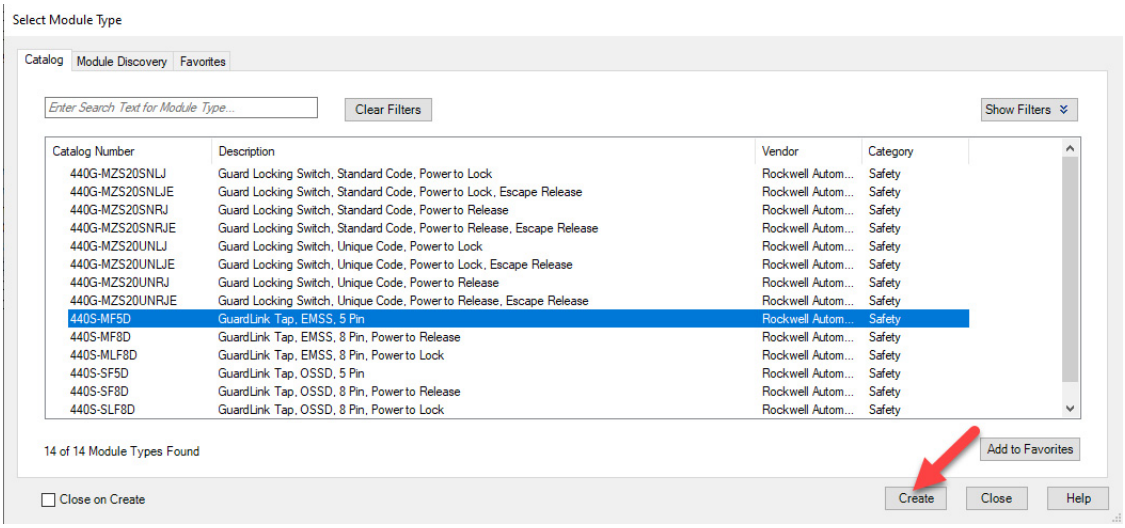


Configure GuardLink Channel 0

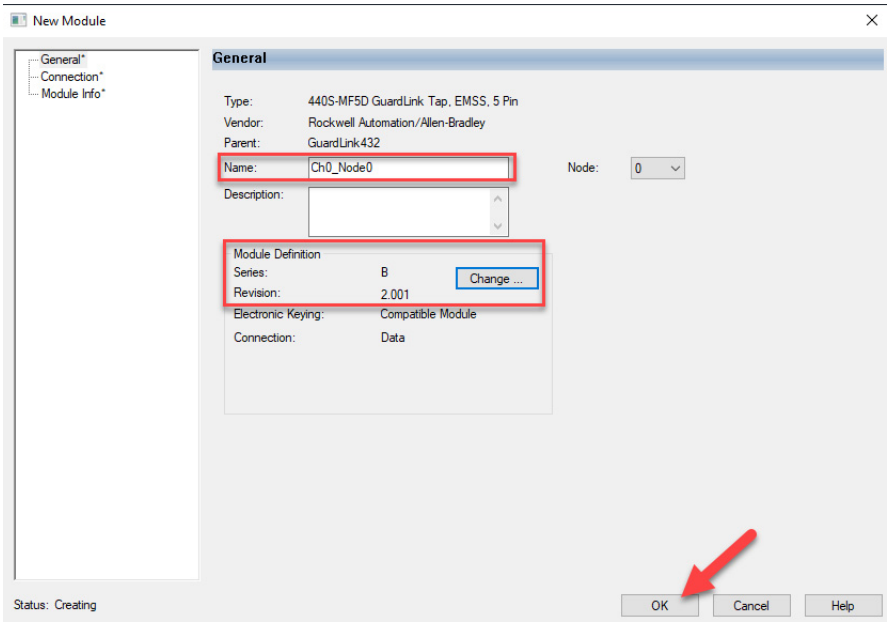
1. To configure GuardLink channel 0, in the I/O Configuration, under the 432ES-IG3, right-click "CH0, GuardLink" and choose New Module.



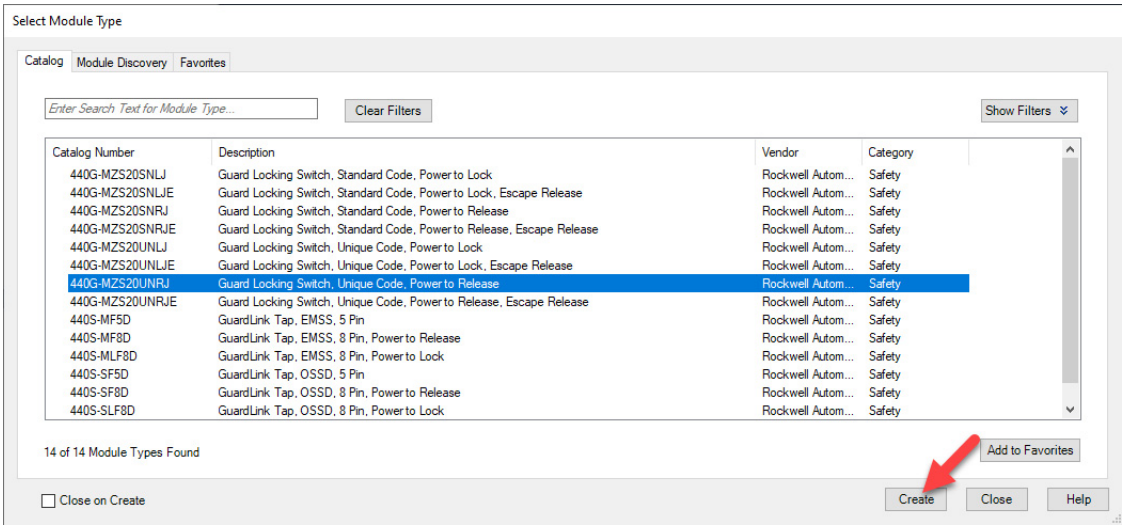
2. In the Select Module Type dialog box, do the following:
   a. Select the 440S-MF5D GuardLink tap to match the E-stop input.
   b. Click Create.



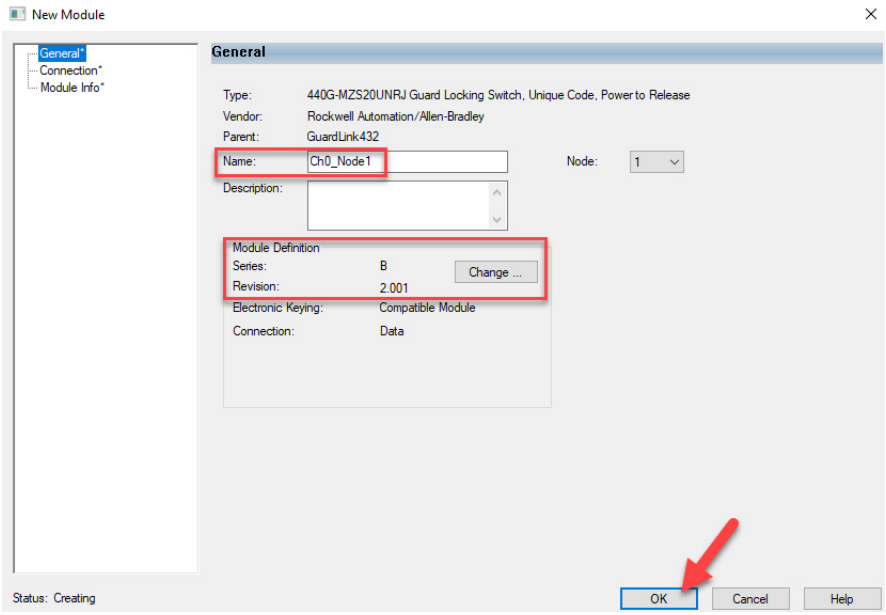
3. In the New Module dialog box, General Tab, do the following:
   a. Name the module (the example uses Ch0_Node0).
   b. Module Definition, Change, Series, and Revision (the example uses Series B, Revision 2.001).
   c. Click OK.



4. In the Select Module Type dialog box, do the following:
   a. Select the 440G-MZS20UNRJ Guard Locking Switch.
   b. Click Create.



5. In the New Module dialog box, General Tab, do the following:
   a. Name the module (the example uses Ch0_Node1).
   b. Module Definition, Change, Series and Revision (the example uses Series B, Revision 2.001).
   c. Click OK.

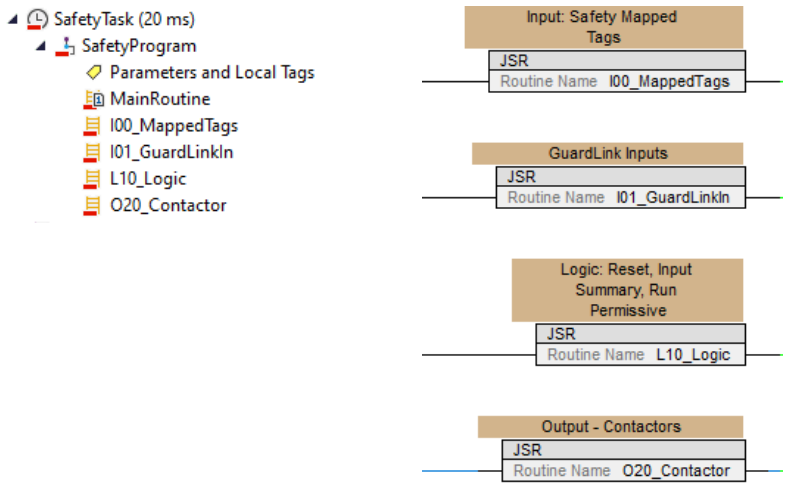


Programming

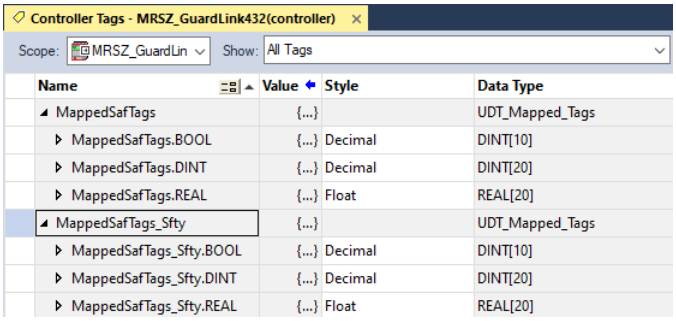
For controller logic that you can download to your controller, see the attached ACD file. For instructions on how to access the attachments, see Use Sample Project Files on page 4.

General Task Configuration — Safety

1. For modularity, and following application software guidance from safety standards, the safety zone program has been broken into routines for input, logic, and output. Be sure to call all routines from the MainRoutine.

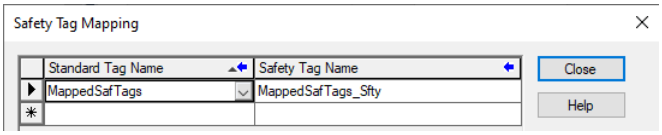


2. Map safety tags using user-defined data type (UDT)
   a. Create Standard and Safety tags of the same data type.

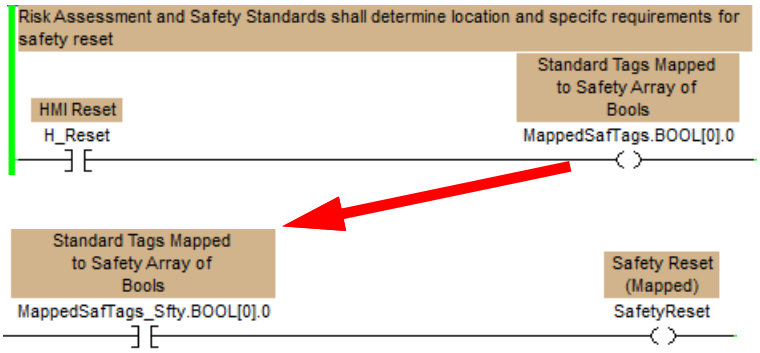


A best practice is to map a UDT of information. In this example, only 1 bit is used.

   b. In the Safety Tag Mapping dialog box, enter the tag name, click Close.



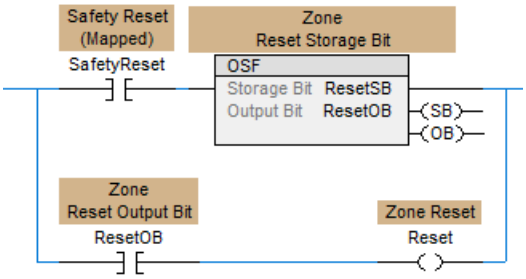
3. The Reset signal for safety logic is mapped from the standard logic with the mapped alias.



Falling Edge Reset

ISO 13849-1 stipulates that instruction reset functions must occur on falling edge signals. To comply with this requirement, a One Shot Falling (OSF) instruction is used on the reset rung. Then, the OSF instruction Output Bit tag is used as the reset bit for the STO output rung.

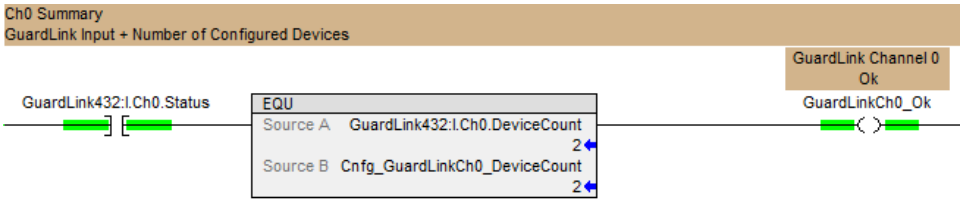
Risk Assessment and Safety Standards shall determine location and specific requirements for safety reset.



Input GuardLink – Safety

I.Ch0.Status is the safety input for GuardLink Channel 0.

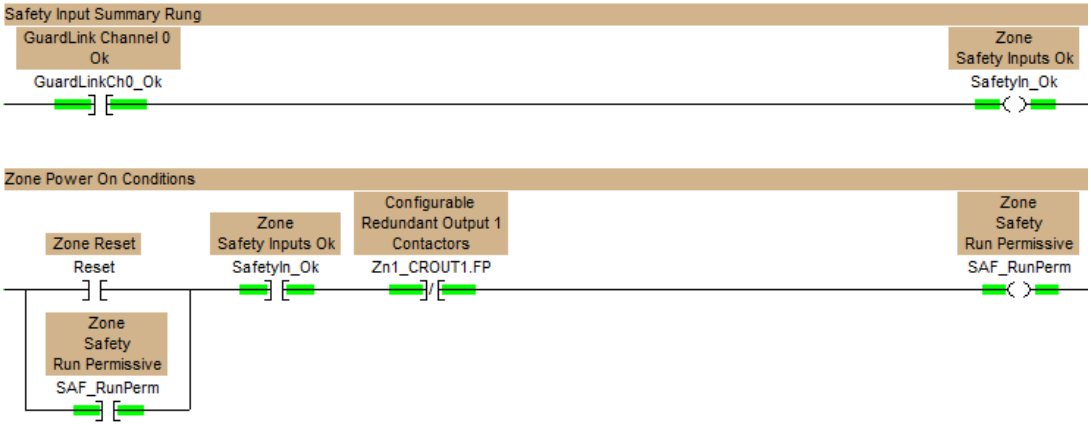
I.Ch0.DeviceCount counts the number of devices that are detected on the GuardLink channel. DeviceCount is used as an additional diagnostic to detect hardware manipulation of the GuardLink system.



Logic Main – Safety

The main logic contains:

1. Reset logic, previously discussed.
2. Safety Run Permissive logic, as shown.



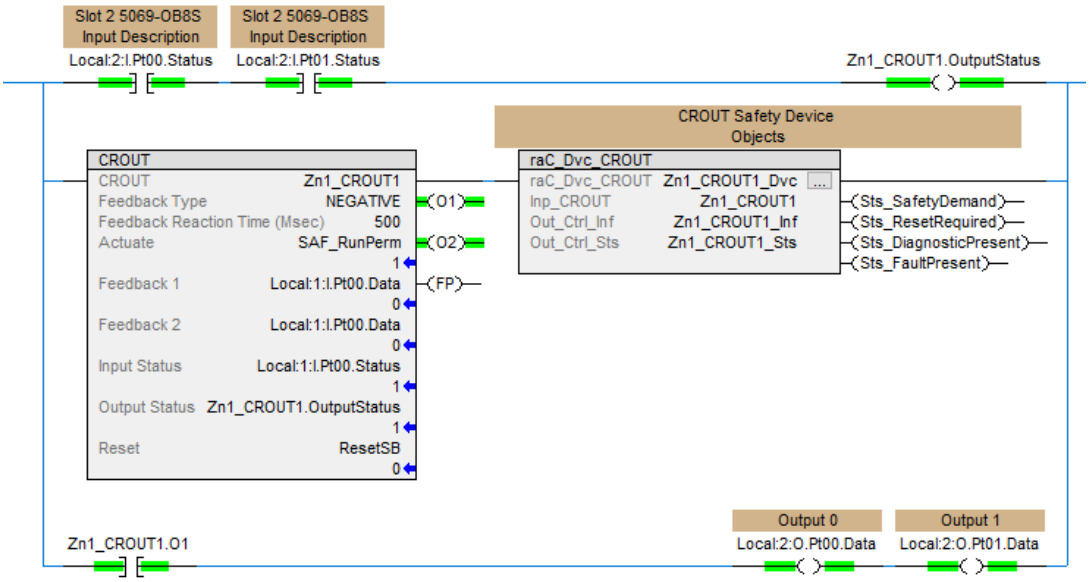
Output Contactors – Safety

Use the CROUT instruction for controlling two outputs and monitoring feedback and associated I/O status.

The use of one feedback for two contactors does not affect functional safety. The use of two feedbacks would provide troubleshooting indication of which contactor was causing the fault.

The optional raC_Dvc_CROUT Add-On Instruction (AOI) connects CROUT to the HMI Faceplate. (ME, SE, PV5000)

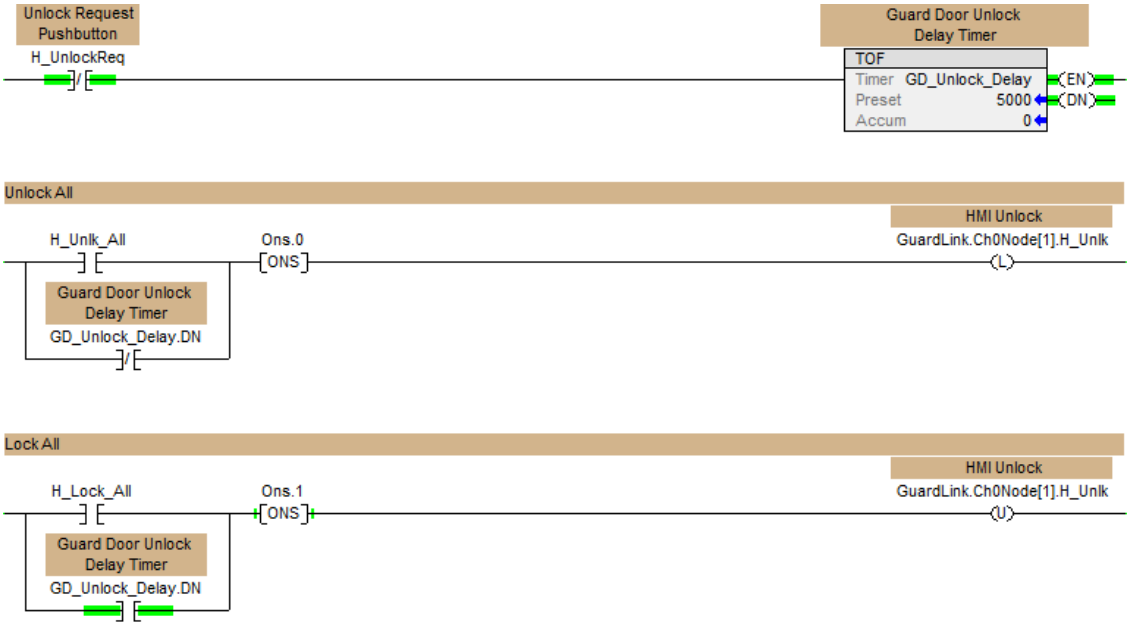
To find faceplate information, go to the Rockwell Automation Product Compatibility Download Center website (rok.auto/pcdc), and search for Safety Device Library.



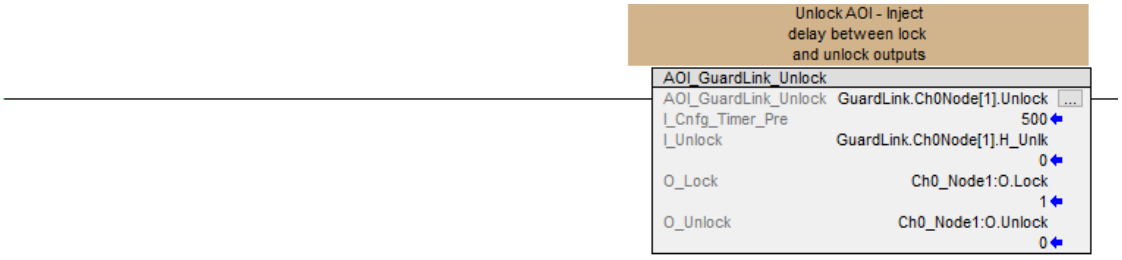
GuardLink Unlock – Standard

The standard outputs from the standard task control the GuardLink lock and unlock function and is not safety rated.

The example uses an unlock request that is connected to a timer to allow the machine to come to a stop before the guard door is unlocked. A placeholder has been created for connecting other lock and unlock commands.



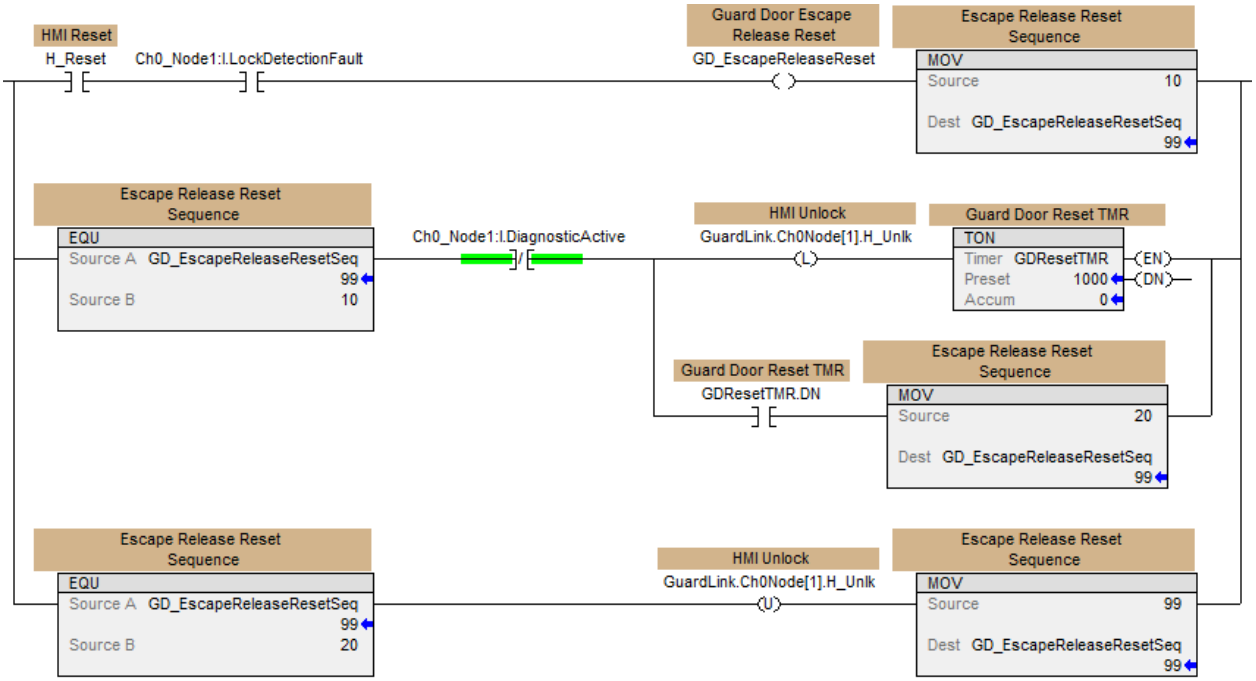
Each GuardLink node receives a separate lock (O.Lock) and unlock (O.Unlock) output signal. GuardLink requires a delay between the lock and unlock signal change. An AOI has been developed to facilitate programming.



The 440G-MZ GuardLink-enabled switch indicates an I.LockDetectFault when forced open either by an escape release or other mechanical means. To reset the fault, the following must happen in sequence:

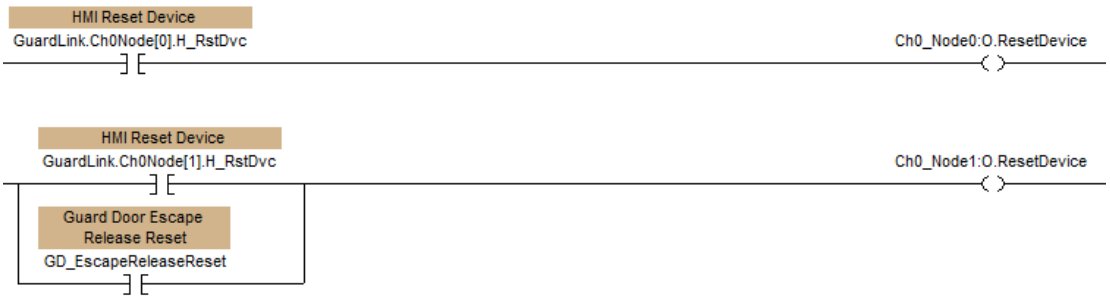
1. Reset device
2. Unlock
3. Lock

The following logic resets the lock detection fault with the machine reset.



GuardLink Reset – Standard

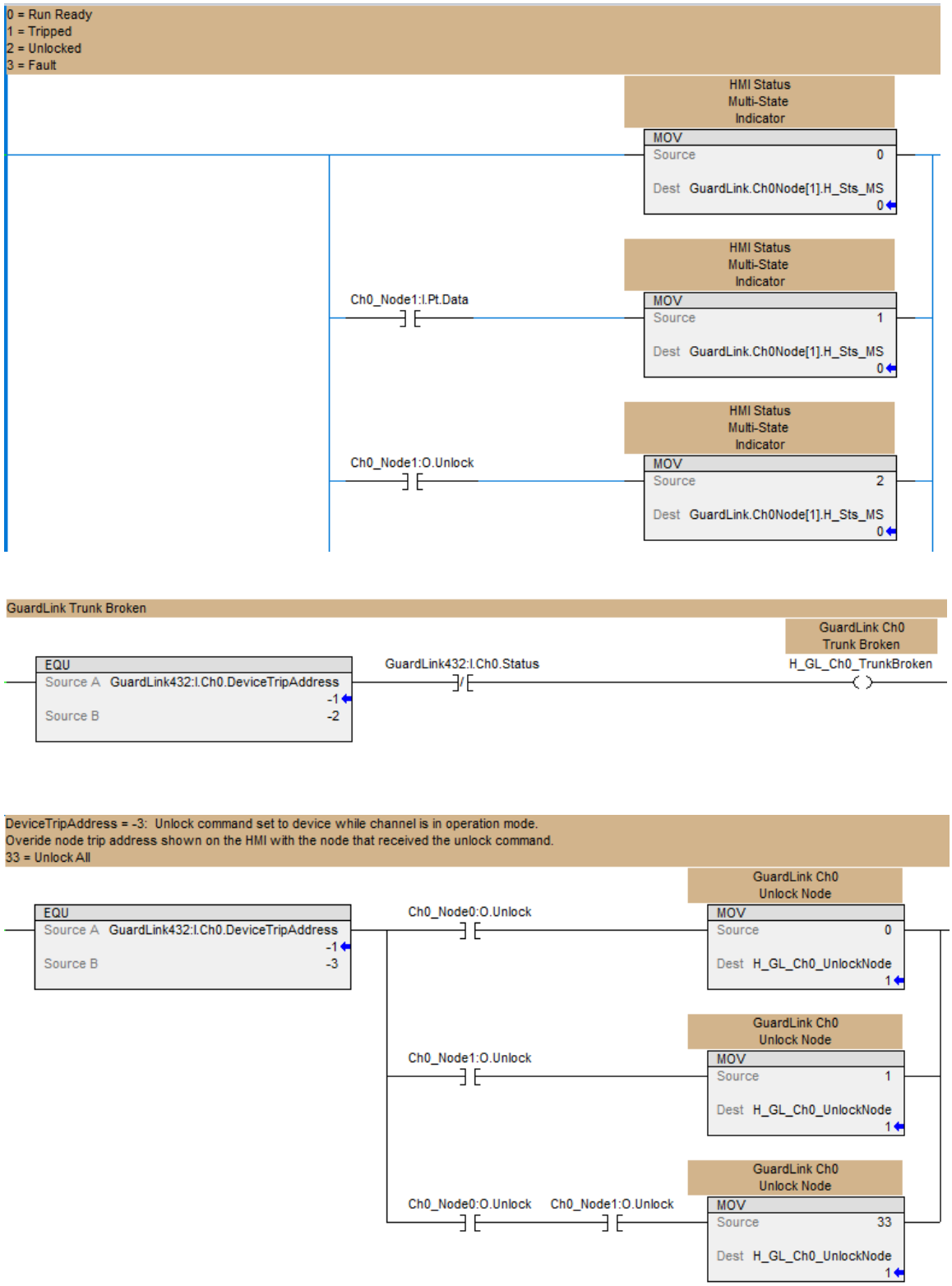
A reset can be used to cycle power to a device on the GuardLink. The example uses a reset from the HMI and as part of the escape release reset.



GuardLink HMI – Standard

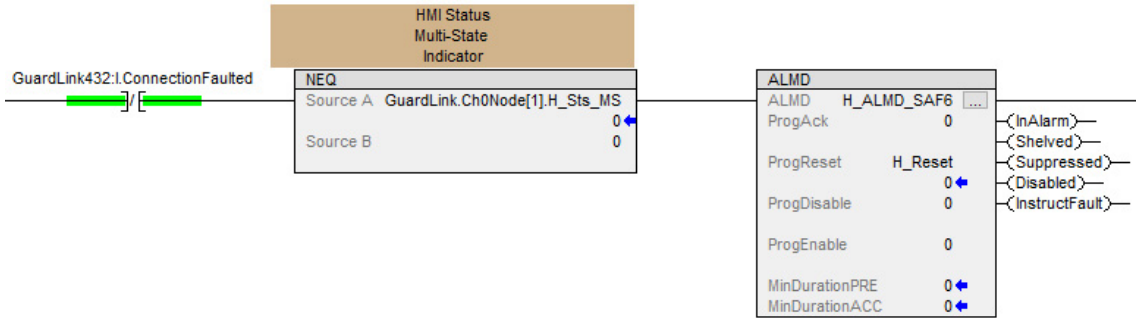
GuardLink can provide significant troubleshooting information to the HMI.

Device Multi-state indicators provide device status, truck broken, and unlock commanded.



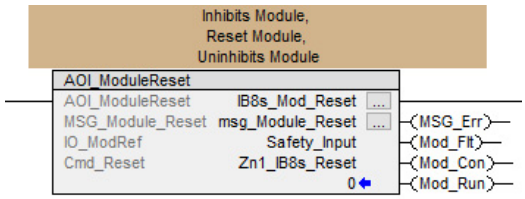
GuardLink Alarm – Standard

The GuardLink Alarm routine provides ALMD instructions to trigger FactoryTalk® Alarms and Events for HMI alarming.



Module Reset – Standard

The Module Reset routine provides AOI to inhibit, reset, and uninhibit safety modules. This feature is useful for clearing IO faults with a safety signature present.



Calculation of the Performance Level

When properly implemented, these safety functions can achieve a safety rating of category 3, Performance Level d (cat. 3, PLd), according to ISO 13849-1: 2015, as calculated by using the SISTEMA software PL calculation tool.

IMPORTANT To calculate the PL of your entire safety function, you must include the specific subsystems you chose. Depending on the devices you choose, the overall safety rating of your system will be different.

The SISTEMA file that is referenced in this safety function application technique is attached to this publication. For instructions on how to access the attachments, see Use Sample Project Files on page 4.

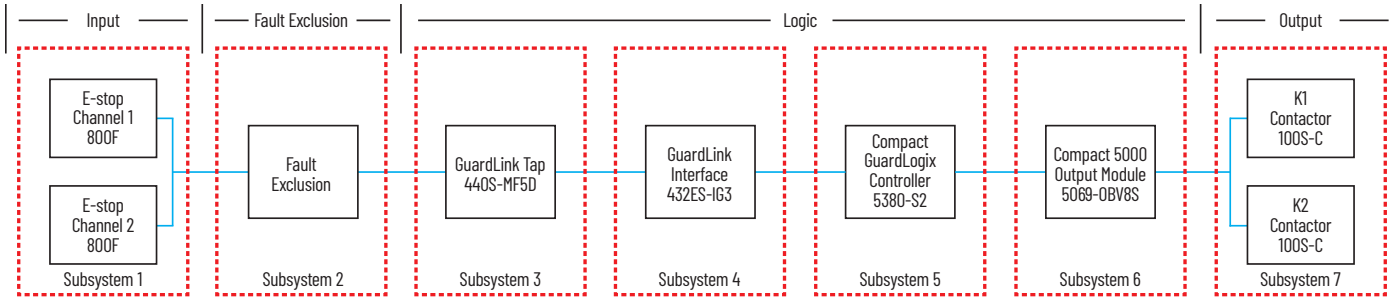
The PFH for electromechanical systems may be calculated differently based on the version of ISO 13849 supported by SISTEMA. ISO 13849-1:2015, which changed the maximum MTTFd from 100 to 2500 years, is supported starting in version 2.0.3 of SISTEMA. As a result, the same SISTEMA data file that is opened in two different versions of SISTEMA can yield different calculated results.

The following PFHd values are for the GuardLogix 5580 and Compact GuardLogix 5380 safety controllers. Either controller can be selected in this example application.

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔ SB	Safety PLC: GuardLogix 1756-L8xES	d	d	6.4E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled

Safety-related Stop Function Initiated by an E-stop

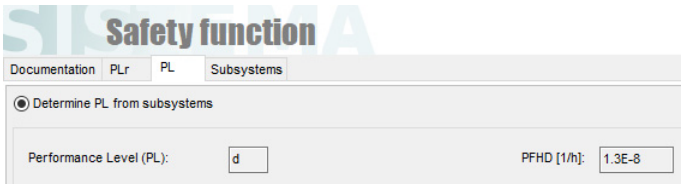
The safety-related stop function that is initiated by an emergency stop safety function can be modeled as follows:



Assuming the use of the following subsystem choices, the overall performance level that is achieved is shown in the graphic.

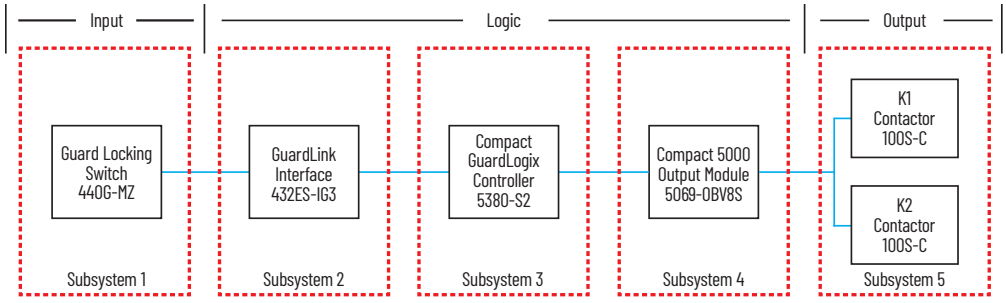
Status	Name	Ref. d...	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔ SB	E-Stop 800FP-MT	01	e	n.a.	9.1E-10	65 (fulfilled)	99 (High)	2,500 (High)	4	fulfilled
✔ SB	Single actuator fault exclusion	02	e	n.a.	0	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	440S-MF*D/440S-MLF*D GuardLink Tap: Electromechanical	03	e	n.a.	2.7E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	GuardLink Interface 432ES-IG3	04	d	d	2.9E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	05	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔ SB	Compact GuardLogix 5069-OBV8S	06	d	d	3.1E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	Safety Contactors 100S-C	07	e	n.a.	1.6E-9	65 (fulfilled)	99 (High)	1,457.5 (High)	4	fulfilled

IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems with 365 annual operations, is 1.3 E-8. The PL for the complete safety function is PLd.



Safety-related Stop Function Initiated by a Safeguard and Prevention of an Unexpected Startup

The safety-related stop function that is initiated by a safeguard and prevention of an unexpected startup safety function can be modeled as follows:



Assuming the use of the following subsystem choices, the overall performance level that is achieved is shown in the graphic.

Status	Name	Ref. d...	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔ SB	Guardmaster 440G-MZ Interlocking Device with Guard Locking	01	e	n.a.	2.9E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	GuardLink Interface 432ES-IG3	02	d	d	2.9E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	03	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔ SB	Compact GuardLogix 5069-OBV8S	04	d	d	3.1E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	Safety Contactors 100S-C	05	e	n.a.	1.6E-9	65 (fulfilled)	99 (High)	1,457.5 (High)	4	fulfilled

IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems with 8760 annual operations, is 1.5 E-8. The PL for the complete safety function is PLd.

Functional Safety Data Required for Determining the Performance Level of Electromechanical Devices

Because these contactors are electromechanical devices, the functional safety data that are required for the Performance Level calculation includes the following:

- Mean Time to Failure, dangerous (MTTFd)
- Diagnostic Coverage (DCavg)
- Common Cause Failure (CCF)

The functional safety evaluations of the electromechanical devices include the following:

- How frequently they are operated
- Whether they are effectively monitored for faults
- Whether they are properly specified and installed

SISTEMA calculates the MTTFd by using B10d data that are provided for the contactors along with the estimated frequency of use, entered during the creation of the SISTEMA project.

The DCavg (99%) for the contactors is selected from the Output Device table of ISO 13849-1 Annex E, Direct Monitoring.

The DCavg (99%) for the E-stop is selected from the Input Device table of ISO 13849-1 Annex E, Cross Monitoring.

The CCF value is generated by using the scoring process that is outlined in Annex F of ISO 13849-1. The complete CCF scoring process must be performed when actually implementing an application. A minimum score of 65 must be achieved.

When an application includes two-channel, single-actuator mechanical safeguarding devices such as interlocks, or mechanical emergency stop devices such as E-stop buttons or cable-pull switches, fault exclusion for single-actuator failure must be considered and, when required, applied when determining the Performance Level.

Verification and Validation Plan

Verification and validation play important roles in the avoidance of faults throughout the safety system design and development process. ISO 13849-2 sets the requirements for verification and validation. The standard calls for a documented plan to confirm that all safety functional requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm that the system meets the required Performance Level (PLr) specified. The SISTEMA software is typically used to perform the calculations and assist with satisfying the requirements of ISO 13849-1.

Validation is a functional test of the safety control system to demonstrate that the system meets the specified requirements of the safety function. The safety control system is tested to confirm that all safety-related outputs respond appropriately to their corresponding safety-related inputs. The functional test includes normal operating conditions and potential fault injection of failure modes. A checklist is typically used to document the validation of the safety control system.

Before validating the GuardLogix Safety System, confirm that the safety system and safety application program have been designed in accordance with the controller safety reference manuals that are listed in the Additional Resources and the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095.

For a validation checklist, see the attached spreadsheet. For instructions on how to access the attachments, see Use Sample Project Files on page 4.

Additional Resources

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

Resource	Description
GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012	Describes the GuardLogix 5580 and Compact GuardLogix 5380 controller system. Provides instructions on how to develop, operate, or maintain a controller-based safety system that uses the Studio 5000 Logix Designer application.
ControlLogix and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information on how to install, configure, and program the GuardLogix 5580 controllers in the Logix Designer application.
CompactLogix™ and Compact GuardLogix Controllers User Manual, publication 5069-UM001	Provides information on how to install, configure, and program the Compact GuardLogix 5380 controllers in the Logix Designer application.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Describes the Rockwell Automation GuardLogix Safety Application Instruction Set. Provides instructions on how to design, program, or troubleshoot safety applications that use GuardLogix controllers.
Compact 5000 I/O Digital Modules User Manual, publication 5069-UM004	Provides information on how to install, configure, and operate 5069 I/O modules.
432ES-IG3 GuardLink EtherNet/IP Interface User Manual, publication 432ES-UM001	Provides information on how to install, configure, and operate the 432ES-IG3 GuardLink interface.
432ES-IG3 GuardLink EtherNet/IP Interface Installation Instructions, publication 432ES-IN001	Provides information on how to install and wire the 432ES-IG3 GuardLink interface.
Guardmaster® DG Safety Relay and GuardLink System, User Manual, publication 440R-UM015	Provides information on how to configure and operate a GuardLink System.
440G-MZ Interlocking Safety Switch User Manual, publication 440G-UM004	Provides information on how to install, configure, and operate the 440G-MZ interlocking safety switch.
IEC Contactor Specifications, publication 100-TD013	Provides specification details on 100S-C contactors.
Rockwell Automation Functional Safety Data Sheet, publication SAFETY-SR001	Provides functional safety data for Rockwell Automation® products.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

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

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	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.

Safety Function Capabilities

Visit rok.auto/safety for more information on our Safety System Development Tools, including Safety Functions.

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

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

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication SAFETY-AT200A-EN-P - June 2023