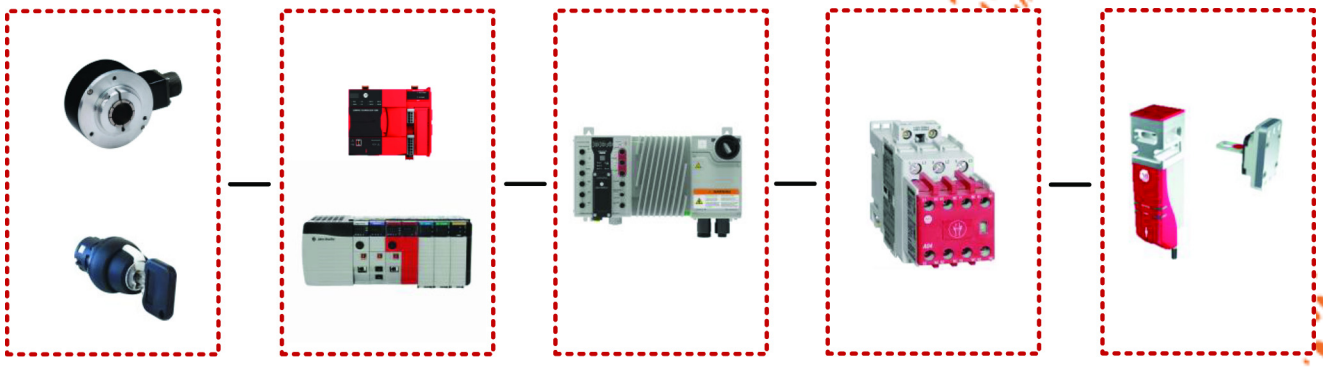
Application Technique

Original Instructions

Safely-limited Speed and Guard Door Unlocking with Armor PowerFlex Safety Function

Products: Guardmaster 440G-MZ Interlocking Switch, GuardLogix 5580 or Compact GuardLogix 5380 Controller, Armor PowerFlex 35S Integrated Safety, 700S-C Relay

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



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 13857:2019 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2019 (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 13857:2019 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2019 (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 a GuardLogix® controller to interface with an Armor™ PowerFlex® integrated safety AC drive to perform Safely-limited Speed (SLS) functions. The integrated safety Armor PowerFlex encoder feedback is used to bring velocity data into the GuardLogix safety task. The GuardLogix safety controller contains logic to monitor SLS. When the hazard is at a safe speed and an SLS request is made, safety logic unlocks the locking guard door. The Armor PowerFlex safety digital safety inputs are used to monitor the guard locking switch and safe speed selector switch. The safety outputs are used to control the lock function of the locking guard door switch.

The motion control actuator for the safety functions is the motor the Armor PowerFlex AC drive controls. Any malfunction the safety system detect results in a Safe Stop 1 (SS1) which is a safely monitored decel, followed by Safe Torque Off (STO).

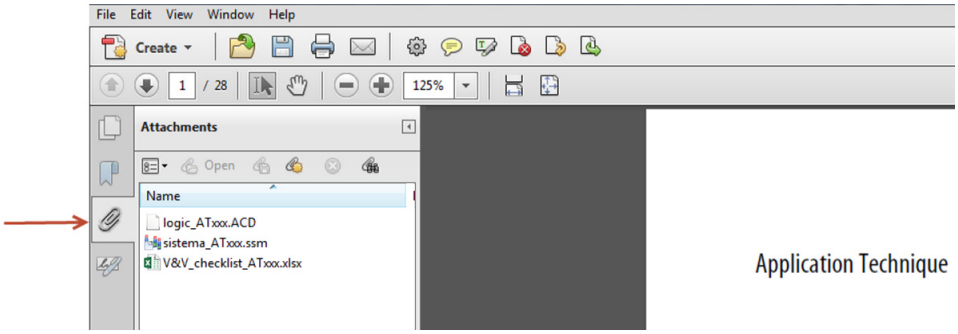
This example uses a 1756-L84ES GuardLogix primary only controller, but you can substitute a Compact GuardLogix controller that supports the safety rating that is demonstrated in this safety function application technique. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) calculations that are shown later in this document must be recalculated if different products are used.

Use Sample Project Files

Sample project files (AutoCAD, EPLAN, 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.

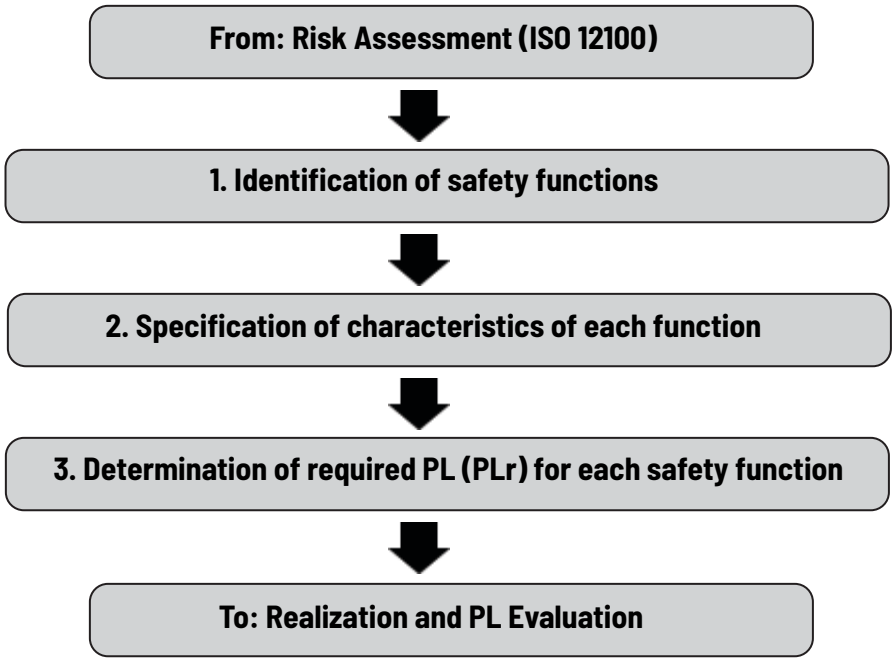
1. If you are viewing the PDF file in a browser and do not see the Attachments link, download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link.
3. Right-click and save the desired file.



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 Function

This application technique includes three Safety Functions:

1. Guard Door Unlock at Safely-limited Speed (SLS)
2. Guard Door Unlock at standstill speed: Safe Stop 1 (SS1)
3. Prevention of an Unexpected Startup with guard door monitoring

Safety Function Requirements

Guard door unlocking is a safety function when used to protect people. The guard door unlock is a safety output function that is based on safety inputs detection of safe-to-enter conditions. All safe entry conditions must be detected with safety integrity that meets the level of the unlock safety function.

When SLS is requested, the motor speed must go below the programmed speed limit before the SLS check time delay expires. After the delay expires, the speed must remain below the limit. After the delay expires, if motor speed is below the SLS, the gate is unlocked, and this action allows access to the hazardous area. You must perform a risk assessment to determine the SLS for the motor.

If the programmed speed limit is exceeded after the delay expires, a Safe Stop 1 (SS1) is generated to stop the motor, after which STO is activated, and this action causes the motor torque to be disabled.

A two-position maintained key selector switch is used to request SLS. When the key is in the SLS mode position, the key can be removed to preserve SLS mode while the task that requires SLS is performed.

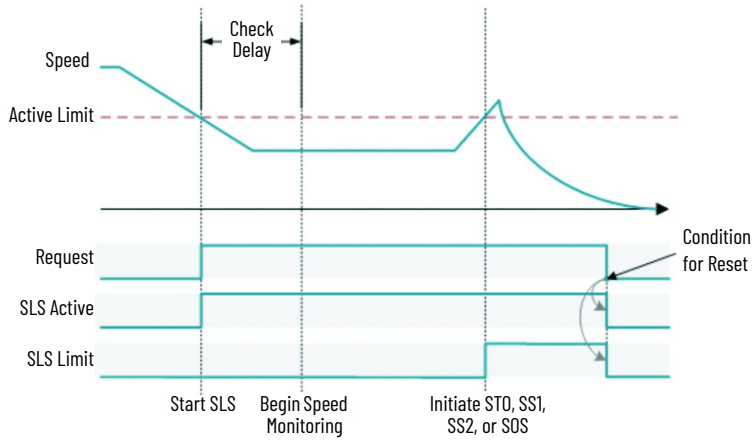
If the door is unlocked or open, and the safety system is not in SLS or SS1 mode, then STO is activated.

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.

Guard Door Unlock at Safely-limited Speed

For tasks that require motion, a safety function to limit and monitor the speed of the motor can be used so that harm can be avoided, or at least reduced, if motion occurs.

Normal operation with Automatic Restart is shown in the following diagram. After Check Delay expires, the speed must stay below the Active Limit, or the SLS Limit will be set to ON(1). The SLS Limit, once set, remains at ON(1) until the SLS function is reset. For automatic restart operation, the SLS function is reset when the request is removed OFF(0), provided no SLS faults have occurred.



Both the door and lock are monitored to help prevent an unexpected startup. Startup cannot occur until the door is closed and locked. After the door is closed, hazardous motion cannot resume until the door is locked via a lock request, and the STO condition is removed by using a manual action (Safety Circuit Reset) so the motor can be enabled.

The safety function meets the requirements for category 3, Performance Level d (cat. 3, PLd), per ISO 13849-1, and SIL 2 per IEC 62061, and control reliable operation per ANSI B11.19.

IMPORTANT Risk assessment is used to determine the SLS limits for the application.

SLS Operation

To operate the SLS function, follow these steps.

1. While the motor is at speed, request SLS if there are no faults within the Safe Motion instructions (SFX/SS1/SLS).
   The SLS request must remain high (1) throughout the SLS procedure. After SLS is requested, the motion application is signaled to reduce the motor speed below the SLS Active Limit. SLS monitoring begins after a programmable time delay (7.3 seconds in this example) to verify that the motor speed is below the programmed SLS Active Limit. Once the monitoring begins, if the motor speed is below the limit, the gate is unlocked to allow access to the hazardous area.
2. When the task that requires access has been completed, close the monitored door.
3. To lock the door, remove the SLS request to initiate a lock request.
4. The SLS request is removed. The motor speed can now be increased above the SLS.

Recover from SS1 Due to Time Delay Expiration

If the speed does not go below the programmed speed limit before the delay expires, a Safe Stop 1 (SS1) is requested. When the SS1 completes (standstill speed is reached), an STO request is made, which causes the motor torque to be disabled. With the motor disabled and speed below standstill, the gate is unlocked. To recover, follow these steps.

1. If the monitored door is open, close it.
2. Remove the SLS request.
3. Press the Safety Reset to lock the guard door, and on the falling edge of the reset the STO is removed, which allows the motor to be enabled.

Recover from SS1 When SLS is Exceeded

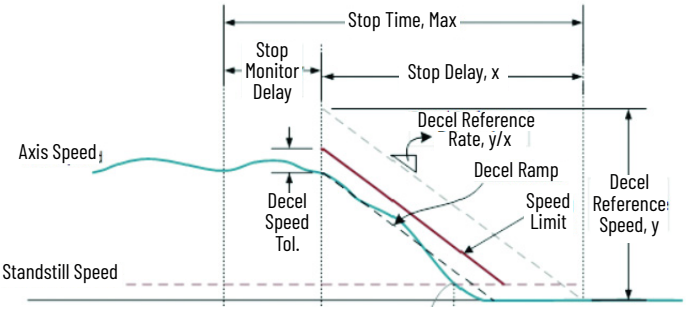
The gate is assumed to be unlocked and open when the speed limit is exceeded.

If SLS is exceeded after the programmable delay expires, an SS1 request is generated. When the SS1 completes (standstill speed is reached), an STO request is made, which causes the motor torque to be disabled. To recover, follow these steps.

1. Close the monitored door.
2. Remove the SLS request.
3. Press the Safety Reset to lock the guard door, and on the falling edge of the reset the STO is removed, which allows the motor to be enabled.

Guard Door Unlock at Zero Speed (Safe Stop 1 and Standstill Monitoring)

A guard door unlock condition for a properly executed SS1 with standstill monitoring allows entry when the actuator is in a standstill condition with STO activated. The safety function for SS1 standstill unlocking uses the same block diagram as SLS and is not analyzed separately in this example.



This example uses an operator interface to trigger the SS1 monitoring that is used to unlock the guard door when the actuator is within standstill speed limits. The triggering event is not considered part of the safety function for this application.

IMPORTANT Risk assessment is used to determine the conditions necessary for guard door unlock.

Prevention of Unexpected Startup with Guard Door Monitoring

The guard door closed/locked status is the input of the subsystem. If the guard door is unlocked or opens when not commanded, or a safety fault is detected the actuator motor control executes an SS1. The SS1 monitors the encoder speed feedback to verify that the properly configured decel ramp is activated, followed by Safe Torque Off (STO) at standstill speed. The motor is prevented from resetting until a safe running condition is confirmed.

Considerations for Safety Distance and Stopping Performance

Based on the selection of a sensor subsystem, 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. If a safety distance calculation is required for this safety function, the following documents can be referenced:

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

IMPORTANT A risk assessment may require additional safeguarding methods such as hold-to-run devices and proximity to complementary safety functions such as E-stops and lifelines.

Bill of Materials

This application technique uses these products.

Quantity	Cat. No.	Description
1	440G-MZS20SNRJ	Guard locking switch — 440G-MZ: OSSD, Power to Release, M12 5-pin QD connector
1	889D-F5AC-*xx*	DC Micro (M12), female, straight, 5-pin, PVC cable, yellow, unshielded, IEC color coded, no connector, specify length
1	800FM-KM22MX02	Two-position key selector switch, metal, maintained, right key removal, two N.C. contacts
1	DSM9H/DSM9X	Incremental encoder. BEI Electronic Version 5G2, SIL 3 type. 2048PPR.
1	700S-CF620EJBC	Safety control relay, 8 pole, 3 N.O./1 N.C. base, 3 N.O./1 N.C. auxiliary, bifurcated contact, 24V DC (with electric coil)
1	1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 120/240V AC 1

Choose one of the following safety-controller hardware groups.

Quantity	Controller	Cat. No.	Description
1	GuardLogix 5580[1]	1756-L81ES	GuardLogix processor, 3 MB standard memory, 1.5 MB safety memory
		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
1		1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC
1		1756-A7	Seven-slot ControlLogix® chassis
1	Compact GuardLogix 5380 SIL 2	5069-L306ERS2	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory
		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	
1		1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 120/240V AC input

(1) If your PLr is SIL 3/PLe, use a GuardLogix 5580 controller with a safety partner, cat. no. 1756-L8SP.

Choose an Armor PowerFlex 35S drive.

Quantity	Cat. No.	Description
1	35S-6*xx-xxxx*	Safety Armor PowerFlex AC drive
3	889D-E5NC-*xx*	DC Micro (M12), female, straight, 5-pin, PVC cable, red, unshielded, IEC color coded, no connector, specify length
1	889D-F8FB-*xx*	DC Micro (M12), female, straight, 8-pin, PVC cable, black, braided shield, IEC color coded, no connector, specify length
1	AC Motor	Application dependent. Use the motor nameplate data to configure the Armor PowerFlex motor control.

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 29.

System Overview

The 440G-MZ guard locking switch is wired to the Safety Armor PowerFlex integrated safety IO. Guard door power is supplied from an external power supply. The dual-channel closed and locked signals are connected to safety inputs 0 and 1. Safety output 0 controls the guard door unlock via an interposing 700S-CF safety relay. The interposing relay is used to interface the bi-polar safety output to the guard door unlock signal.

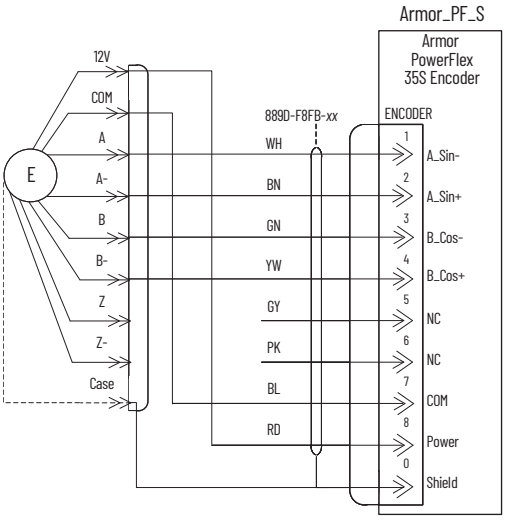
An external power supply is connected to the 440G-MZ switch to provide solenoid power.

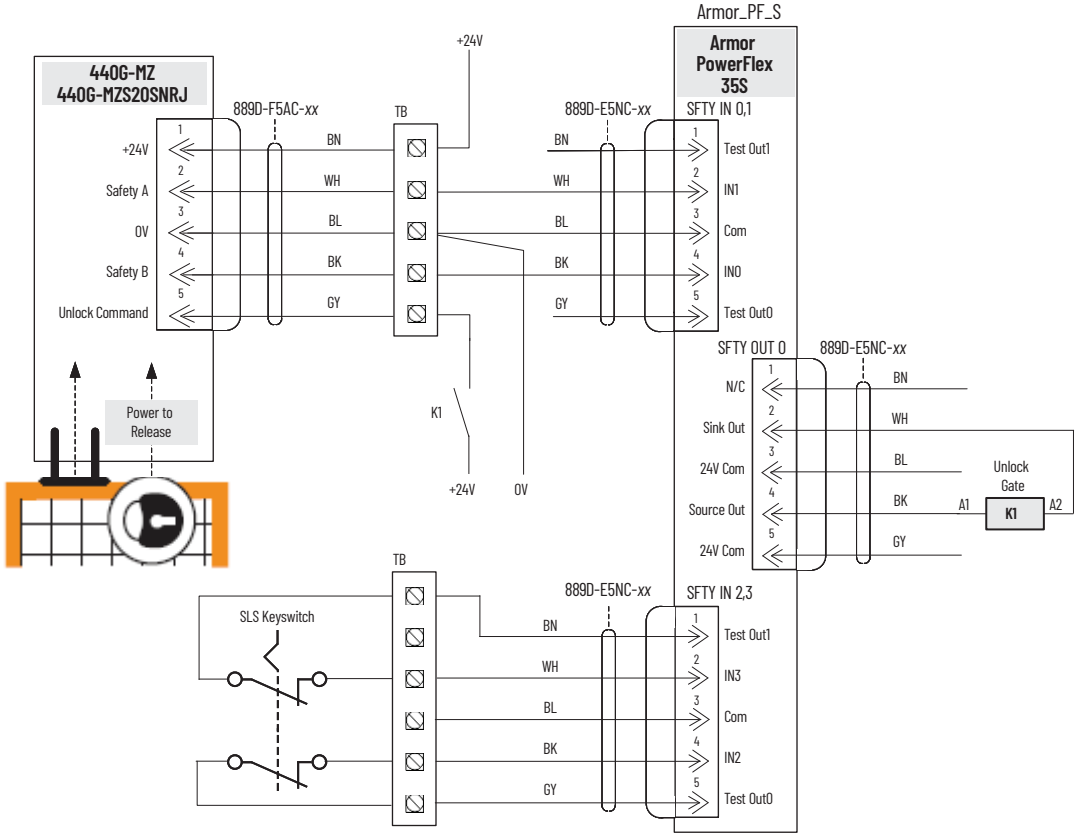
Safety speed feedback is supplied by one incremental encoder monitoring the AC motor actuator. The encoder is wired to the encoder input of the safety Armor PowerFlex 35S AC drive. The data for the encoder is passed internal to the drive to the internal safety speed-monitoring channel.

This example was tested using available components. An induction AC motor with dual-channel incremental encoder feedback that is compatible with the encoder input of the safety Armor PowerFlex AC drive was used for this example.

Electrical Schematic

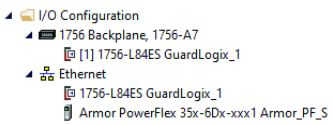
For an electrical schematic in AutoCAD or EPLAN format, see the attached files. For instructions on how to access the attachments, see Use Sample Project Files on page 4.



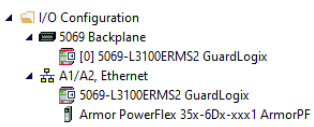


Network Architecture

GuardLogix 5580 Controller



Compact GuardLogix 5380 Controller



Configuration

The GuardLogix controller is configured by using the Studio 5000 Logix Designer® application, version 31 or later. You must create a project and add the Armor PowerFlex 35S AC drive. 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 5580 controller, but if you choose a 5380 controller, you can change the controller in the Logix Designer application.

Product	Minimum Software Version
GuardLogix 5580 or Compact GuardLogix 5380 controller	31.0 or later
Studio 5000 Logix Designer	31.0 or later
FactoryTalk® Linx [1]	6.20 or later
Armor PowerFlex AC drive firmware	1.04 or later
Studio 5000® Add-On-Profile (AOP) for Armor PowerFlex AC drive	1.1 or later

[1] Must be used as the Logix communication software. RSLinx® Classic does not allow connection to the Armor PowerFlex drive AOP.

IMPORTANT Only the safety-related programming and configuration are discussed in this document. Standard motion control required to satisfy the safety monitoring functions are out of scope of this document.

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.

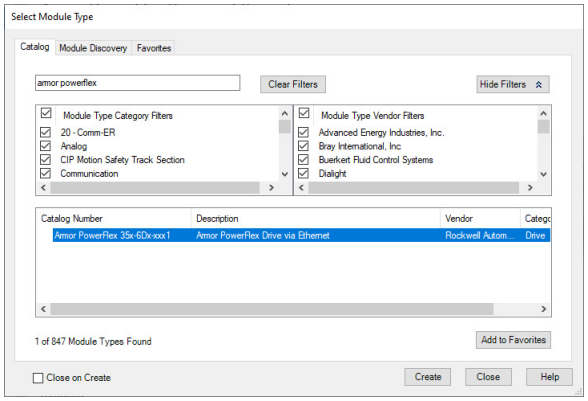
1. In the Logix Designer application, create a project with a GuardLogix controller.

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 install a 1756-L8SP Safety Partner to the right of the primary controller.

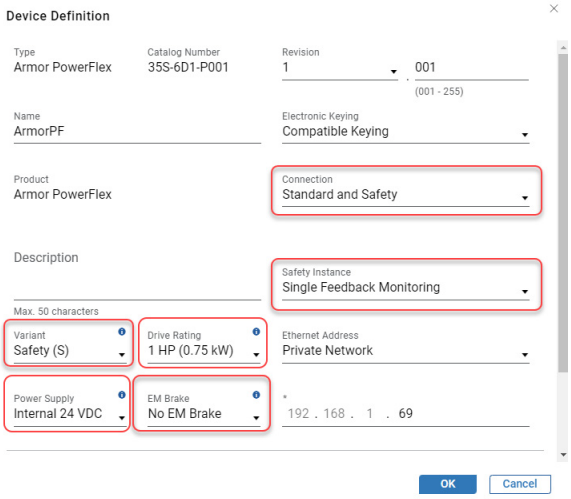
2. Set the IP address for the controller and the Armor PowerFlex 35S.

Armor PowerFlex 35S Configuration - Device Definition

1. Create an Armor PowerFlex Drive via Ethernet to the project I/O Configuration.

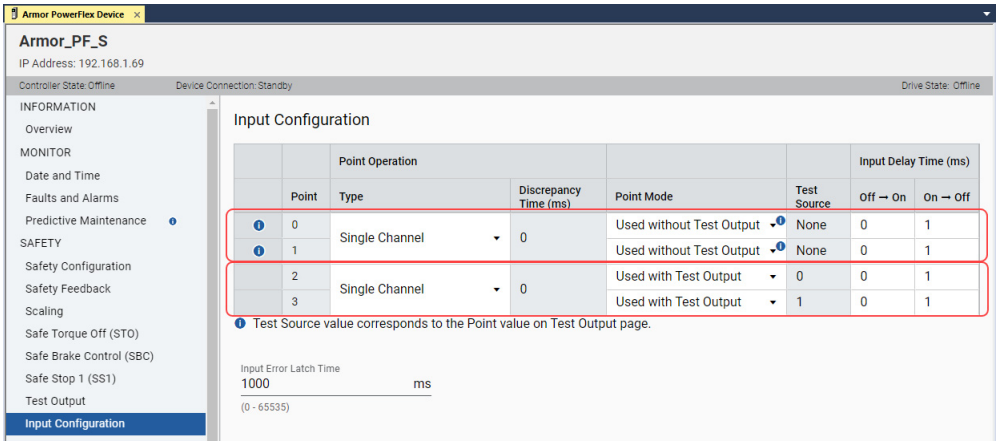


2. Identity - configure Connection, Safety Variant, and Safety Instance.
   a. Variant is product-dependent; you must use a 35S catalog number. Set to Safety (S).
   b. EM Brake is product-dependent; must be set to match the catalog number specified.
   c. Connection set to Standard and Safety
   d. Safety Instance set to Single Feedback Monitoring. Even though we are using controller-based safety functions, not drive-based, the safety instance must be set to feedback monitoring to enable encoder connection to the Logix safety tasks.
   e. Select the drive rating and 24V power supply source that matches your equipment.

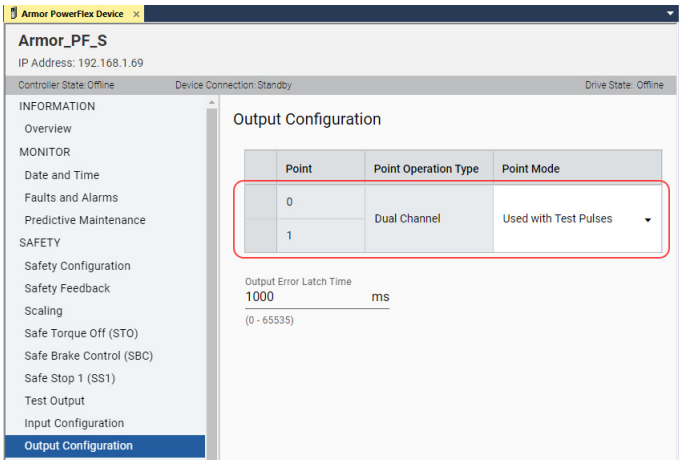


Armor PowerFlex 35S Configuration - Initial Safety Configuration

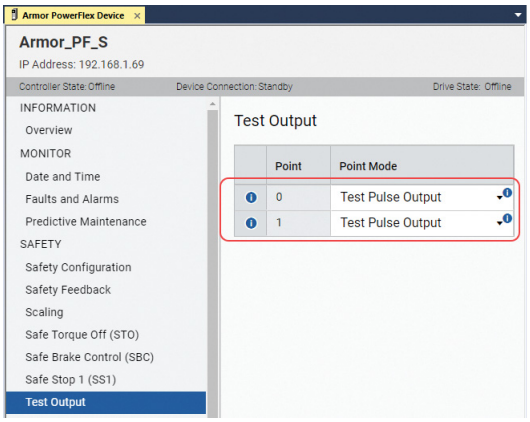
1. Input Configuration:
   a. Point Mode 0,1 - Single-channel, which is used without Test Output (Safety, not pulse test). Safety input device (440G-MZ) wired to points 0 and 1 is an Output Signal Switching Device (OSSD). Set the Input Delay Time for these inputs to 1 ms.
   b. Point Mode 2,3 - Single-channel equivalent, which is used with Test Output. Safety input device (SLS Keyswitch) wired to points 2 and 3 is a standard contact device.



2. Output Configuration: Type - Dual Channel, Point Mode - Safety Pulse Test. To control guard door solenoid interposing safety relay.

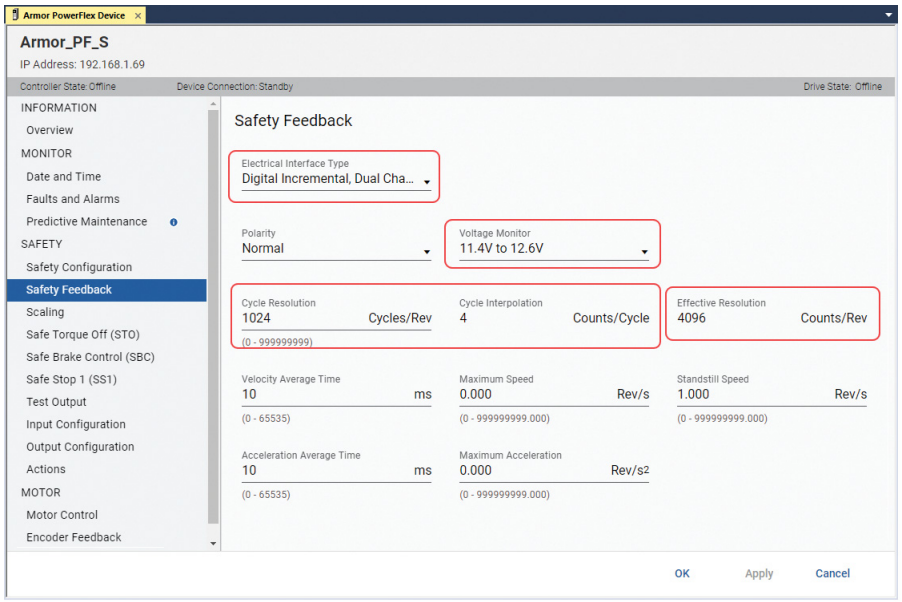


3. Test Output: Point Mode - Test Pulse Output. Used for pulse testing the SLS Keyswitch input.



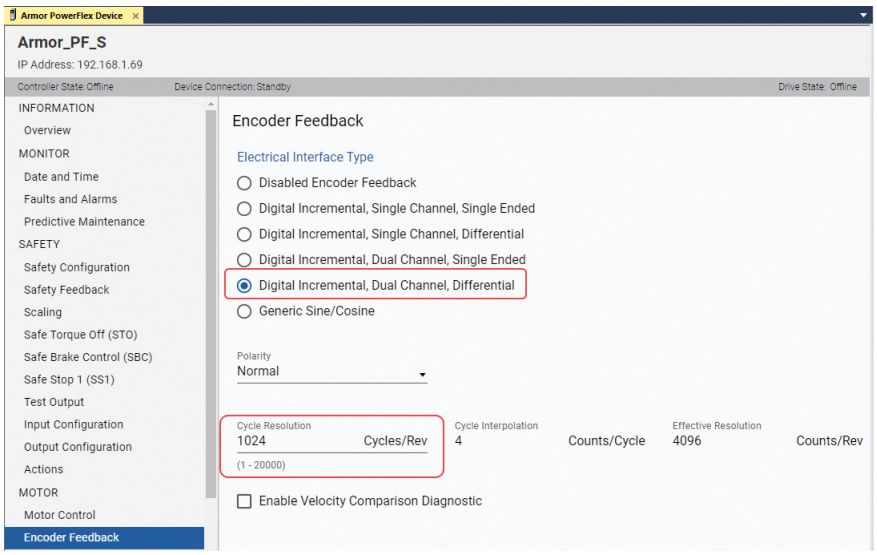
4. Safety Feedback: The motor actuator drives the encoder, which wired to the Armor PowerFlex encoder input.
   a. Per the encoder specifications, the cycle resolution is a dual channel incremental type.
   b. The encoder is powered by 12V DC from the Armor PowerFlex drive.
   c. The encoder cycle resolution is 1024 cycles/rev.
   d. The encoder input circuits detect the rising and falling edges of the encoder pulse out for 4 counts/cycle.
   e. Leave all other settings at default values. The Logix safety instructions are used for the SLS and SS1 safety functions.

The Effective Resolution (4096 count/rev) is required to configure the GuardLogix SFX instruction.

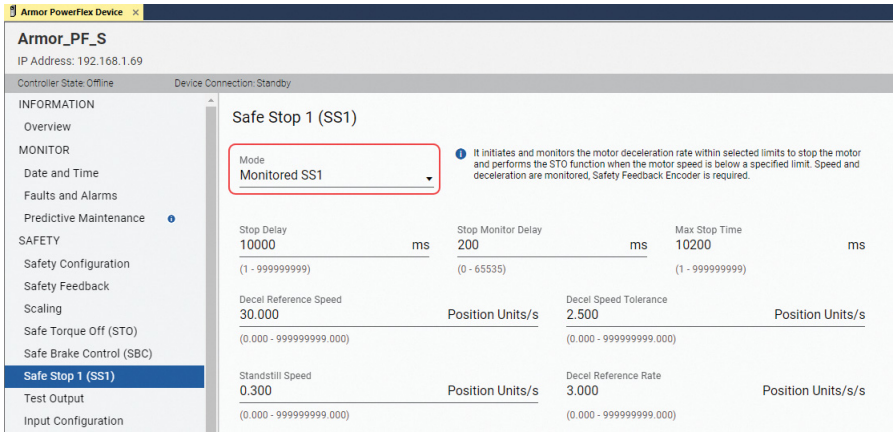


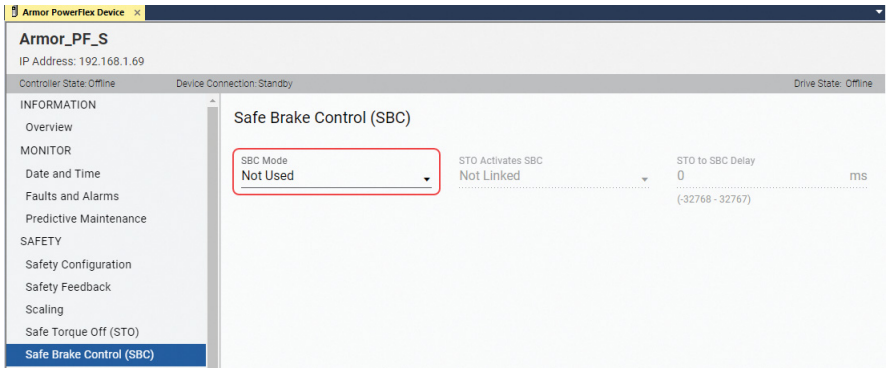
5. Scaling: For this example, we are not using position feedback, leave values at default.

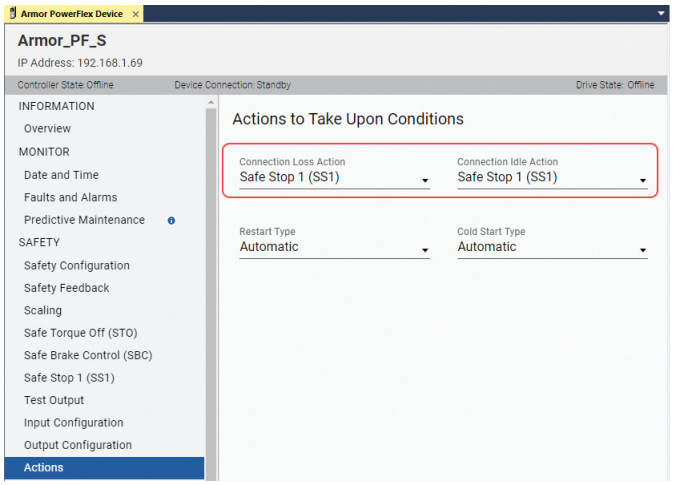
6. Motor Encoder Feedback: Set to match encoder specifications. These settings must match the Safety Feedback configuration (step 4).



7. Safety: Configure drive-based Safe Stop 1 (SS1) for Monitored SS1. Configure these settings to the same values as the corresponding settings in the Logix SS1 instruction. This setting is the action that the drive takes when a communication loss or communication timeout occurs. Safe Brake Control (SBC) is not used. The communication connection loss and connection idle action is set to drive based SS1.





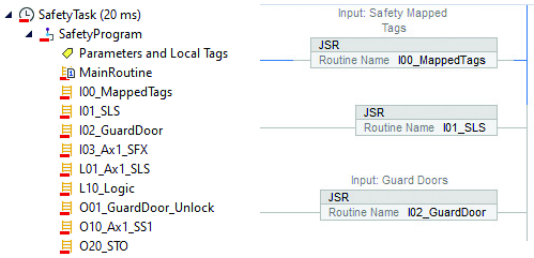


Programming

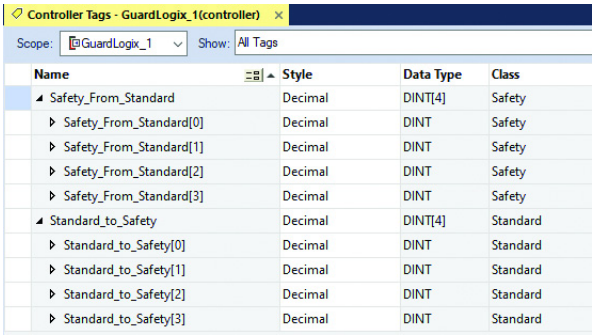
For controller logic that you can download to your controller, see the attached ACD file. For instructions on how to access the attachments, see Use Sample Project Files on page 4.

General Safety Task Configuration

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 with the 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.

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

3. The Reset and Safe Stop 1 (SS1) signals for safety logic are mapped from the standard logic with the mapped alias.

Figure 1 - Standard Program, Any Routine

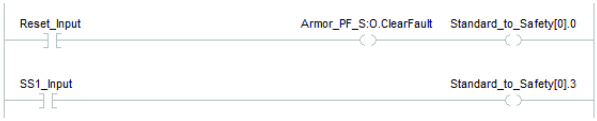


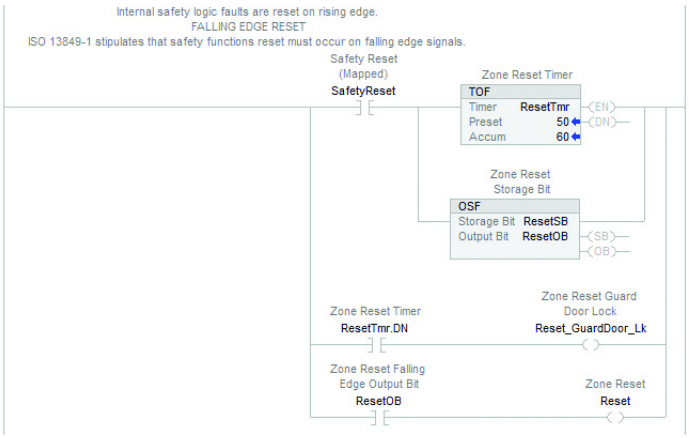
Figure 2 - Safety Program, I00_MappedTags Routine

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 the location and specific requirements for safety reset.

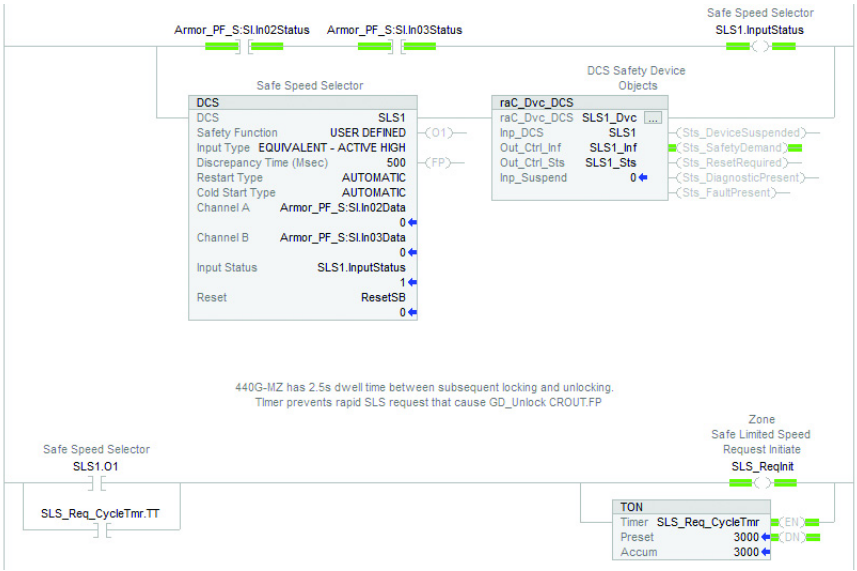
Figure 3 - Safety Routine L10_Logic



Input Safely-limited Speed (SLS) Selector Switch — Safety Routine I01_SLS

Monitor SLS selector switch status inputs.

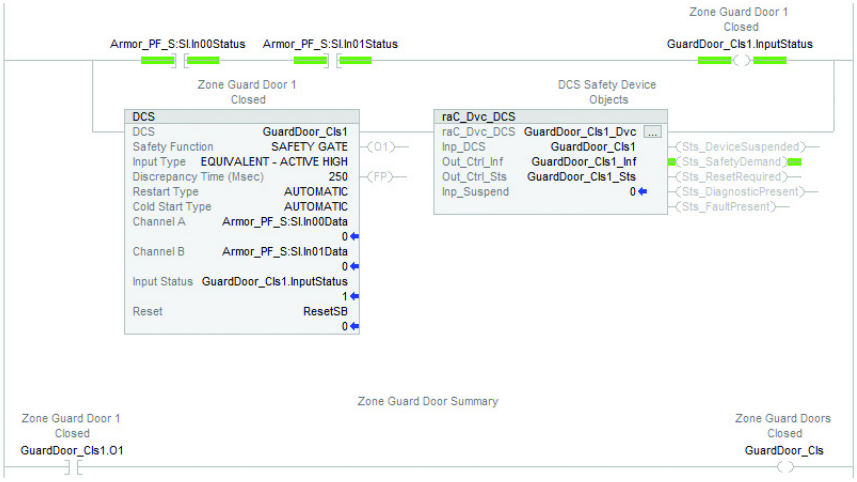
Tag	Description
InputStatus	Combine the input status of the inputs before the DCS.
DSC	Dual Channel Stop instruction for monitoring two inputs and associated I/O status.
raC_Dvc_DCS	The optional raC_Dvc_DCS Add-On Instruction (AOI) connects DCS to the HMI faceplate. (ME, SE, PV5000) To find this information, go to the Product Compatibility Download Center website, and search for Safety Device Library.



Input Guard Door Closed and Locked – Safety Routine I02_GuardDoor

Monitor guard door lock status inputs.

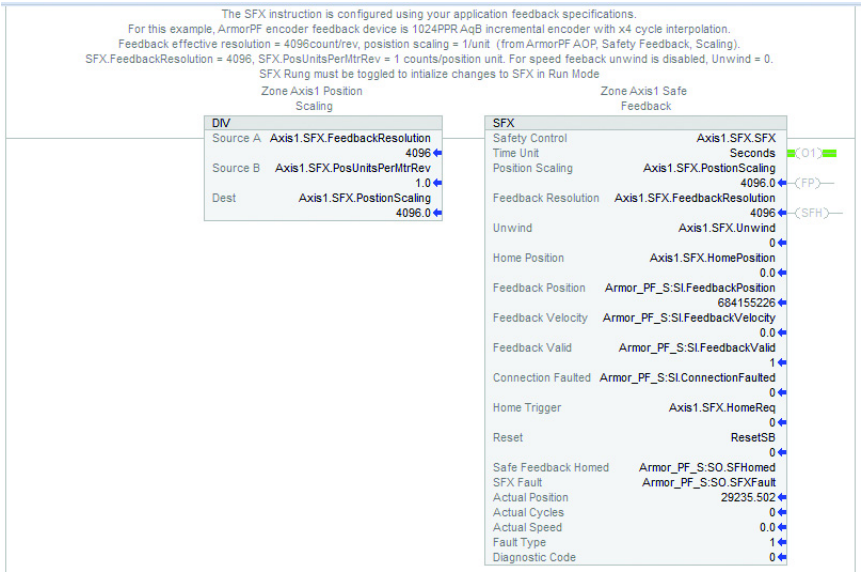
Tag	Description
InputStatus	Combine the input status of the inputs before the DCS.
DSC	Dual Channel Stop instruction for monitoring two inputs and associated I/O status.
raC_Dvc_DCS	The optional raC_Dvc_DCS AOI connects DCS to the HMI faceplate. (ME, SE, PV5000) To find this information, go to the Product Compatibility Download Center website, and search for Safety Device Library.



Input SFX – Safety Routine I03_Ax1_SFX

The Input SFX routine brings safe speed and velocity feedback into the safety task. Primary feedback scaling and home proximity switch (not used).

Tag	Description
DIV	Feedback resolution is taken directly from the Armor PowerFlex module feedback properties. PositionUnitsPerMtrRev: Application scaling factor. This example, 4096 count/rev. Position Scaling: Counts/rev
SFX	Safe Feedback Interface Monitors safety position, velocity, and feedback status Scales position and velocity to proper units. SFX.ActualSpeed is used by the SLS and SS1 instructions to monitor actual motor velocity.



Logic SLS – Safety Routine L01_Ax1_SLS

The Logic SLS routine performs the Safely-limited Speed (SLS) logic. SLS is used for guard door unlocking. When the SLS request is removed the timer allows time for the Guard Door to lock before stopping SLS monitoring. The timer preset value is dependent upon the guard locking device lock and feedback response time.

The 440G-MZ lock feedback from Armor PowerFlex output through 700S safety relays trends about 500 ms.

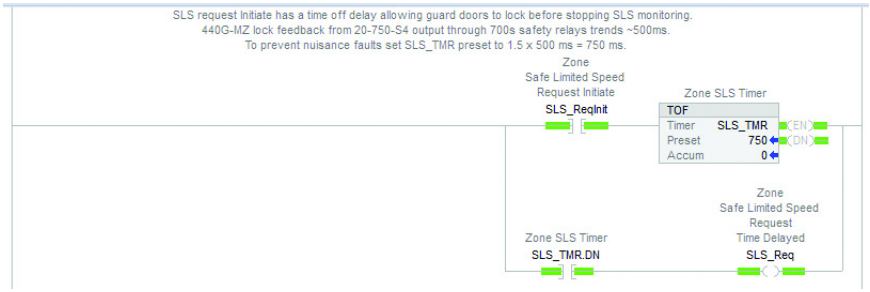


Table 1 - SLS Instruction

Tag	Description
MOV	Actual velocity visual for the programmer to see what speed the SLS is monitoring.
SLS	Safely-limited Speed instruction Velocity Active Limit is the maximum velocity. Can be programmatically changed. Feedback SFX is the SFX being monitored. SLS Active, Limit, Fault values sent to the drive for pass through standard tags.

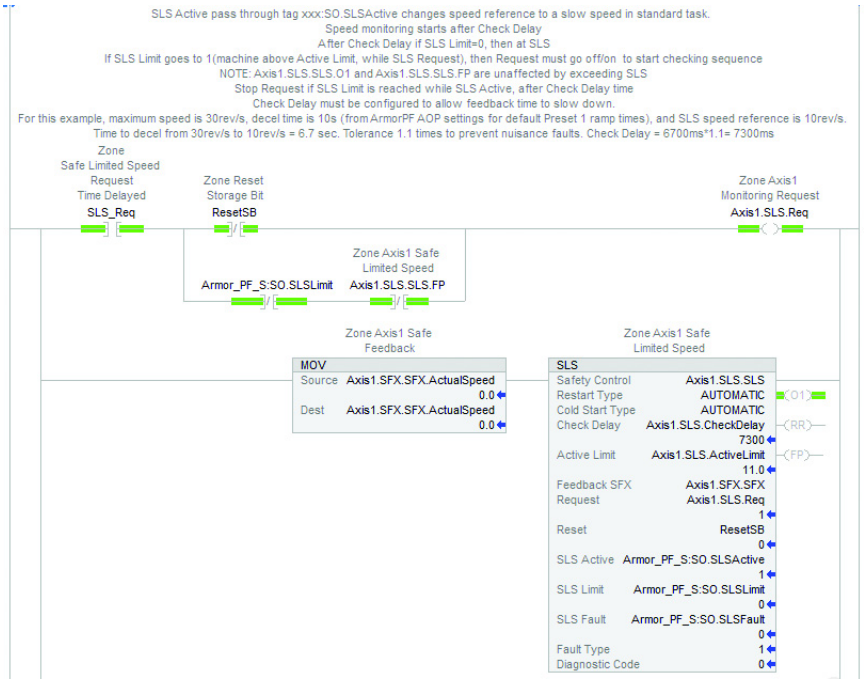
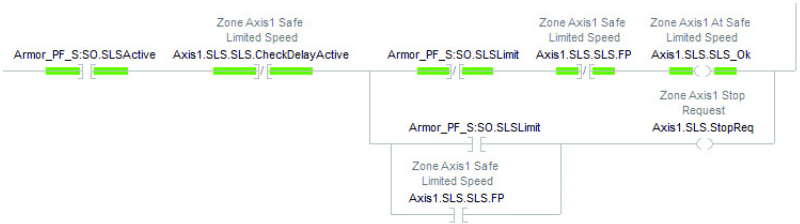


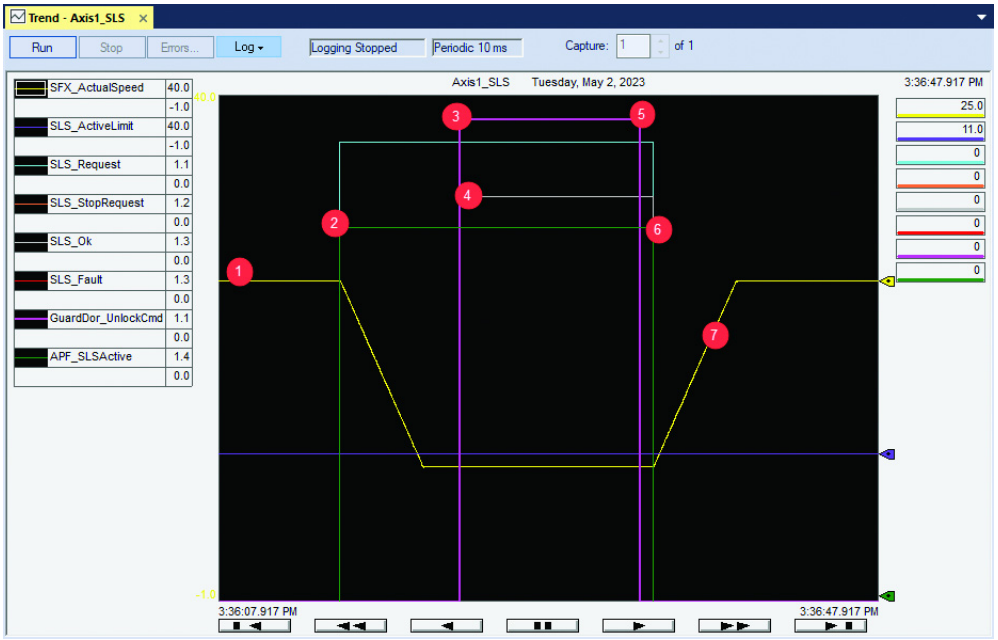
Table 2 - SLS Output Status

Tag	Description
SLS_Ok	IF SLS is Active, check-delay expired, not over speed limit, no SLS fault THEN SLS is OK. SLS Limit is the key variable for SLS out of Active Limit. SLS does not fault when exceeding the active limit.
StopReq	IF SLS is Active, check-delay expired, and (limit or SLS fault) THEN SLS Stop Request. Safe stop the application due to SLS malfunction or overspeed limit. In this example, initiate Safe Stop 1 (SS1).



Example of Safely-limited Speed Monitoring

This trend example shows the key elements for normal (no faults) operation of Safely-limited Speed monitoring for guard door unlock control. This trend file, Axis1_SLS, is available within the attached Logix project file under >Assets>Trends.



Item	Description
1	Motor running at normal speed.
2	With an SLS_Req, the SLS instruction initiates. SLS.CheckDelayActive goes true. The Armor PowerFlex passthrough tag SLSActive goes true and is used to select the Safely-limited Speed in the standard task.
3	When the SLS.CheckDelay time has expired SLS.CheckDelayActive goes false, the SFX.ActualSpeed is compared to the SLS.ActiveLimit speed. If the Armor PowerFlex tag S0.SLSLimit is false, the SFX.ActualSpeed is less than the SLS.ActiveLimit speed. If the SLSLimit tag is true, the SFX.ActualSpeed is greater than the SLS.ActiveLimit speed.
4	If the S0.SLSLimit tag is false, SLS.SLS_Ok goes true and initiates a GuardDoor_Unlk_Cmd, unlocking the guard door. If the S0.SLSLimit tag is true, SLS.SLS_Ok is false, the guard door does not unlock and the SLS instruction, SAF_RunPerm goes false and initiates a Safe Stop 1 (SS1).
5	Exit SLS, tag SLS_ReqInit goes false, the GuardDoor_Unlk_Cmd goes false locking the guard door.
6	SLS_TMR provides time for the guard door to lock and the closed/locked feedback to be received before the SLS_Req tag goes false.
7	Armor PowerFlex tag S0.SLSActive goes false and the speed resumes to normal running speed.

A trend can be used to verify the timing of the safety functions. Understanding sequential logic timing is important to allow time for a system to respond and help prevent nuisance tripping.

Logic Main – Safety Routine L10_Logic

The main safety logic contains reset logic, device status summary, and the main run permissive.

Table 3 - Zone Safety Motion Ready and Safety Reset Required

Tag	Description
Axis1.SFX.SFX.01 Axis1.SS1.SS1.01 Axis1.SLS.SLS.01	Safety instructions monitoring and ready.
SAF_RunPerm	On loss of safe run permissive, a Safe Stop 1 (SS1) is executed.
STO_ResetReq	Safe Torque Off (STO) requesting reset.
SafeMotion_Rdy	Safety instructions ready. Important for fault recovery.

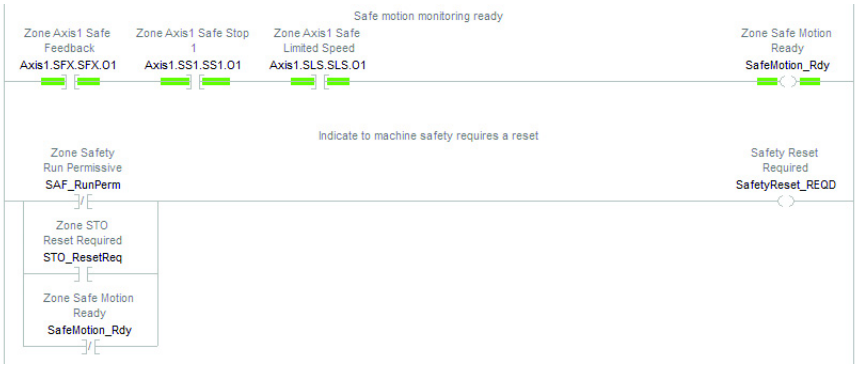


Table 4 - Safety Input Summary

Tag	Description
GuardDoor_Cls	Guard Door Closed Status
GuardDoor_Lk	Guard Door Locked Status
SLS_Ok	SLS actively monitoring allows the guard door to be unlocked and open.

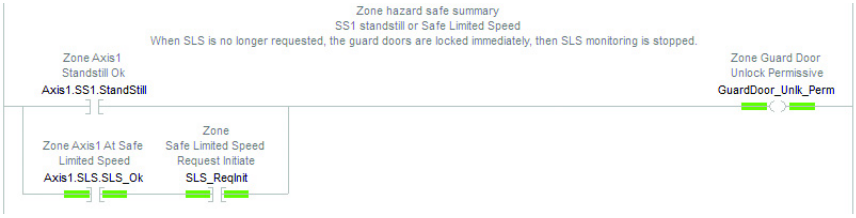
Table 5 - Drive Run Permissive

Tag	Description
SafetyIn_Ok	Input summary from previous rung.
SS1_Req	Safe Speed 1 (SS1) request mapped from standard.
SLS.StopReq	SLS malfunction or velocity over limit removes run permissive.
SAF_RunPerm	On loss of safe run permissive, a Safe Stop 1 (SS1) is executed

Output Guard Door Unlock – Safety Routine 001_GuardDoor_Unlock

The output guard door unlock routine contains the logic that controls the guard door lock and unlock function.

Guard door unlock permissive is based on SS1 at standstill or SLS monitoring velocity is below limit:



Guard door unlock command requires the unlock permissive, no unlock faults, and is removed on a safety reset to allow restart:

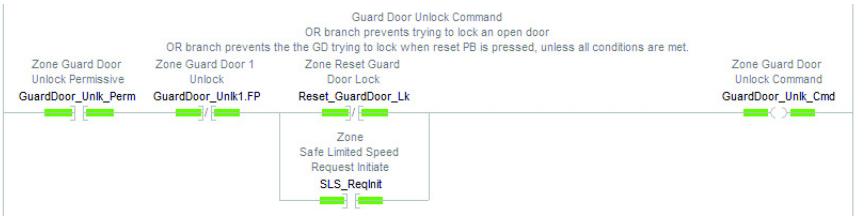


Table 6 - Guard Door Solenoid and Lock Monitoring

Tag	Description
InputStatus	Combine the input status of the inputs before the CROUT.
CROUT	Configurable Redundant Output instruction for controlling the locking outputs and monitoring two locked feedback inputs and associated I/O status. Provides continuous monitoring of locked feedback relationship to commanded unlock output.
raC_Dvc_CROUT	The optional raC_Dvc_CROUT AOI connects CROUT to the HMI faceplate. (ME, SE, PV5000) To find this information, go to the Product Compatibility Download Center website, and search for Safety Device Library.

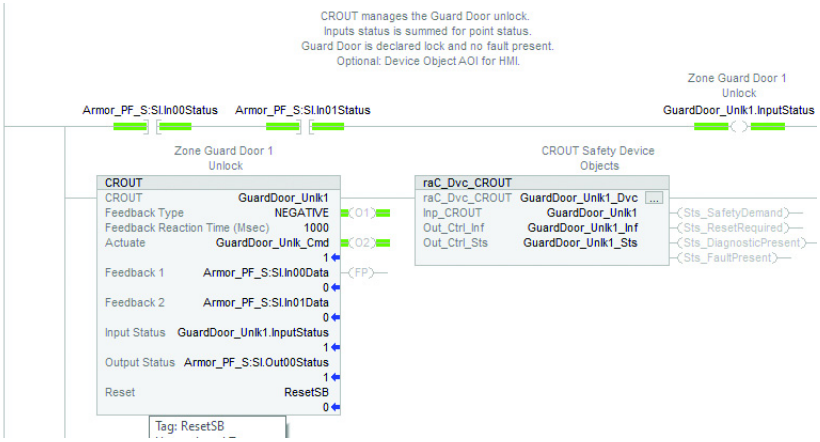
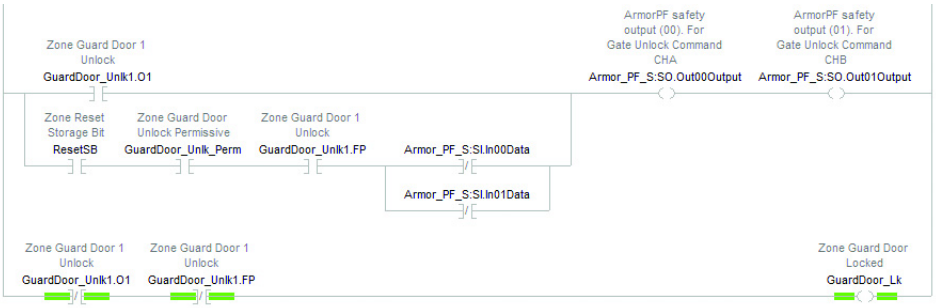


Table 7 - Solenoid Output

Tag	Description
GuardDoor_Unlk1.01	CROUT output actuates the interposing relay controlling guard door unlock solenoid
GuardDoor_Lk	Status of guard door lock for other safety task routines.



Output SS1 – Safety Routine 010_Ax1_SS1

The Output SS1 routine performs the Safe Stop 1 (SS1) safety function.

SS1 Request on loss of run permissive and no SS1 fault.

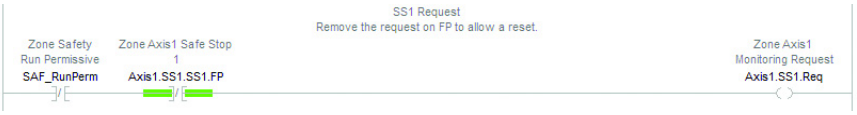
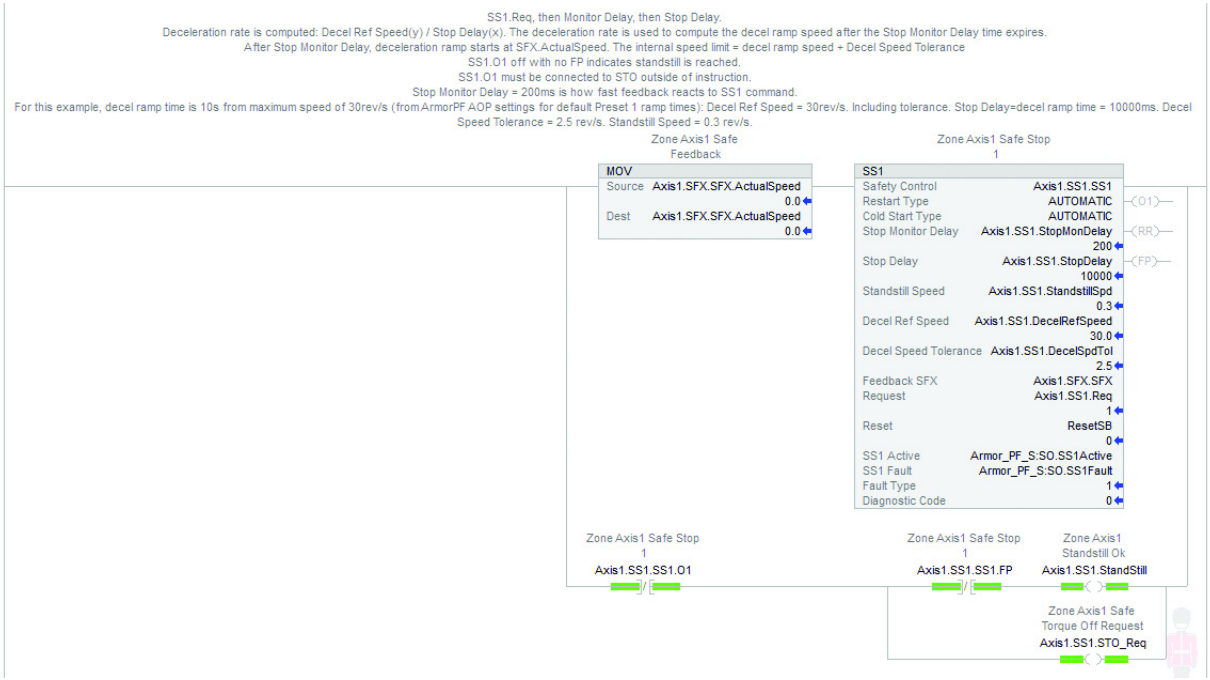


Table 8 - SS1 Instruction

Tag	Description
MOV	Actual Speed visual for the programmer to see what speed the SS1 is monitoring.
SS1	Safe Stop 1 instruction. • Stop Monitor Delay; time after request to start monitor decel ramp. • Stop Delay; used to build X-axis of decel monitor ramp, and maximum allowed time to reach standstill. The deceleration time from maximum speed to zero in ms. • Decel Ref Speed; used to build Y-axis of decel monitor ramp. Typically the maximum speed reference. • Standstill Speed; is the speed that standstill is declared and STO request is made. • Decel Speed Tolerance is the tolerance shift between actual ramp and fault point. Typically set to 10% or less of the maximum speed reference. Experiment with setting this value as low as possible. Too low a value can cause nuisance faulting of the SS1 instruction so include some tolerance for varying operating conditions. Feedback SFX is the SFX being monitored. SS1 Active, Fault values sent to the drive for pass through standard tags.
Standstill	When SS1.O1 goes off and there is no SS1 fault, SS1 has passed through standstill. This standstill is based on STO, which results in no additional motion. Not valid for overdriving loads or gravitational loads that can move after motor torque has been removed. For these applications, use other forms of stop monitoring such as Safe Operating Stop.
STO_Req	This bit is used to have the SS1 instruction initiate the drive STO.



Example of Safe Stop 1

This trend example shows the key elements for an SLS instruction detecting safe speed limit exceeded safety function, initiating Safe Stop 1 with STO and guard door unlock at standstill speed. This trend file, Axis1_SS1, is available within the attached Logix project file under >Assets>Trends.

Item	Description
1	SLS is initiated. The drive speed reference is changed to the SLS velocity.
2	When SLS.CheckDelay time expires, the SLS instruction is monitoring SFX.ActualSpeed versus SLS.ActiveLimit speed. The SLS instruction finds the SFX.ActualSpeed is greater than SLS.ActiveLimit speed, Armor PowerFlex passthrough tag SLSLimit and SLS.StopReq are set true. This setting causes SAF_RunPerm to go false, which then triggers an SS1.Req and a drive normal stop via the Armor PowerFlex passthrough tag SS1Active going true.
3	SS1.StopMonDelay provides time for the drive to begin deceleration repeatably. When the SS1.StopMonDelayActive goes false, the SS1 instruction monitors SFX.ActualSpeed versus SS1.SpeedLimit during the ramp deceleration. If the SFX.ActualSpeed is less than the SS1.SpeedLimit speed the drive follows the normal deceleration during the SS1.StopDelay. If the SFX.ActualSpeed is greater than the SS1.SpeedLimit speed or SS1.StopDelay times out before standstill speed, the SS1 instruction faults initiating an immediate SS1.STO_Req.
4	When SFX.ActualSpeed is less than the SS1.StandstillSpd, SS1.STO_Req is set true, and the guard door is unlocked. To resume operation a Reset is required.

Safe Stop 1 must be configured for the application. A trend can be used to verify the load deceleration response and timing that is required for the safety function. The system dynamics must be understood to configure the SS1 to monitor deceleration repeatably without nuisance faulting.

Output STO – Safety Routine 020_STO

The output STO routine contains drive safety reset logic, device status summary, and the main run permissive.

Table 9 - Drive Safety Reset Request

Tag	Description
STOOutput	Must be on to reset drive safety

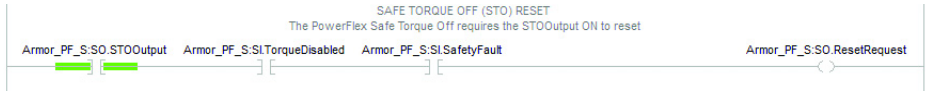
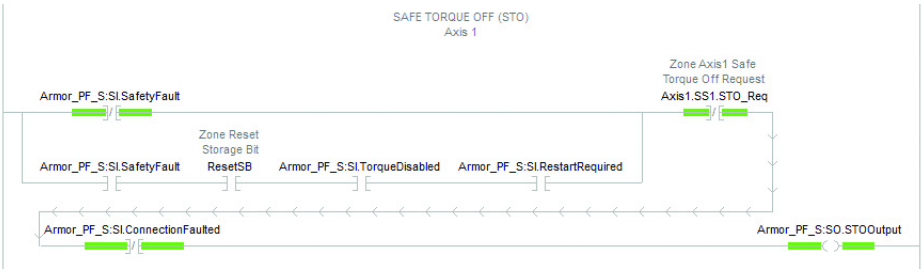
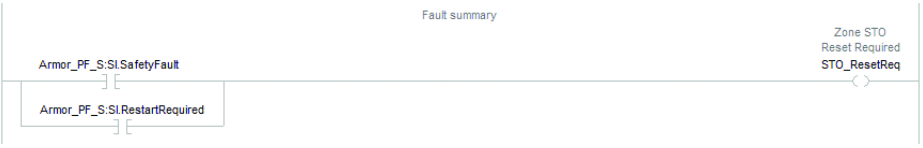


Table 10 - STO Output - True is Drive Enabled, False is Drive Disabled

Tag	Description
No Safety Fault	Follow the SS1.STO_Req
Safety Fault	Turn on STO when reset and all interlock conditions are met.



STO reset required indication:

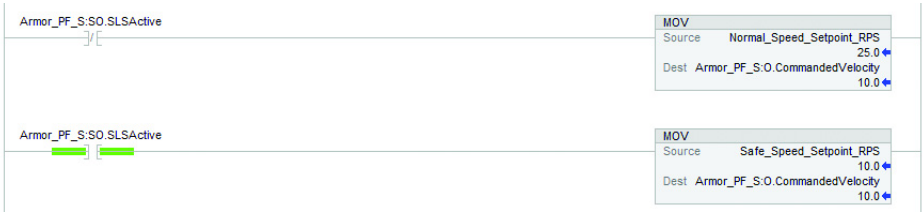


Standard Task Drive Control — R01_StartStopReset

The drive control routine provides drive speed reference selection for SLS.

Table 11 - Drive Safely-limited Speed Reference Request

Tag	Description
SLSActive	Armor PowerFlex safety output tag, indicates that SLS is requested and is used to select the drive SLS reference during SLS monitoring.
MOV	Move instructions transfer the drive speed reference between normal and safe speed references. The safe speed reference must be less than the SLS instruction Active Limit value.



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 that you chose. Depending on the devices you choose, the overall safety rating of your system is 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. The maximum MTTFd of 2500 years is supported starting in version 2.0.3 of SISTEMA. As a result, the same SISTEMA data file that is opened in different versions of SISTEMA can yield different calculated results.

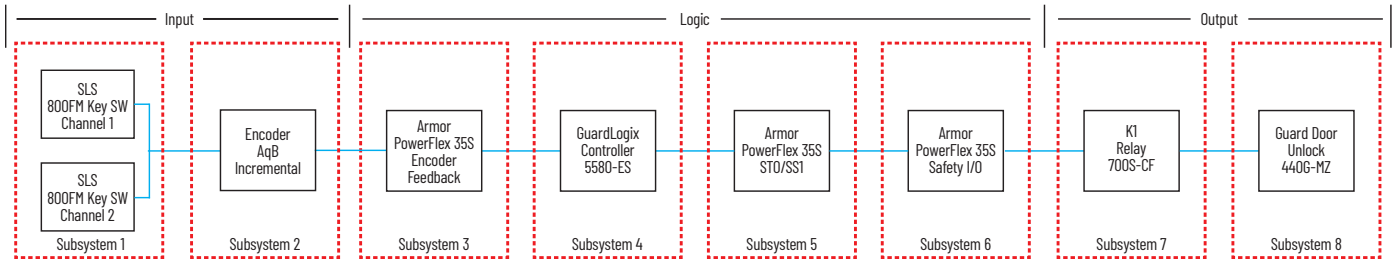
Status	Name	PL	PL-Software	PFHD [1/h]	Category	Requirements of the category	Use case
SB	Safety PLC: GuardLogix 1756-L8xES	d	d	6.4E-9	3	fulfilled	[Standard Use Case]
SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	3	fulfilled	[Standard Use Case]

Guard Door Unlock at Safely-limited Speed

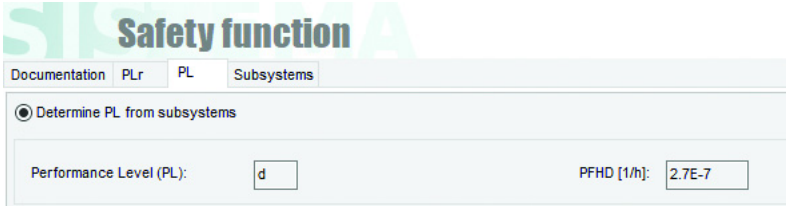
Assuming the use of the following subsystem choices, the overall Performance Level that is achieved is shown in the graphic.

Status	Name	Ref. des.:	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
SB	SLS Mode Select Key Swi...	01	e	n.a.	2.5E-8	80 (fulfilled)	99 (High)	100 (High)	3	fulfilled
SB	Incremental Encoder	02	e	n.a.	1.1E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
SB	AC Drive: Armor PowerFle...	03	d	d	3.3E-10	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	Safety PLC: GuardLogix 1...	04	d	d	6.4E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	AC Drive: Armor PowerFle...	05	d	d	1.8E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	AC Drive: Armor PowerFle...	06	d	d	1.3E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
SB	700SCF_Relay	07	d	n.a.	2.3E-7	65 (fulfilled)	99 (High)	100 (High)	2	fulfilled
SB	Guardmaster 440G-MZ Int...	08	e	n.a.	3.2E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

The Guard Door Unlock at Safely-limited Speed safety function can be modeled as follows:



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 2.7E-7. The PL for the complete safety function is PLd.

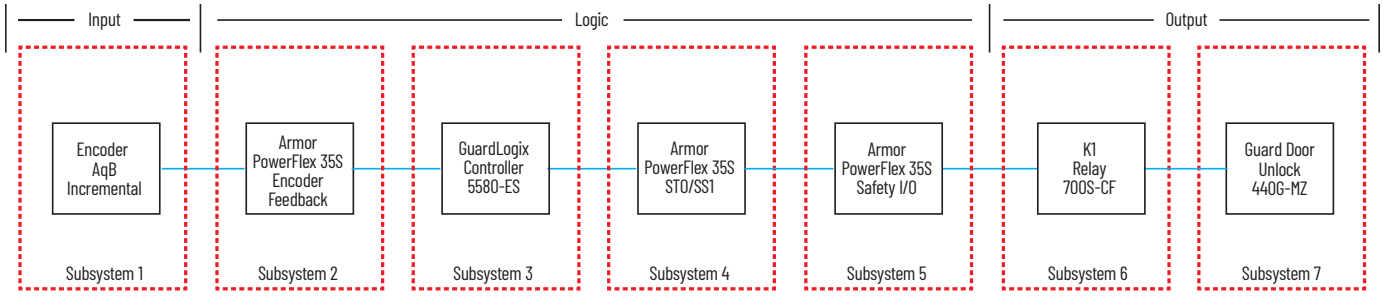


Guard Door Unlock at Zero Speed (SS1 and Standstill Monitoring)

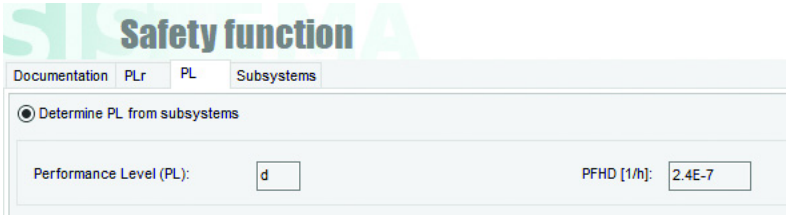
Assuming the use of the following subsystem choices, the overall Performance Level that is achieved is shown in the graphic.

Status	Name	Ref. des.:	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
SB	Incremental Encoder	01	e	n.a.	1.1E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
SB	AC Drive: Armor PowerFlex 35S Encoder Feedback	02	d	d	3.3E-10	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	Safety PLC: GuardLogix 1756-L8xES	03	d	d	6.4E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	AC Drive: Armor PowerFlex 35S Network STO/Timed SS1	04	d	d	1.8E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
SB	AC Drive: Armor PowerFlex 35S Safety IO	05	d	d	1.3E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
SB	700SCF_Relay	06	d	n.a.	2.3E-7	65 (fulfilled)	99 (High)	100 (High)	2	fulfilled
SB	Guardmaster 440G-MZ Interlocking Device with Guard Locking	07	e	n.a.	3.2E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

The Guard Door Unlock at Safely-limited Speed safety function can be modeled as follows:



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 2.4E-7. The PL for the complete safety function is PLd.

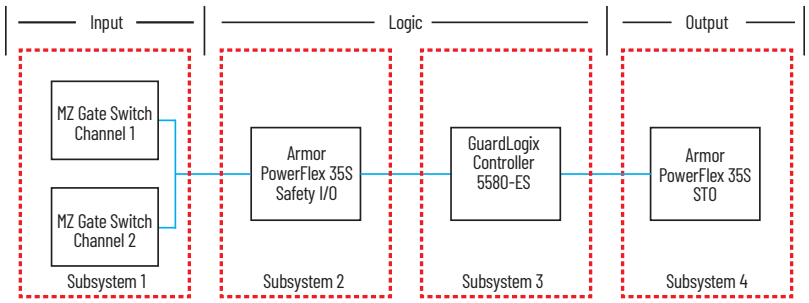


Prevention of Hazardous Motion using Guard Door Switch

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

Status	Name	Ref. des.:	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.	3.2E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	AC Drive: Armor PowerFlex 35S Safety IO	02	d	d	1.3E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	Safety PLC: GuardLogix 1756-L8xES	03	d	d	6.4E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔ SB	AC Drive: Armor PowerFlex 35S Network STO/Timed SS1	04	d	d	1.8E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled

The prevention of hazardous motion with the guard door switch safety function can be modeled as follows:



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

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 on page 29 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.
Rockwell Automation Functional Safety Data Sheet, publication SAFETY-SR001	Provides functional safety data for Rockwell Automation® products.
440G-MZ Guardmaster® Guard Locking Switch User Manual, publication 440G-UM004	Provides information on how to install and operate the 440G-MZ guard locking switch.
Armor PowerFlex AC Drive User Manual, publication 35-UM001	Provides information on how to install, configure, and program the Armor PowerFlex AC drive.
Armor PowerFlex AC Drive Technical Data Manual, publication 35-TD001	Provides specifications and technical details of the Armor PowerFlex AC drive.
Bulletin 700 Relay and Timer Specifications Technical Data, publication 700-TD552	Provides technical documentation about the 700S-CF safety relays.
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-AT201A-EN-P - August 2023