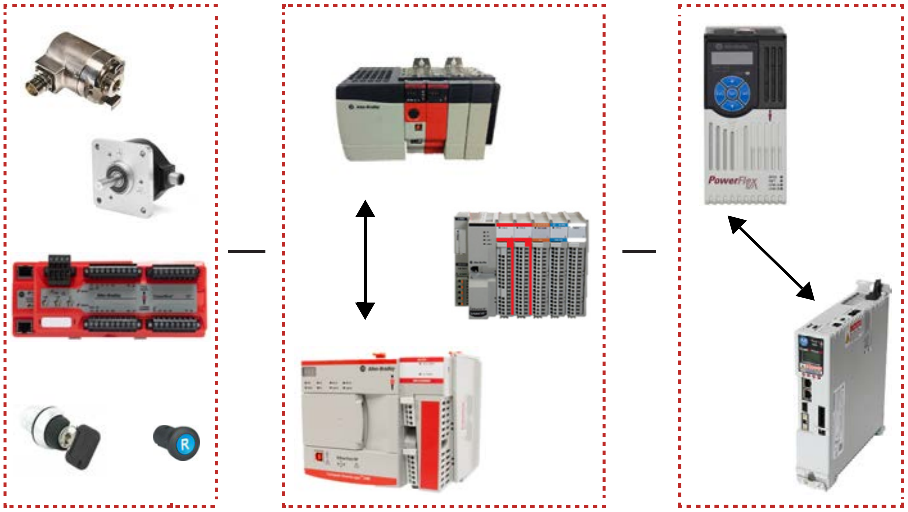
Application Technique

Original Instructions

Safely-limited Speed and Safely-limited Position via a GuardLogix Controller Safety Function

Products: 842HR Encoder, 847H Encoder, 1791ES-ID2SSIR CompactBlock Guard I/O Module, GuardLogix 5580 or Compact GuardLogix 5380 Controller, 5069 Compact I/O Safety Module, Kinetix 5500 or PowerFlex 527 Drive with Networked Safe Torque Off

Safety Rating: Cat. 3, PLe to ISO 13849-1: 2015



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 configure and program a GuardLogix® 5580 controller and a 1791ES-ID2SSIR CompactBlock™ Guard I/O™ module to perform the safely-limited speed (SLS) and the safely-limited position (SLP) safety functions. This document also includes a safe stop (SS1) safety function.

This example assumes the use of two encoders that are connected to channel 0 and channel 1 inputs of the 1791ES-ID2SSIR module. You can select the type of the two encoders based on your motor requirements so that a dual channel system with diagnostic coverage (DC) of 99% can be achieved.

This example uses a two-position, maintained-key selector switch to separately request SLS and SLP. When the key is in the active mode position, low (0), the key can be removed to preserve mode activation while the task that requires the safety functions is performed.

In the GuardLogix safety task, Drive Safety instructions are used to provide actual speed and position (SFX instruction), initiate, and monitor the SLS and SLP safety functions. When the SLS limit or the SLP limit is exceeded, while the SLS and SLP instructions are active, the GuardLogix controller de-energizes the final control device, in this case a Kinetix® 5500 or PowerFlex® 527 safety drive.

Because the Kinetix 5500 drive and the PowerFlex drive do not have advanced safety capabilities, the safety actions have to be executed in the GuardLogix safety program. Standard motion logic is executed when SLS or SLP are requested. The use of the term standard motion program is used throughout this document. It implies the use of the Motion Instruction library, so when this term is used, consider that it means different programming methods (logic with the Add On Profile (AOP)) to control the PowerFlex or Kinetix drive and motor. If the standard motion logic is not executed properly, the Drive Safety instructions detect this condition and maintain a safe machine state. The safety function, by itself, does not control the motor. The standard motion logic is used to manage control of the motor based on the safety function that is executing.

The example uses the 1791ES-ID2SSIR module that provides dual-feedback monitoring. The dual-channel system structure is used to fulfill the SLS- and SLP-required performance level for this example (Ple), without fault exclusion.

Discrepancy checking between the feedback of the two channels aids the achievement of the high Diagnostic Coverage required to achieve Ple.

The purpose of discrepancy checking is to perform an evaluation of the speed and position discrepancy between channel 0 and channel 1 feedback.

IMPORTANT All monitoring functions are based on the speed and position output of the channel 0 SFX instruction.
The channel 1 signal is used for fault diagnostics.

When using two independent encoders to monitor motion, and when they are installed in a manner to avoid any common cause dangerous failure, the 1791ES-ID2SSIR module can be used in applications up to and including SIL CL 3, and cat. 4, PLe.

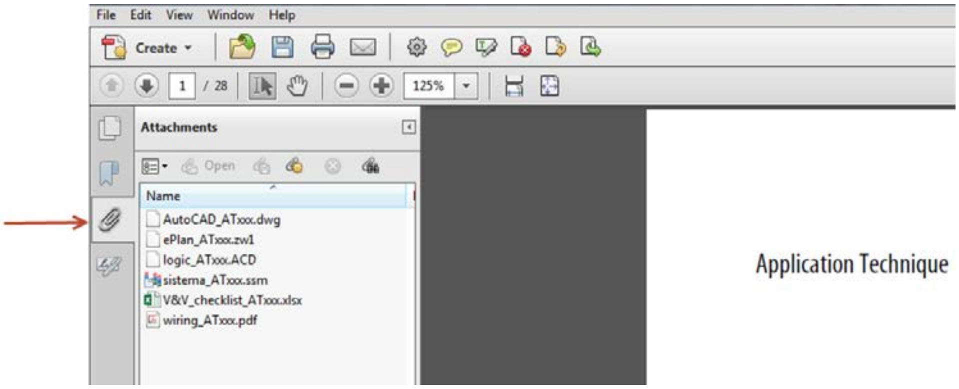
This example uses a 1756-L84ES GuardLogix controller, but you can substitute a Compact GuardLogix controller that supports the safety rating that is demonstrated in this safety function application technique. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) calculations 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.

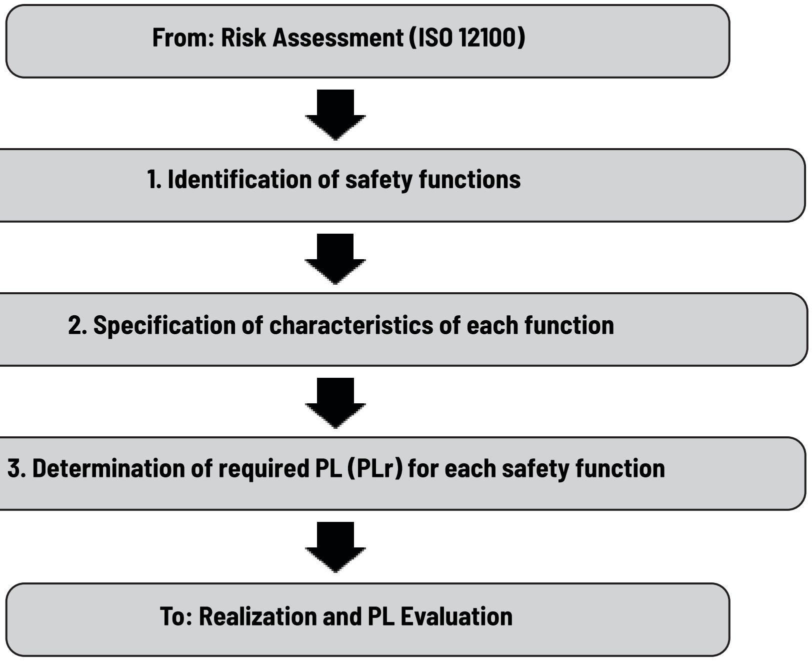
1. If you are viewing the PDF file in a browser and do not see the Attachments link 📎, download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link 📎.
3. Right-click the desired file and save it.



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 e (cat. 3, PLe), 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.


From: Risk Assessment (ISO 12100)
1. Identification of safety functions
2. Specification of characteristics of each function
3. Determination of required PL (PLr) for each safety function
To: Realization and PL Evaluation

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

Safety Functions

This application technique includes three safety functions:

- Safely-limited speed (SLS)
- Safely-limited position (SLP)
- Safe stop 1 (SS1)

Safety Function Requirements

The SS1 safety function is triggered by an SLS or SLP safe monitoring safety function to monitor that the motor stops in a controlled manner. When the motor speed is at or below the Standstill Speed, a Safe Torque Off (STO) in the drive is initiated.

SLS and SLP can be activated independently from each other.

The following sections describe the requirements for both the SLS, SLP, and SS1 safety functions.

Safely-limited Speed Requirements

When SLS is requested, the motor speed must go below the programmed speed limit before the SLS Check Delay time expires. After the delay expires, the speed must remain below the limit.

IMPORTANT You must perform a risk assessment to determine the safely-limited speed for the motor.

If the programmed speed limit is exceeded after the delay expires, an SS1 is initiated to stop the motor. When the motor reaches standstill speed, the SS1 initiates a safe torque-off (STO) function that disables the motor and removes the ability to produce torque.

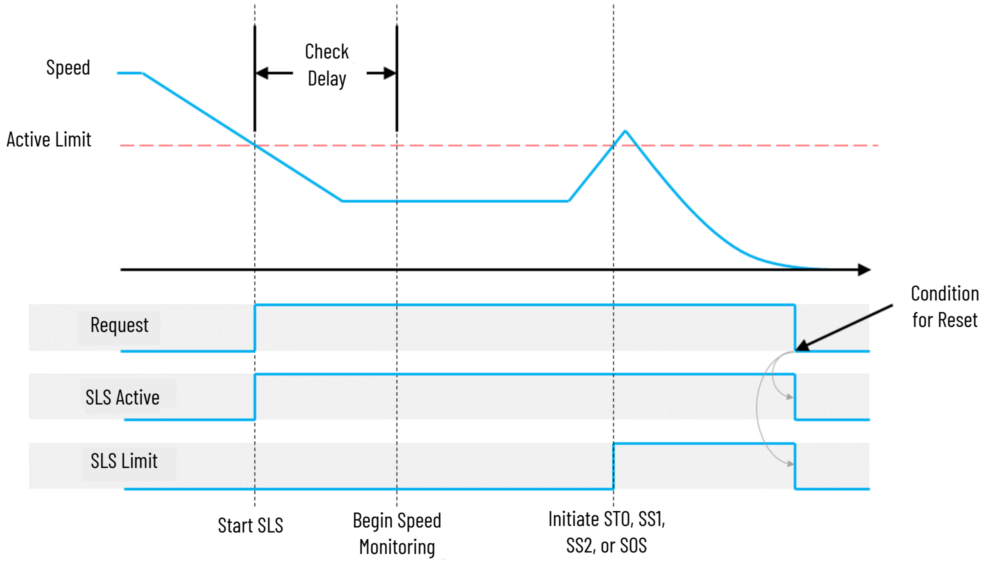
A two-position, maintained-key selector switch is used to request SLS. When the key is in the SLS mode position, the key can be removed to preserve SLS mode while the task that requires SLS is performed.

Safely-limited Speed Functional Safety Description

For tasks that require hazardous motion, a safety function that limits and monitors the speed of the motor can be used to help to avoid or reduce harm.

Normal Operation, Automatic Restart

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 high (1). The SLS Limit, once set, remains high (1) until the SLS function is reset. For automatic restart operation, the SLS function is reset when the request is cleared low (0), provided no SLS faults have occurred.



SLS Operation

The SLS function operates in the following sequence.

1. Enable SLS monitoring:
   - While the motor is at speed, the SLS request is set high (1) when there are no faults with the Drive Safety instructions (SFX, SS1, and SLS).
   - The SLS request must remain high (1) throughout the SLS procedure.

- After SLS is requested, the motion application program is signaled that an SLS instruction is active, by using the SLS_instruction.SLS_Active output bit.
- Standard motion instructions are used to bring the motor speed below the SLS Active Limit.
- SLS monitoring begins after a programmable Check Delay expires (3 seconds in this example).
- The SLS instruction monitors the motor speed and remains active while the motor speed is below the programmed SLS Active Limit.

2. When the task that requires SLS has been completed, the SLS request is removed.
3. 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, an SS1 function is requested.

When the SS1 function indicates that standstill speed is reached, the STO request is made. When STO is complete, the torque-producing ability of the motor is disabled. To recover, follow these steps.

1. Remove the SLS request.
2. Press the Fault Reset push button.
3. To remove the STO condition so that the motor can be enabled, press the Safety Reset push button.

Recover from SS1 when SLS is Exceeded

The SLS request is assumed to be active when the speed limit is exceeded.

If the SLS Active Limit is exceeded after the programmable delay expires, an SS1 request is initiated. When the SS1 function indicates that standstill speed is reached, an STO request is automatically initiated as a result of the SS1, and when completed, removes the ability to produce motor torque. To recover, follow these steps.

1. Remove the SLS request.
2. To remove the STO condition so that the motor can be enabled, press the Safety Circuit Reset push button.

Safely-limited Position Requirements

The SLP instruction monitors the position of a motor or axis to confirm that the position does not deviate above or below defined limits.

When SLP is requested, the motor position must stay in between the programmed Positive Travel Limit and Negative Travel Limit before the SLP Check Delay time expires. After the delay expires, the position must remain above the Negative Travel Limit and below the Positive Travel Limit.

IMPORTANT You must perform a risk assessment to determine the safely-limited position for the motor.

If the motor position moves outside of the specified limits after the delay expires, an SS1 is initiated to stop the motor. When the motor reaches standstill speed, the SS1 initiates an STO function that disables the motor and removes the ability to produce torque.

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

IMPORTANT The SFX instruction must be homed before the SLP function operates.

Position values that are used in the SLP instruction are in Position units. A Position unit is user-defined according to the specific application and is configured in the SFX instruction.

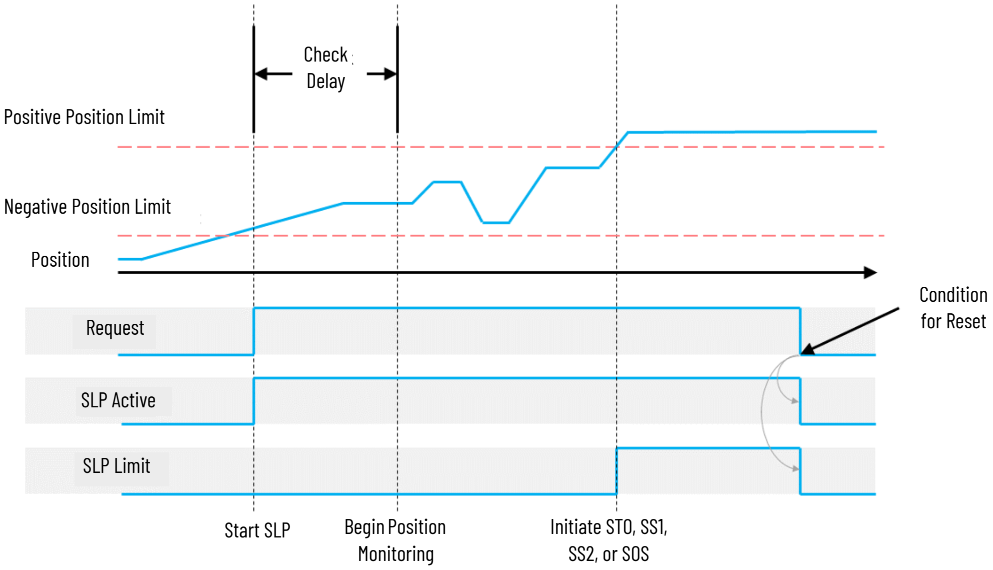
For more information on homing techniques, see Safe Homing for Position Safety Function Application Technique, publication SAFETY-AT183.

Safely-limited Position Functional Safety Description

For tasks that require hazardous motion, a safety function to limit and monitor the position of the motor can be used to help to reduce or avoid harm.

Normal Operation, Automatic Restart

Normal operation with Automatic Restart is shown in the following diagram. After Check Delay expires, the position must stay within the Positive Position Limit and Negative Position Limit, or the SLP Limit output is set to high (1). The SLP Limit, once set, remains high (1) until the SLP function is reset. For automatic restart operation, the SLP function is reset when the request is cleared low (0), provided no SLP faults have occurred.



SLP Operation

The SLP function operates in the following sequence:

1. Enable SLP monitoring.
    - While the motor is energized, the SLP request is set high (1) when there are no faults with the Drive Safety instructions (SFX, SS1, and SLP).
    - The SLP request must remain high (1) throughout the SLP procedure.
    - After SLP is requested, the motion application program is signaled that an SLP instruction is active, by using the SLP_instruction.SLP_Active output bit.
    - Standard motion instructions are used to keep the motor position within the Positive Position Limit and Negative Position Limit.
    - SLP monitoring begins after a programmable Check Delay expires (3 seconds in this example).
    - SLP monitors the motor position and remains active while the motor position is above the Negative Position Limit and below the Positive Position Limit.
2. When the task that requires SLP has been completed, the SLP request is removed.
3. The motor position can now be moved outside the limits.

Recover from SS1 due to Time Delay Expiration

If the position does not go inside the programmed Positive and Negative Position limits before the delay expires, an SS1 is requested.

When the SS1 function indicates that standstill speed is reached, the STO request is made. When STO is complete, the torque-producing ability of the motor is disabled. To recover, follow these steps.

1. Remove the SLP request.
2. To remove the STO condition so that the motor can be enabled, press the Safety Circuit Reset push button.

Recover from SS1 when SLP is Exceeded

The SLP request is assumed to be active when the position limit is exceeded.

If the position goes outside the programmed Positive and Negative Position limits after the programmable delay expires, an SS1 request is initiated. When the SS1 function indicates that standstill speed is reached, an STO request is automatically initiated as a result of the SS1, and when completed, removes the ability to produce motor torque. To recover, follow these steps.

1. Remove the SLP request.
2. To remove the STO condition so that the motor can be enabled, press the Safety Circuit Reset push button.

Diagnostics

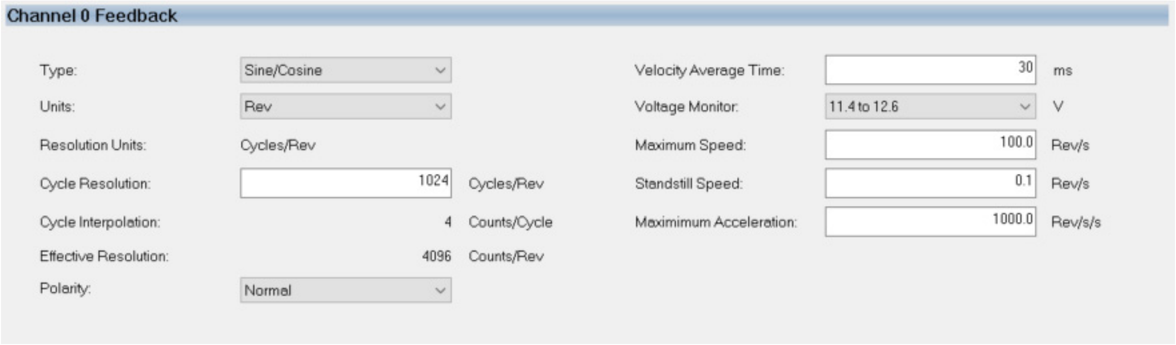
The purpose of a diagnostic is to check whether faults can be detected and to verify that 99% diagnostic coverage is achieved. Diagnostic coverage of 99% is a precondition for satisfying the cat. 4 dual-channel architecture requirements in accordance with ISO 13849-1. Depending on the encoder type, the module performs several diagnostic tests on encoder signals to detect faults in the encoder. You must determine if the combination of the selected encoder device type and the diagnostics that are described in this chapter satisfy the required safety function rating. The use of non-safety, standard encoders can require further analysis and assessment activities. The following encoder diagnostics are available for all supported encoder types:

- Encoder Voltage Monitoring
- Maximum Speed Limit
- Maximum Acceleration

IMPORTANT The configured diagnostic parameters that are shown in this document are solely examples. You must perform a risk assessment to determine the encoder diagnostics parameter.

842HR Encoder Diagnostic

In this example, the diagnostic is set for the 842HR Encoder.



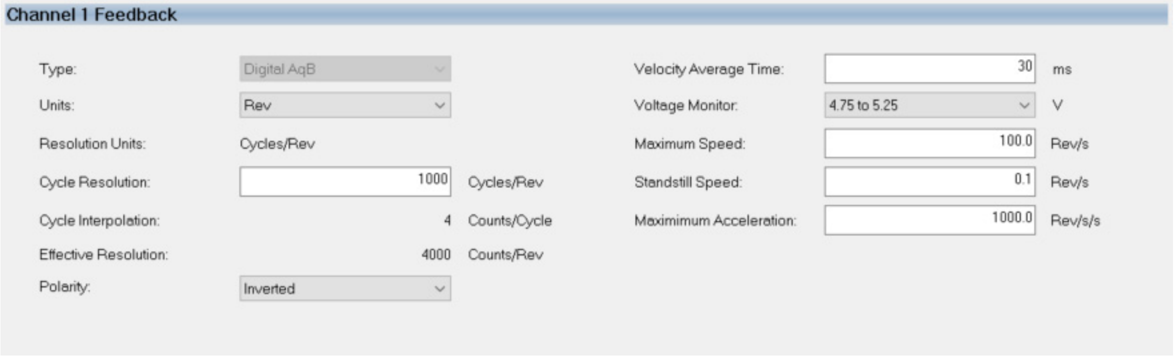
Channel 0 Feedback

Type: Sine/Cosine
Units: Rev
Resolution Units: Cycles/Rev
Cycle Resolution: 1024 Cycles/Rev
Cycle Interpolation: 4 Counts/Cycle
Effective Resolution: 4096 Counts/Rev
Polarity: Normal

Velocity Average Time: 30 ms
Voltage Monitor: 11.4 to 12.6 V
Maximum Speed: 100.0 Rev/s
Standstill Speed: 0.1 Rev/s
Maximimum Acceleration: 1000.0 Rev/s/s

847H Encoder Diagnostic

In this example, the diagnostic is set for the 847H Encoder.



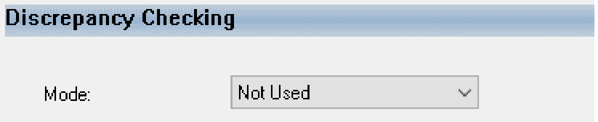
Channel 1 Feedback

Type: Digital AqB
Units: Rev
Resolution Units: Cycles/Rev
Cycle Resolution: 1000 Cycles/Rev
Cycle Interpolation: 4 Counts/Cycle
Effective Resolution: 4000 Counts/Rev
Polarity: Inverted

Velocity Average Time: 30 ms
Voltage Monitor: 4.75 to 5.25 V
Maximum Speed: 100.0 Rev/s
Standstill Speed: 0.1 Rev/s
Maximimum Acceleration: 1000.0 Rev/s/s

Dual Encoder Velocity and/or Position Discrepancy Checking

In this example, the module Discrepancy Checking is disabled.



Discrepancy Checking

Mode: Not Used

The Dual Encoder Velocity and/or Position Discrepancy diagnostic function is performed in the controller safety task.

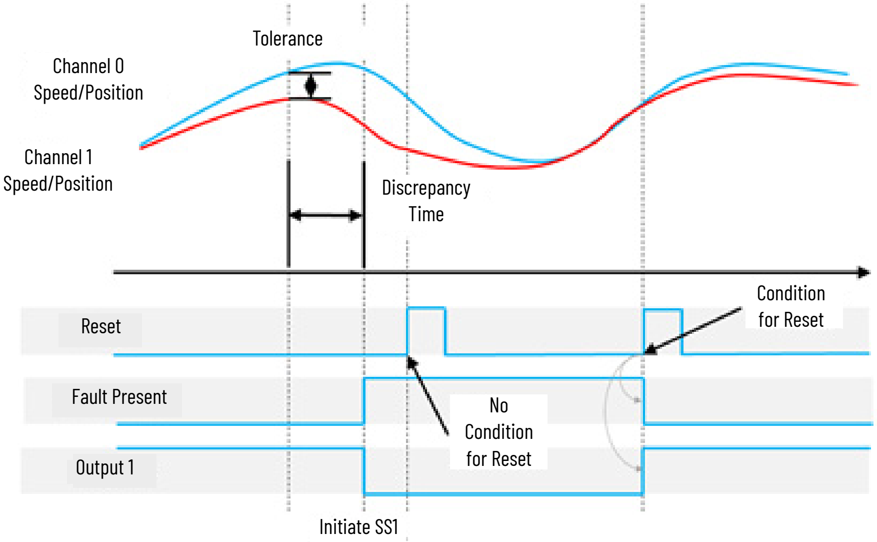
Discrepancy Checking monitors the channel 0 versus channel 1 feedback values for consistency within the specified Tolerance limit boundary by using the Dual-channel Analog Input Floating Point (DCAF) instruction. The Discrepancy Checking monitor is always active and, if the DCAF instruction detects a discrepancy between the two channels for more than the Discrepancy Time, an SS1 request is initiated.

The cross-evaluation of the two feedback signals allows detection of several faults, such as mechanical coupling faults, interchanging of sine and cosine, inversion and the breakage of the drive shaft of rotary measuring systems, or freezing of digitized analog values for the sine and cosine.

IMPORTANT Channel 0 feedback is used for safe monitoring functions (SLS, SLP, and SS1).
Channel 1 feedback is used for Discrepancy Checking diagnostics (DCAF).
Discrepancy Checking is always active.

Recover from Discrepancy Fault (Manual Restart)

The timing diagram illustrates a fault occurring when the difference between channel 0 and channel 1 exceeds the Tolerance for longer than the Discrepancy Time. When channel 0 and channel 1 go out of Tolerance, the discrepancy timer starts. If the two channels stay out of Tolerance for at least the configured Discrepancy Time, a discrepancy fault occurs. The fault cannot be cleared while the difference between the two channels is greater than the Tolerance. When the difference between the two channel inputs falls within the Tolerance, press the Fault Reset push button to clear the fault.



Integrated Safety: Safe Torque Off Considerations for a Stop Category 1

In the event of a malfunction, the most likely stop category is stop category 0. When designing the machine application, timing and distance must be considered for a coast-to-stop action, and the possibility of the loss of control of a vertical load. These malfunctions include a transition (programmatic or keyswitch) from Run to Program mode, or any loss of communications that drops out the STO networked tags. Use additional protective measures if this occurrence might introduce unacceptable risks to personnel.

Bill of Material

This application technique uses these products.

Cat. No.	Description	Quantity
800FP-F611PX10V	800F push button, (fault reset), plastic, flush, blue, R, plastic latch mount, 1 N.O. contact, 0 N.C. contact, low voltage, standard pack (qty. 1)	1
800FP-G1PX10V	800F push button, (safety reset), plastic, guarded, white, no legend, plastic latch mount, 1 N.O. contact, 0 N.C. contact, low voltage, standard pack (qty. 1)	1
800FM-KM22XM02	Two-position key selector switch, metal, maintained, right key removal, 2 N.C. contacts	2
5069-AEN2TR[1]	5069 Compact I/O™ EtherNet/IP adapter	1
5069-RTB64-SCREW	5069 Compact I/O power terminal RTB kit for both 4- and 6-pin screw type	1
5069-IB8S	5069 Compact I/O 8-channel safety sink input module	1
5069-RTB18-SCREW	5069 Compact I/O 18-pin screw type terminal block	1
1791ES-ID2SSIR	EtherNet/IP safety CompactBlock™ input module, 2-channel incremental encoder / serial synchronous interface	1
1606-XLP15E	1606-XLP15E: Compact power supply, 24…28V DC, 15 W, 120/240V AC input voltage	1
842HR-MJA4115FWYD	842HR sine cosine/serial encoder multi-turn (4096 turns), hub shaft, 10 mm (.39 in.) blind hollow shaft, 5…12V DC, M23 17-pin connector	1
1606-XLP15A	1606-XLP15B: compact power supply, 12…15V DC, 15 W, 120/240V AC input voltage	1
2090-XXNFMF-S02	Cable, feedback, DIN Type 4-connector, non-flex, flying lead, 2 m (6.56 ft)	1
847H-DL14-RG01000	Incremental encoder, standard square flange, 10 mm (.39 in.) diameter shaft with flat, 4.5…5.5V line driver, TTL (A-Leads-B, CW, Z gated with A), MS connector, 10-pin with mating connector, 1000 pulses per revolution	1
1606-XLP15A	1606-XLP15A: compact power supply, 5…5.5V DC, 15 W, 120/240V AC input voltage	1
845-10P	Mating connector, 10-pin, straight, (845F, H, T, PY)	1

[1] Only required for the GuardLogix 5580S option, if the Compact GuardLogix 5380S option is selected the 5069 safety modules are used as local I/Os.

Choose one of the following safety-controller hardware groups.

Controller	Cat. No.	Description {Fill in SAP description}	Quantity
GuardLogix 5580[1]	1756-L81ES 1756-L82ES 1756-L83ES 1756-L84ES	GuardLogix processor, 3 MB standard memory, 1.5 MB safety memory GuardLogix processor, 5 MB standard memory, 2.5 MB safety memory GuardLogix processor, 10 MB standard memory, 5 MB safety memory GuardLogix processor, 20 MB standard memory, 6 MB safety memory	1
	1756-L8SP	GuardLogix 5580, safety partner controller	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 3	5069-L306ERMS3 5069-L310ERMS3 5069-L320ERMS3 5069-L330ERMS3 5069-L340ERMS3 5069-L350ERMS3 5069-L380ERMS3 5069-L3100ERMS3	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	1
	1606-XLP72E	Compact power supply, 24…28V DC, 72 W, 120/240V AC 1 5069-	1
	5069-ECR	Right end cap and terminator	1

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

Choose either a Kinetix 5500 or PowerFlex 527 drive.

Cat. No.	Description	Quantity
2198-xxx-ERS2	Kinetix 5500 servo drive with integrated safe torque-off on the EtherNet/IP network, any ratings	1
	or	
25C-xxx	PowerFlex 527 drive, any ratings	1

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.

System Overview

In this example, SLS and/or SLP mode can be requested via their dedicated two-position, maintained-key selector switch. The mode request selector switches are wired to the 5069-IB8S safety input module.

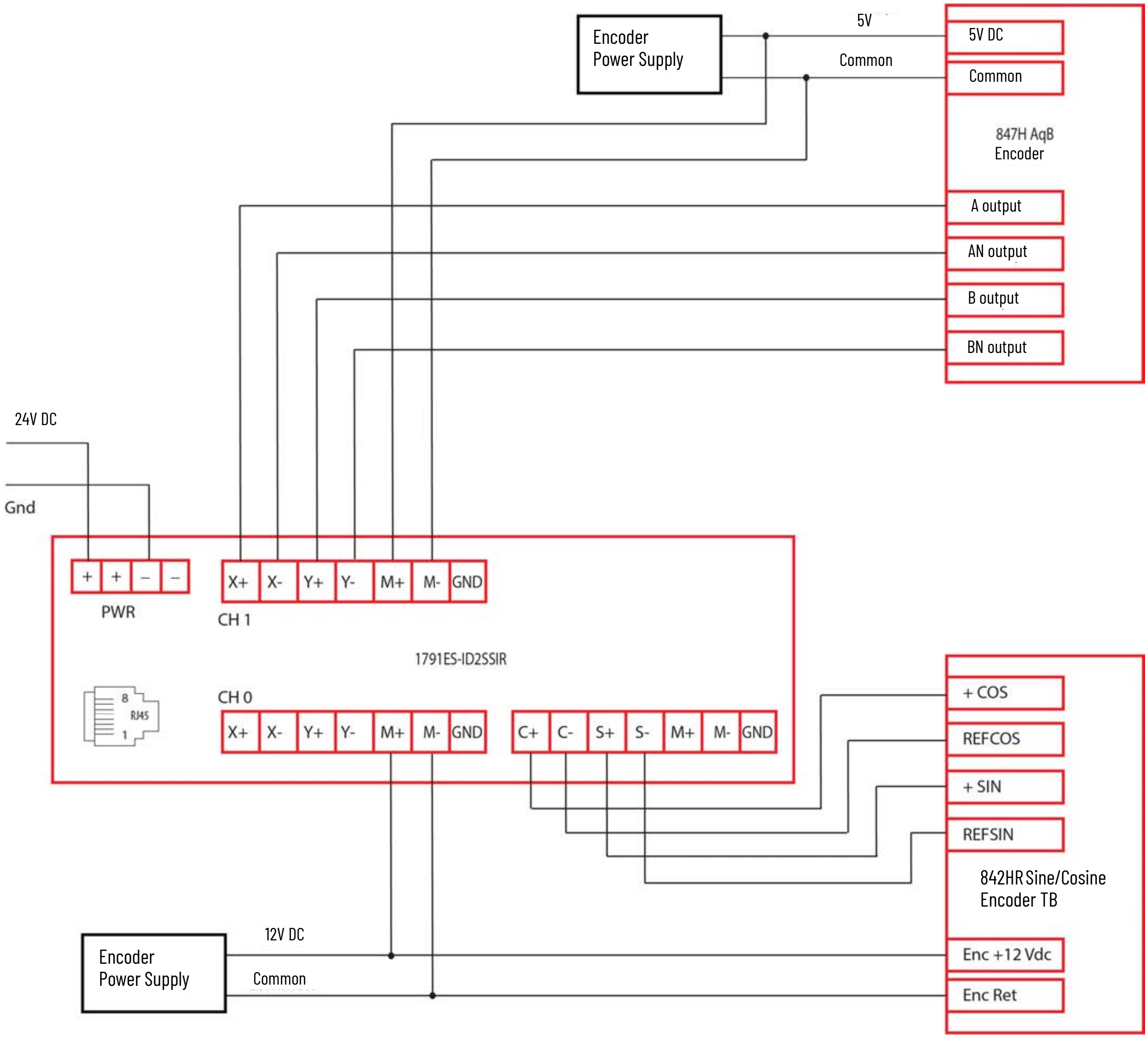
Test outputs are used to source the 24V DC for the SLS and SLP mode key selector switches. The SLS and SLP mode key switches are sourced from two separated pairs of test outputs. Sourcing multiple devices from one pair of test outputs has no effect on safety integrity, because the diagnostic coverage is not affected, but it does reduce diagnostic granularity as any single-channel short to 24V DC is proliferated to both devices.

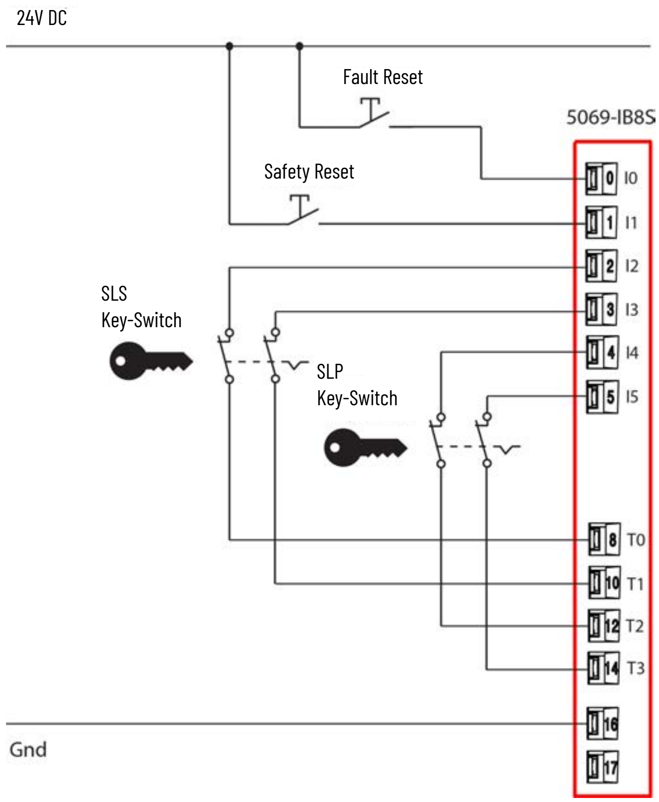
The Fault Reset and Safety Reset buttons are all wired to the 5069-IB8S safety input module. This configuration is not required for functional safety. These two inputs could be wired to a standard input module.

The GuardLogix controller (by using the integrated Ethernet port) uses safety connections to the 5069-IB8S module over an EtherNet/IP network. CIP Safety™ protocol makes the network architecture a black channel, and thus not part of the safety (PL) calculation.

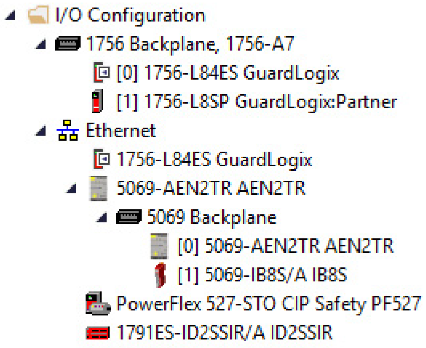
Electrical Schematic

For an electrical schematic in AutoCAD or EPLAN format, see the attached files.



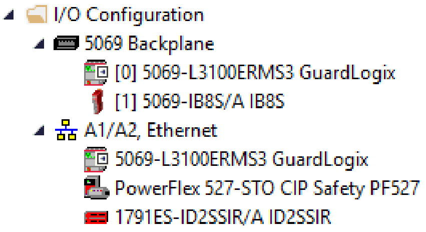


Network Architecture



- I/O Configuration
  - 1756 Backplane, 1756-A7
    - [0] 1756-L84ES GuardLogix
    - [1] 1756-L8SP GuardLogix:Partner
  - Ethernet
    - 1756-L84ES GuardLogix
    - 5069-AEN2TR AEN2TR
      - 5069 Backplane
        - [0] 5069-AEN2TR AEN2TR
        - [1] 5069-IB8S/A IB8S
    - PowerFlex 527-STO CIP Safety PF527
    - 1791ES-ID2SSIR/A ID2SSIR

GuardLogix 5580 Controller with remote Guard I/O



- I/O Configuration
  - 5069 Backplane
    - [0] 5069-L3100ERMS3 GuardLogix
    - [1] 5069-IB8S/A IB8S
  - A1/A2, Ethernet
    - 5069-L3100ERMS3 GuardLogix
    - PowerFlex 527-STO CIP Safety PF527
    - 1791ES-ID2SSIR/A ID2SSIR

GuardLogix 5380 Controller with local Guard I/O

Note: When using a GuardLogix 5580 controller, note that slot 1 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 31 or later. You must create a project and add the 1791ES-ID2SSIR, the drive (Kinetix 5500-ERS2 or PowerFlex 527) and appropriate safety and standard I/O modules. The integrated EtherNet/IP port on the GuardLogix controller is used, so no Ethernet bridge 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. The attached ACD file includes a GuardLogix 5580 controller, but if you choose a Compact GuardLogix 5380 controller, you can change the controller in the Logix Designer program.

Minimum Logix Designer Application Version	Product
31	GuardLogix 5580 controller
31	Compact GuardLogix 5380 controller

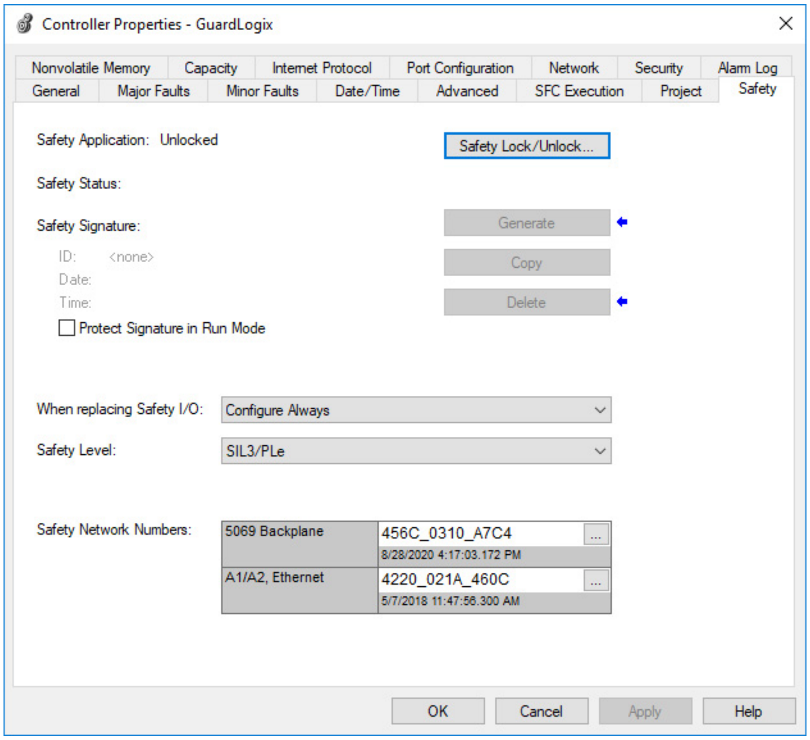
IMPORTANT Only the GuardLogix safety programming and configuration for SLS, SLP, and SS1 are shown in this example. Standard motion control required to satisfy the safety monitoring functions are out of scope of this document.

Create a Project with a GuardLogix Controller

If you are not using the attached ACD file, follow these steps to create a project.

GuardLogix Controller Properties

1. Create a GuardLogix project at revision 31. Revision 31 or later is a requirement for the SLS and SLP functions.
2. On the Safety tab for the controller, select SIL3/PLe in the Safety Level field.



Controller Properties - GuardLogix

Safety Application: Unlocked

Safety Status:

Safety Signature:

ID: <none>

Date:

Time:

☐ Protect Signature in Run Mode

When replacing Safety I/O: Configure Always

Safety Level: SIL3/PLe

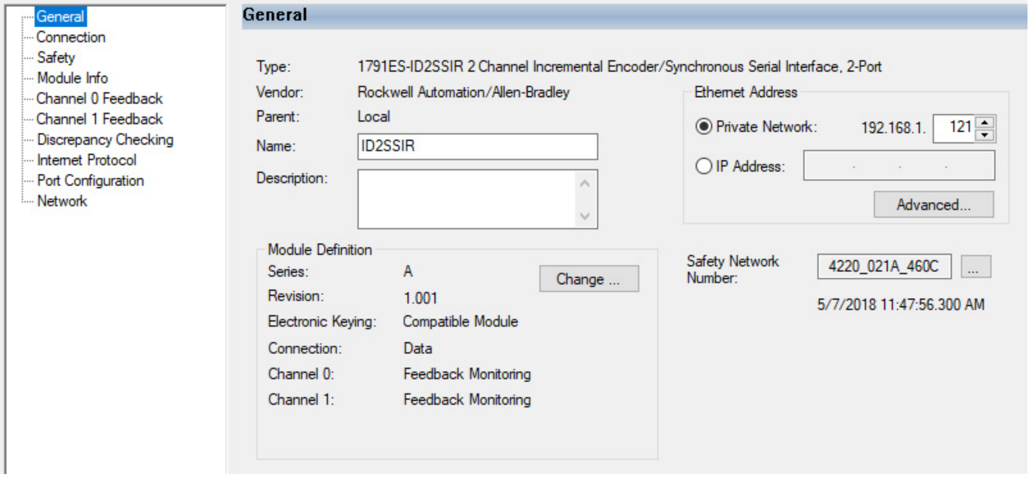
Safety Network Numbers:

5069 Backplane	456C_0310_A7C4 8/28/2020 4:17:03.172 PM
A1/A2, Ethernet	4220_021A_460C 5/7/2018 11:47:56.300 AM

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.

1791ES-ID2SSIR Module Configuration

1. Add the 1791ES-ID2SSIR module to the I/O configuration.
2. Configure the general safety properties of the 1791ES-ID2SSIR module as shown in the following screen capture.



General

Type: 1791ES-ID2SSIR 2 Channel Incremental Encoder/Synchronous Serial Interface, 2-Port

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name: ID2SSIR

Description:

Module Definition

Series: A

Revision: 1.001

Electronic Keying: Compatible Module

Connection: Data

Channel 0: Feedback Monitoring

Channel 1: Feedback Monitoring

Ethernet Address

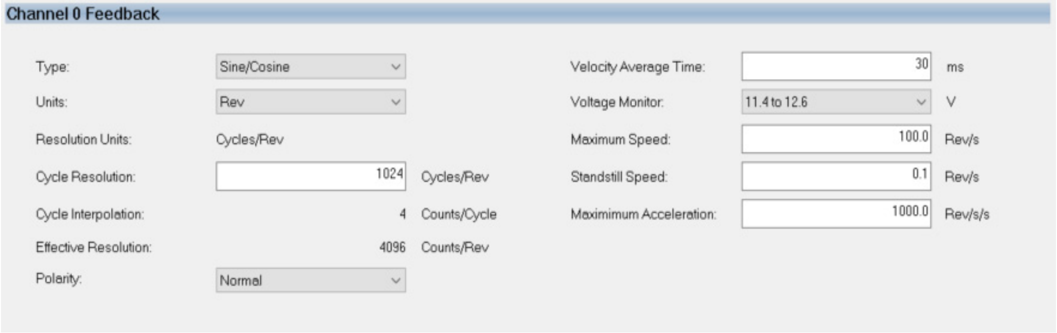
● Private Network: 192.168.1. 121

○ IP Address:

Safety Network Number: 4220_021A_460C

5/7/2018 11:47:56.300 AM

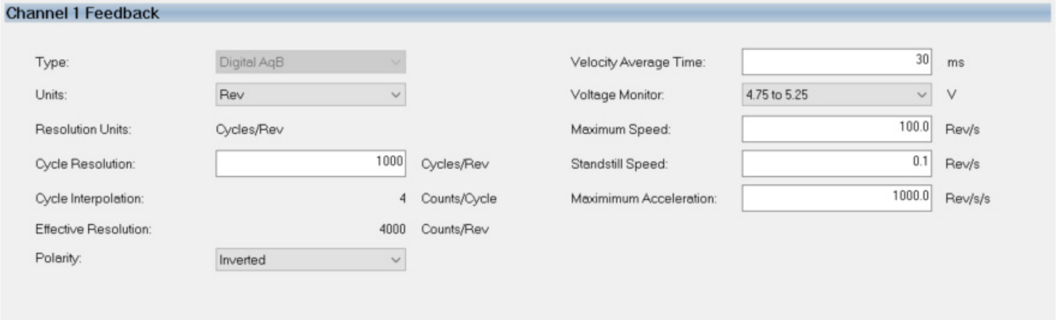
a. In the left panel, click Channel 0 Feedback, and in the Units field, select Rev.



Channel 0 Feedback

Type:	Sine/Cosine		Velocity Average Time:	30	ms
Units:	Rev		Voltage Monitor:	11.4 to 12.6	V
Resolution Units:	Cycles/Rev		Maximum Speed:	100.0	Rev/s
Cycle Resolution:	1024	Cycles/Rev	Standstill Speed:	0.1	Rev/s
Cycle Interpolation:	4	Counts/Cycle	Maximimum Acceleration:	1000.0	Rev/s/s
Effective Resolution:	4096	Counts/Rev			
Polarity:	Normal				

b. In the left panel, click Channel 1 Feedback, and in the Units field, select Rev.

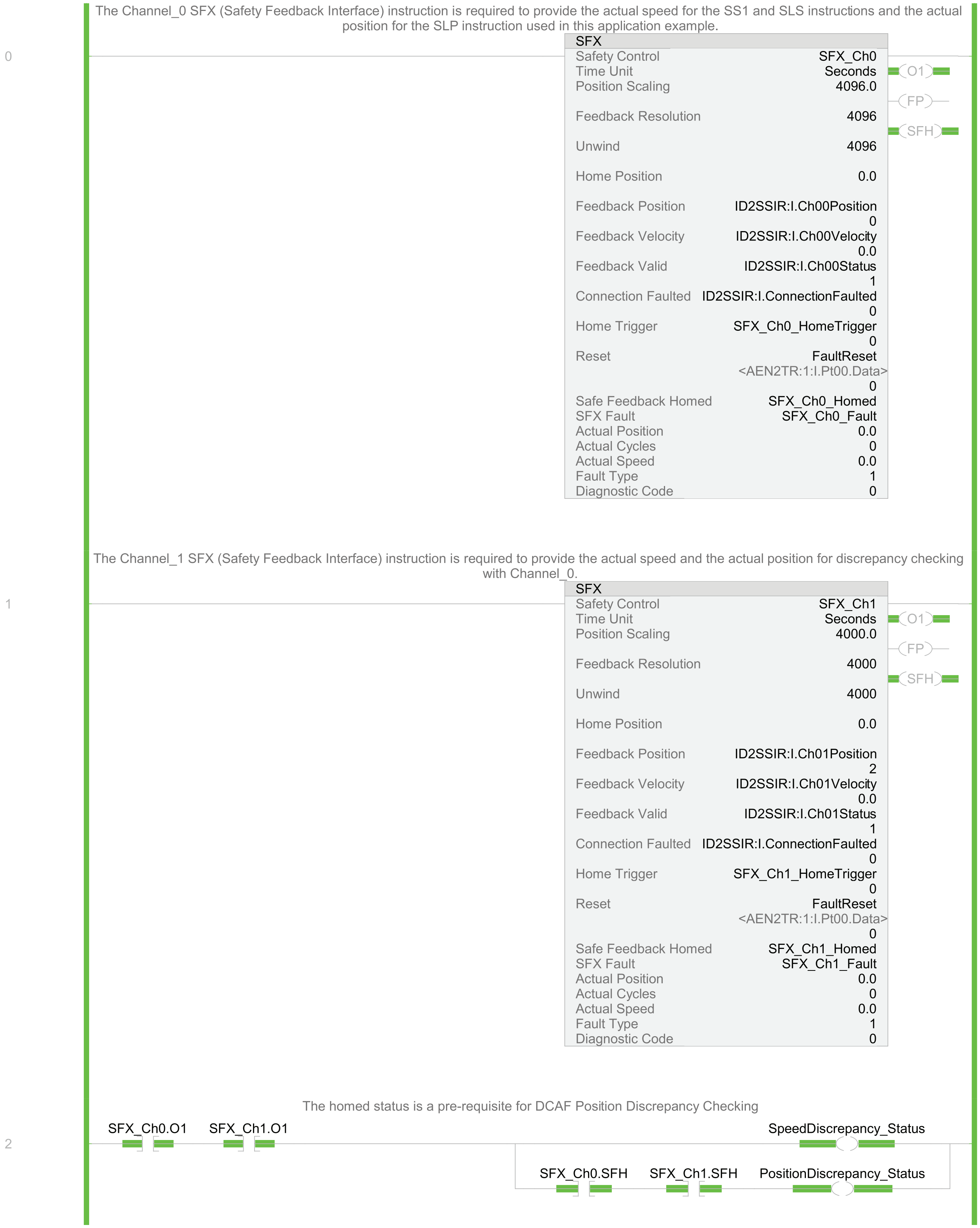


Channel 1 Feedback

Type:	Digital AqB		Velocity Average Time:	30	ms
Units:	Rev		Voltage Monitor:	4.75 to 5.25	V
Resolution Units:	Cycles/Rev		Maximum Speed:	100.0	Rev/s
Cycle Resolution:	1000	Cycles/Rev	Standstill Speed:	0.1	Rev/s
Cycle Interpolation:	4	Counts/Cycle	Maximimum Acceleration:	1000.0	Rev/s/s
Effective Resolution:	4000	Counts/Rev			
Polarity:	Inverted				

Programming

For controller logic that you can download to your controller, see the attached ACD file. The following example logic from the safety task is for the 5580 GuardLogix safety controller. The software documentation is embedded in the ACD file in the form of rung comments. Each rung contribution to the safety function is briefly explained.



0

The Channel_0 SFX (Safety Feedback Interface) instruction is required to provide the actual speed for the SS1 and SLS instructions and the actual position for the SLP instruction used in this application example.

SFX
Safety Control SFX_Ch0
Time Unit Seconds
Position Scaling 4096.0
Feedback Resolution 4096
Unwind 4096
Home Position 0.0
Feedback Position ID2SSIR:I.Ch00Position 0
Feedback Velocity ID2SSIR:I.Ch00Velocity 0.0
Feedback Valid ID2SSIR:I.Ch00Status 1
Connection Faulted ID2SSIR:I.ConnectionFaulted 0
Home Trigger SFX_Ch0_HomeTrigger 0
Reset FaultReset <AEN2TR:1:I.Pt00.Data> 0
Safe Feedback Homed SFX_Ch0_Homed
SFX Fault SFX_Ch0_Fault
Actual Position 0.0
Actual Cycles 0
Actual Speed 0.0
Fault Type 1
Diagnostic Code 0

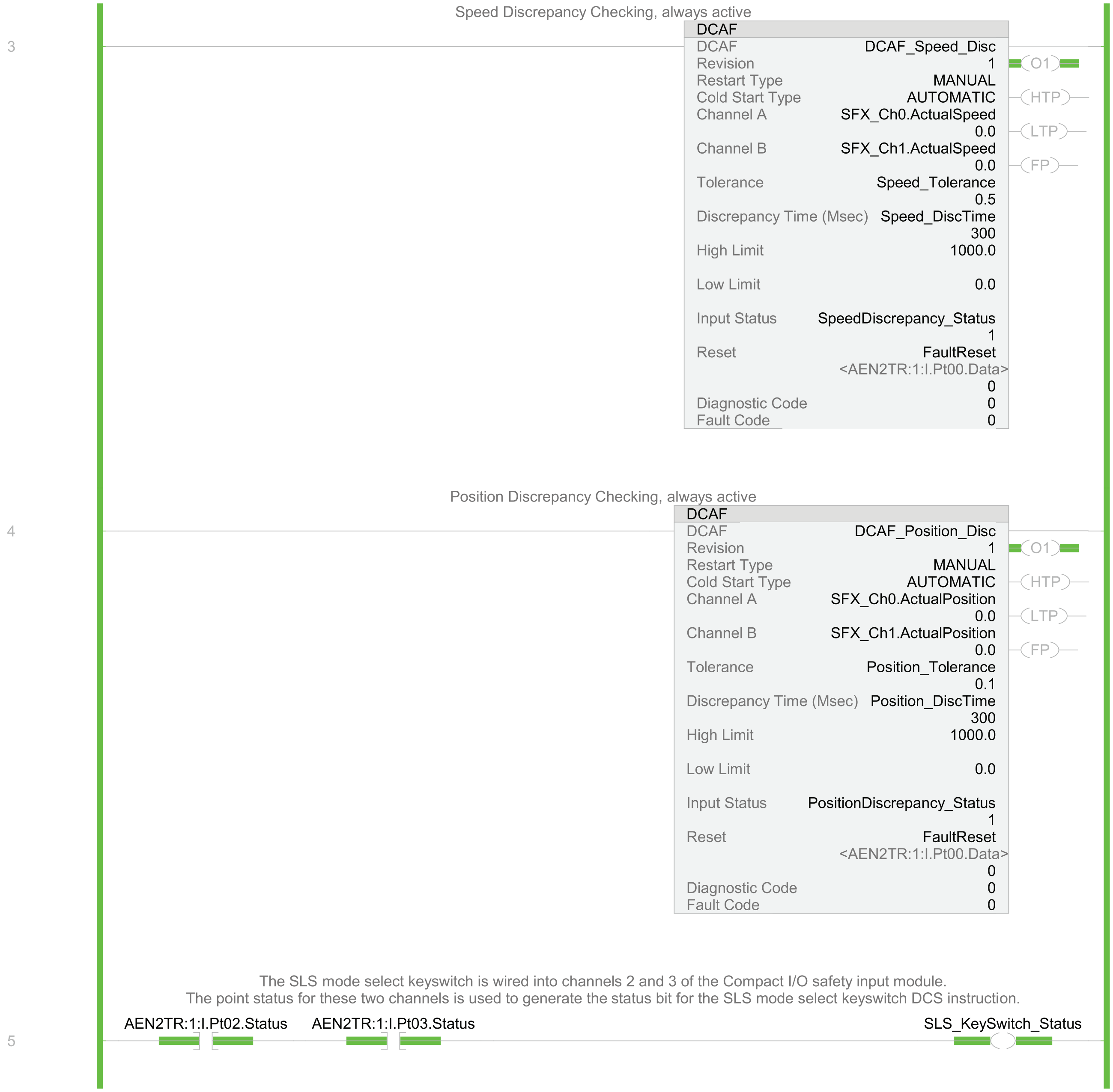
1

The Channel_1 SFX (Safety Feedback Interface) instruction is required to provide the actual speed and the actual position for discrepancy checking with Channel_0.

SFX
Safety Control SFX_Ch1
Time Unit Seconds
Position Scaling 4000.0
Feedback Resolution 4000
Unwind 4000
Home Position 0.0
Feedback Position ID2SSIR:I.Ch01Position 2
Feedback Velocity ID2SSIR:I.Ch01Velocity 0.0
Feedback Valid ID2SSIR:I.Ch01Status 1
Connection Faulted ID2SSIR:I.ConnectionFaulted 0
Home Trigger SFX_Ch1_HomeTrigger 0
Reset FaultReset <AEN2TR:1:I.Pt00.Data> 0
Safe Feedback Homed SFX_Ch1_Homed
SFX Fault SFX_Ch1_Fault
Actual Position 0.0
Actual Cycles 0
Actual Speed 0.0
Fault Type 1
Diagnostic Code 0

2

The homed status is a pre-requisite for DCAF Position Discrepancy Checking



3

Speed Discrepancy Checking, always active

DCAF	
DCAF	DCAF_Speed_Disc
Revision	1
Restart Type	MANUAL
Cold Start Type	AUTOMATIC
Channel A	SFX_Ch0.ActualSpeed 0.0
Channel B	SFX_Ch1.ActualSpeed 0.0
Tolerance	Speed_Tolerance 0.5
Discrepancy Time (Msec)	Speed_DiscTime 300
High Limit	1000.0
Low Limit	0.0
Input Status	SpeedDiscrepancy_Status 1
Reset	FaultReset <AEN2TR:1:I.Pt00.Data> 0
Diagnostic Code	0
Fault Code	0

4

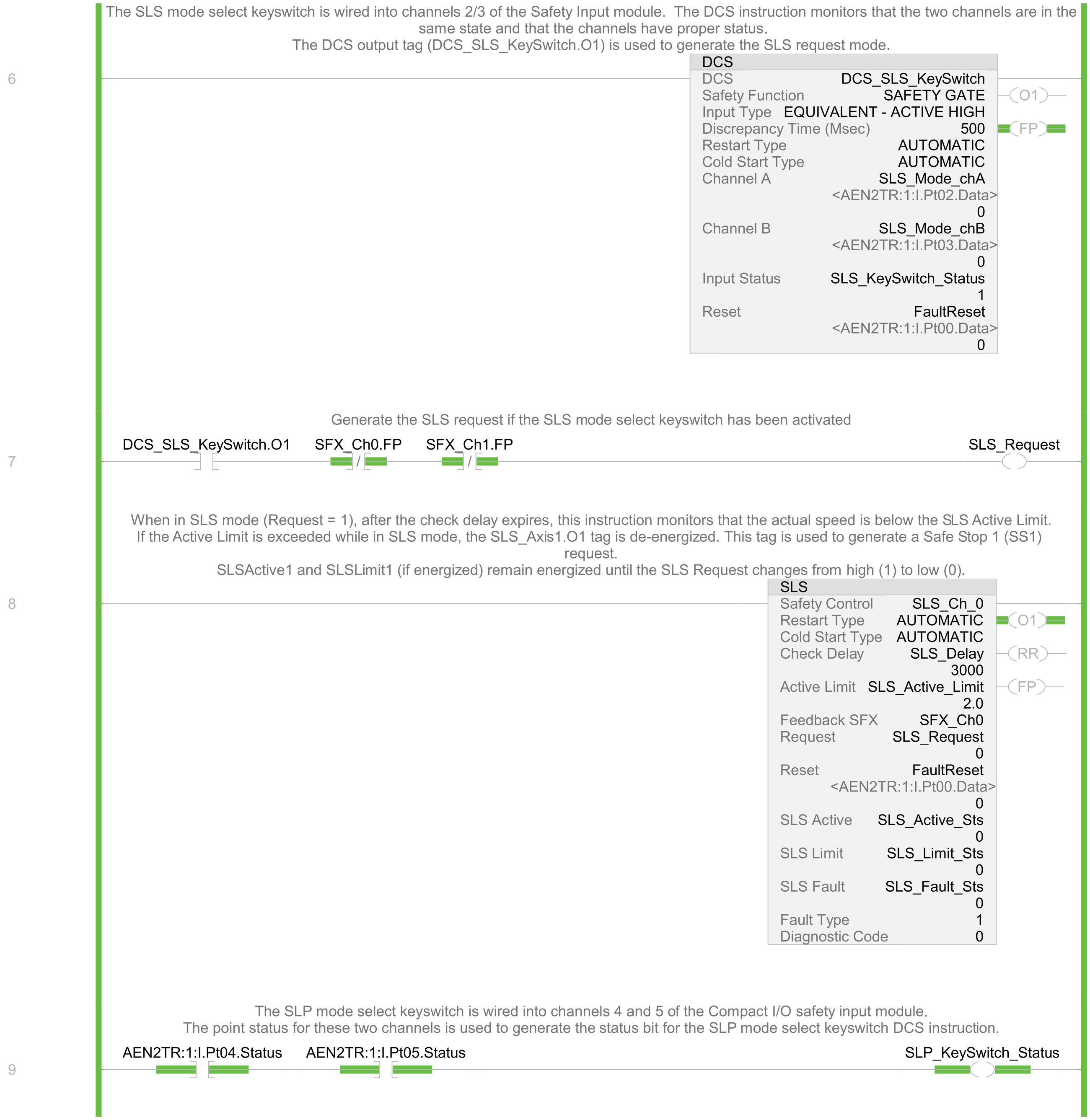
Position Discrepancy Checking, always active

DCAF	
DCAF	DCAF_Position_Disc
Revision	1
Restart Type	MANUAL
Cold Start Type	AUTOMATIC
Channel A	SFX_Ch0.ActualPosition 0.0
Channel B	SFX_Ch1.ActualPosition 0.0
Tolerance	Position_Tolerance 0.1
Discrepancy Time (Msec)	Position_DiscTime 300
High Limit	1000.0
Low Limit	0.0
Input Status	PositionDiscrepancy_Status 1
Reset	FaultReset <AEN2TR:1:I.Pt00.Data> 0
Diagnostic Code	0
Fault Code	0

5

The SLS mode select keyswitch is wired into channels 2 and 3 of the Compact I/O safety input module.
The point status for these two channels is used to generate the status bit for the SLS mode select keyswitch DCS instruction.

AEN2TR:1:I.Pt02.Status AEN2TR:1:I.Pt03.Status SLS_KeySwitch_Status



The SLS mode select keyswitch is wired into channels 2/3 of the Safety Input module. The DCS instruction monitors that the two channels are in the same state and that the channels have proper status.
The DCS output tag (DCS_SLS_KeySwitch.O1) is used to generate the SLS request mode.

6

```
DCS
DCS                          DCS_SLS_KeySwitch      O1
Safety Function                    SAFETY GATE
Input Type            EQUIVALENT - ACTIVE HIGH
Discrepancy Time (Msec)                    500      FP
Restart Type                         AUTOMATIC
Cold Start Type                      AUTOMATIC
Channel A                          SLS_Mode_chA
                           <AEN2TR:1:I.Pt02.Data>
                                             0
Channel B                          SLS_Mode_chB
                           <AEN2TR:1:I.Pt03.Data>
                                             0
Input Status                 SLS_KeySwitch_Status
                                             1
Reset                                FaultReset
                           <AEN2TR:1:I.Pt00.Data>
                                             0
```

Generate the SLS request if the SLS mode select keyswitch has been activated

7

```
DCS_SLS_KeySwitch.O1   SFX_Ch0.FP   SFX_Ch1.FP                SLS_Request
--] [----------------]/[----------]/[------------------------------( )--
```

When in SLS mode (Request = 1), after the check delay expires, this instruction monitors that the actual speed is below the SLS Active Limit.
If the Active Limit is exceeded while in SLS mode, the SLS_Axis1.O1 tag is de-energized. This tag is used to generate a Safe Stop 1 (SS1) request.
SLSActive1 and SLSLimit1 (if energized) remain energized until the SLS Request changes from high (1) to low (0).

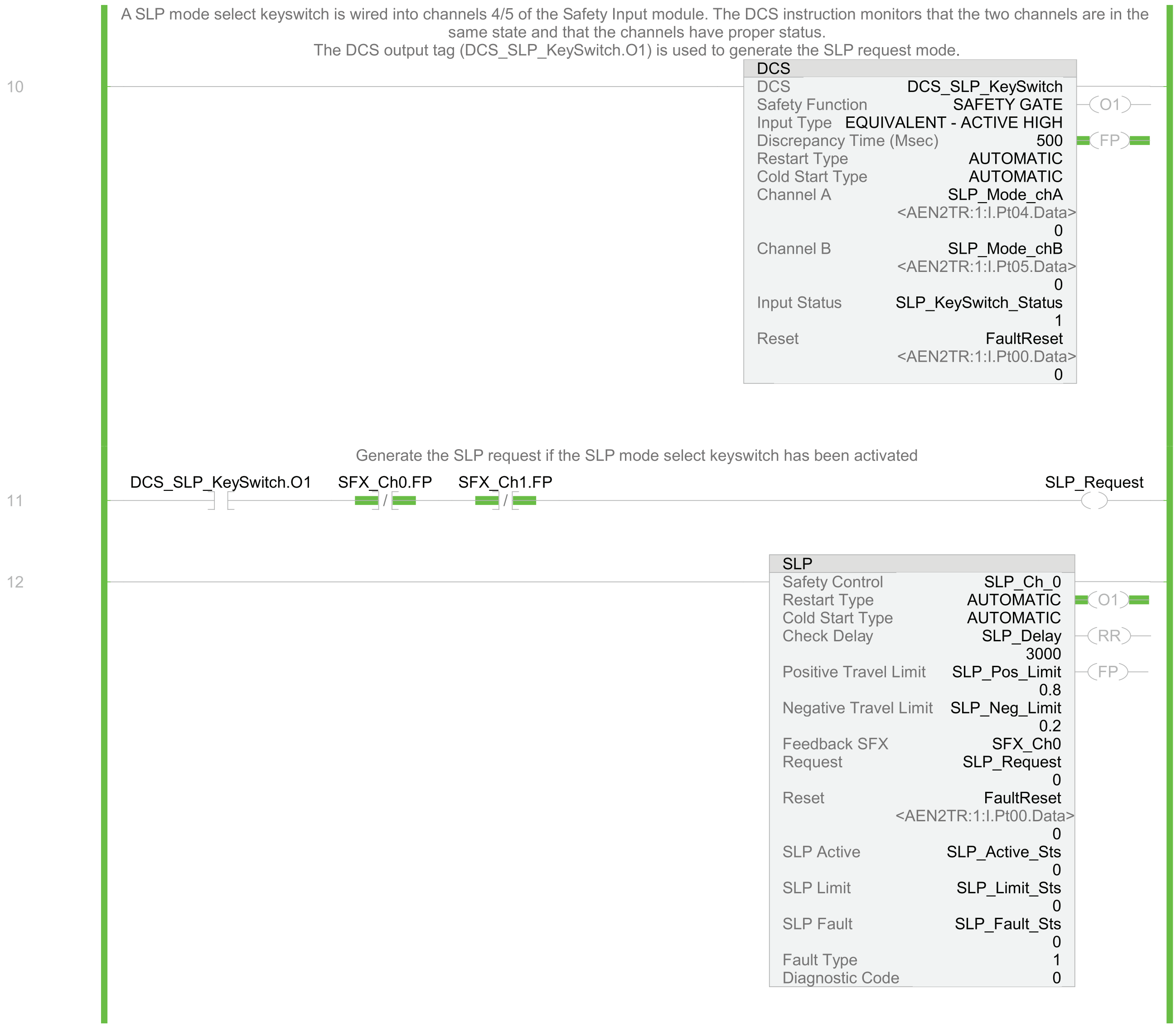
8

```
SLS
Safety Control          SLS_Ch_0
Restart Type           AUTOMATIC      O1
Cold Start Type        AUTOMATIC
Check Delay            SLS_Delay      RR
                            3000
Active Limit    SLS_Active_Limit      FP
                             2.0
Feedback SFX             SFX_Ch0
Request              SLS_Request
                               0
Reset                 FaultReset
          <AEN2TR:1:I.Pt00.Data>
                               0
SLS Active        SLS_Active_Sts
                               0
SLS Limit          SLS_Limit_Sts
                               0
SLS Fault          SLS_Fault_Sts
                               0
Fault Type                     1
Diagnostic Code                0
```

The SLP mode select keyswitch is wired into channels 4 and 5 of the Compact I/O safety input module.
The point status for these two channels is used to generate the status bit for the SLP mode select keyswitch DCS instruction.

9

```
AEN2TR:1:I.Pt04.Status   AEN2TR:1:I.Pt05.Status         SLP_KeySwitch_Status
--] [--------------------] [------------------------------------( )--
```



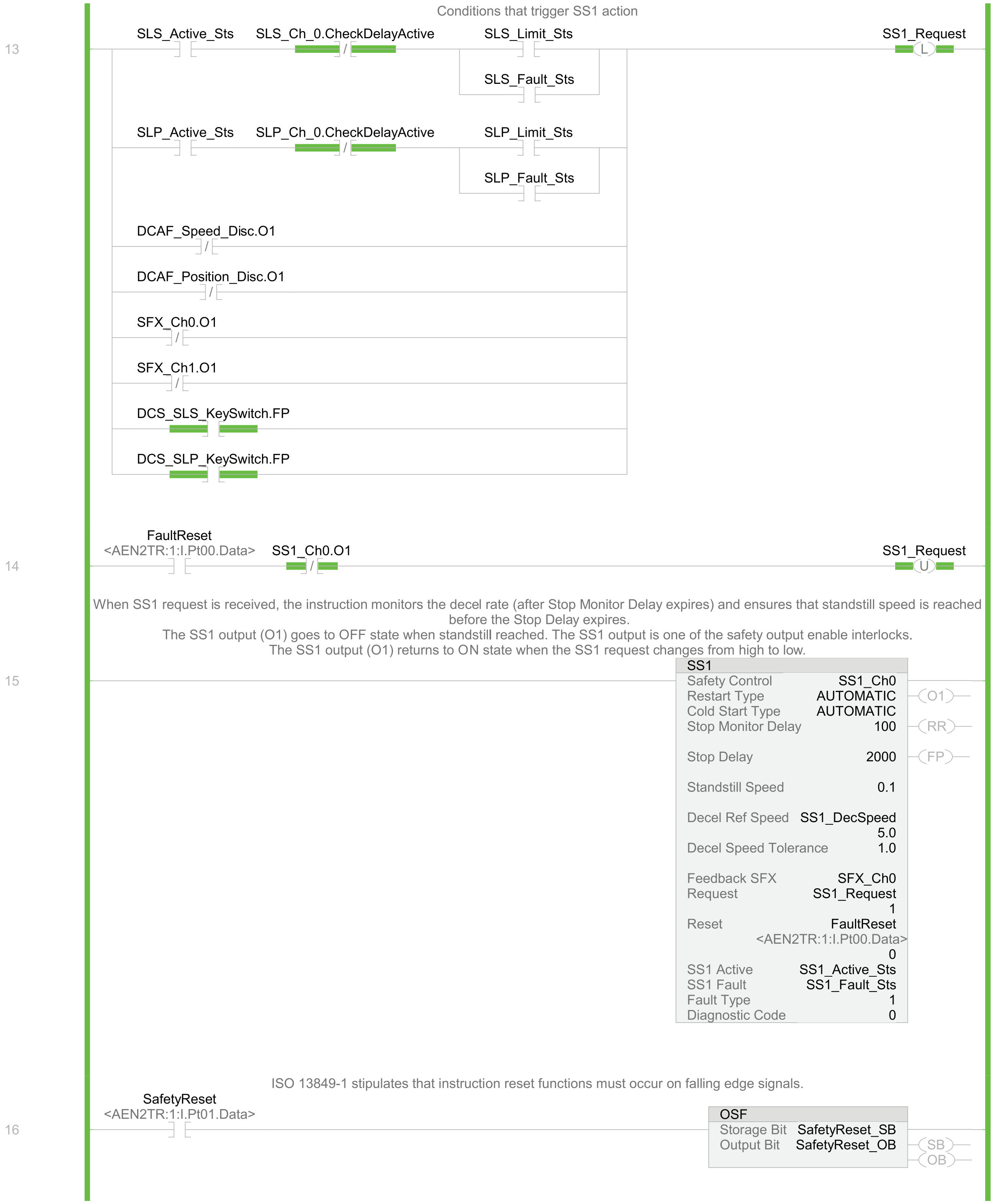
A SLP mode select keyswitch is wired into channels 4/5 of the Safety Input module. The DCS instruction monitors that the two channels are in the same state and that the channels have proper status.
The DCS output tag (DCS_SLP_KeySwitch.O1) is used to generate the SLP request mode.

```
10
DCS
DCS                        DCS_SLP_KeySwitch      O1
Safety Function            SAFETY GATE
Input Type    EQUIVALENT - ACTIVE HIGH
Discrepancy Time (Msec)    500                    FP
Restart Type               AUTOMATIC
Cold Start Type            AUTOMATIC
Channel A                  SLP_Mode_chA
                           <AEN2TR:1:I.Pt04.Data>
                           0
Channel B                  SLP_Mode_chB
                           <AEN2TR:1:I.Pt05.Data>
                           0
Input Status               SLP_KeySwitch_Status
                           1
Reset                      FaultReset
                           <AEN2TR:1:I.Pt00.Data>
                           0
```

Generate the SLP request if the SLP mode select keyswitch has been activated

```
11
DCS_SLP_KeySwitch.O1    SFX_Ch0.FP    SFX_Ch1.FP                SLP_Request
]  [                    ]/[           ]/[                       (  )
```

```
12
SLP
Safety Control             SLP_Ch_0
Restart Type               AUTOMATIC              O1
Cold Start Type            AUTOMATIC
Check Delay                SLP_Delay              RR
                           3000
Positive Travel Limit      SLP_Pos_Limit          FP
                           0.8
Negative Travel Limit      SLP_Neg_Limit
                           0.2
Feedback SFX               SFX_Ch0
Request                    SLP_Request
                           0
Reset                      FaultReset
                           <AEN2TR:1:I.Pt00.Data>
                           0
SLP Active                 SLP_Active_Sts
                           0
SLP Limit                  SLP_Limit_Sts
                           0
SLP Fault                  SLP_Fault_Sts
                           0
Fault Type                 1
Diagnostic Code            0
```



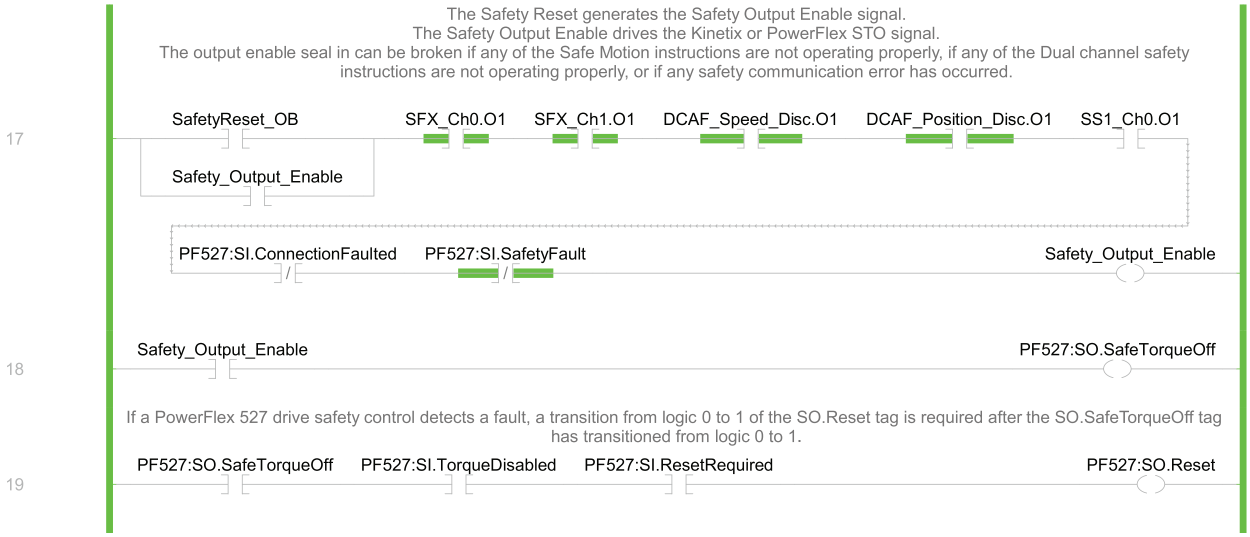
Conditions that trigger SS1 action

When SS1 request is received, the instruction monitors the decel rate (after Stop Monitor Delay expires) and ensures that standstill speed is reached before the Stop Delay expires.
The SS1 output (O1) goes to OFF state when standstill reached. The SS1 output is one of the safety output enable interlocks.
The SS1 output (O1) returns to ON state when the SS1 request changes from high to low.

SS1	
Safety Control	SS1_Ch0
Restart Type	AUTOMATIC
Cold Start Type	AUTOMATIC
Stop Monitor Delay	100
Stop Delay	2000
Standstill Speed	0.1
Decel Ref Speed	SS1_DecSpeed 5.0
Decel Speed Tolerance	1.0
Feedback SFX	SFX_Ch0
Request	SS1_Request 1
Reset	FaultReset <AEN2TR:1:I.Pt00.Data> 0
SS1 Active	SS1_Active_Sts
SS1 Fault	SS1_Fault_Sts
Fault Type	1
Diagnostic Code	0

ISO 13849-1 stipulates that instruction reset functions must occur on falling edge signals.

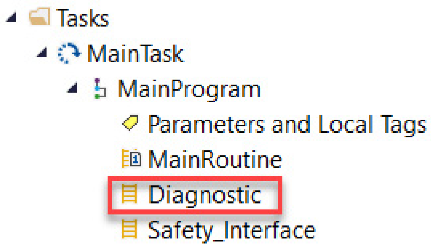
OSF	
Storage Bit	SafetyReset_SB
Output Bit	SafetyReset_OB



The Safety Reset generates the Safety Output Enable signal.
The Safety Output Enable drives the Kinetix or PowerFlex STO signal.
The output enable seal in can be broken if any of the Safe Motion instructions are not operating properly, if any of the Dual channel safety instructions are not operating properly, or if any safety communication error has occurred.

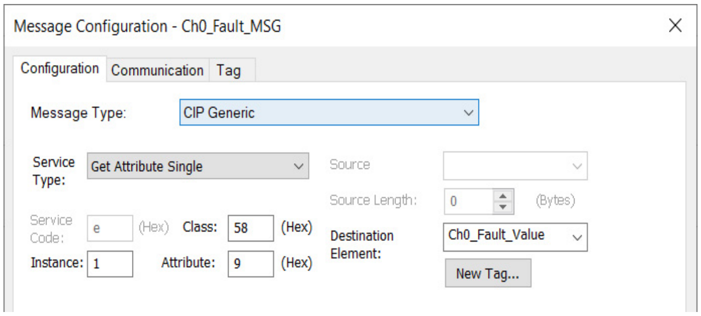
If a PowerFlex 527 drive safety control detects a fault, a transition from logic 0 to 1 of the SO.Reset tag is required after the SO.SafeTorqueOff tag has transitioned from logic 0 to 1.

The standard task contains a Diagnostic routine for the 1791ES-ID2SSIR module fault log. The Diagnostic routine is also referred to in the V&V checklist.



The fault codes of the two channels can be retrieved by a couple of MSG instructions, configured as shown below.

Channel 0 Message configuration



Message Configuration - Ch0_Fault_MSG

Configuration | Communication | Tag

Message Type: CIP Generic

Service Type: Get Attribute Single

Service Code: e (Hex) Class: 58 (Hex)

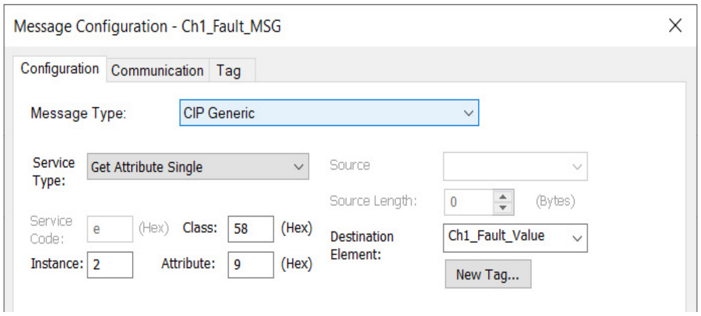
Instance: 1 Attribute: 9 (Hex)

Source:

Source Length: 0 (Bytes)

Destination Element: Ch0_Fault_Value

Channel 1 Message configuration



Message Configuration - Ch1_Fault_MSG

Configuration | Communication | Tag

Message Type: CIP Generic

Service Type: Get Attribute Single

Service Code: e (Hex) Class: 58 (Hex)

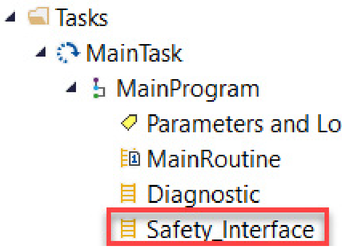
Instance: 2 Attribute: 9 (Hex)

Source:

Source Length: 0 (Bytes)

Destination Element: Ch1_Fault_Value

The standard task contains a Safety_Interface routine that contains triggers from safety to standard motion control.



- Tasks
  - MainTask
    - MainProgram
      - Parameters and Local Tags
      - MainRoutine
      - Diagnostic
      - Safety_Interface

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.

Calculation of the Performance Level

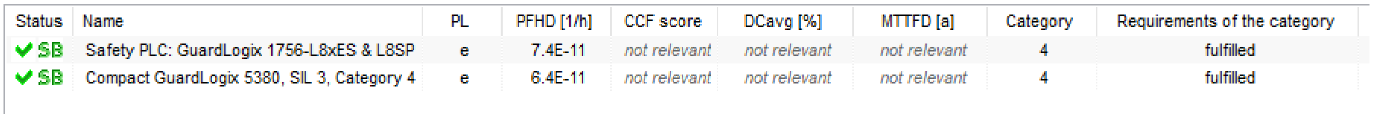
When properly implemented, these safety functions can achieve a safety rating of category 3, Performance Level e (cat. 3, PLe), according to ISO 13849-1: 2015, as calculated by using the SISTEMA software PL calculation tool.

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 will be different.

The SISTEMA file that is referenced in this safety function application technique is attached to this publication.

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.

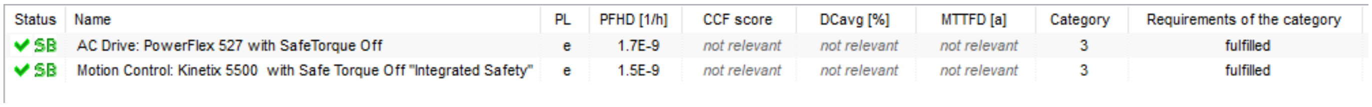
The PFHd values for the GuardLogix 5580 and Compact GuardLogix 5380 safety controllers are shown in the following graphic. Either controller can be selected in this example application.



Status	Name	PL	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✓ SB	Safety PLC: GuardLogix 1756-L8xES & L8SP	e	7.4E-11	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✓ SB	Compact GuardLogix 5380, SIL 3, Category 4	e	6.4E-11	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

Either the Kinetix or PowerFlex drive can be selected in this example application.

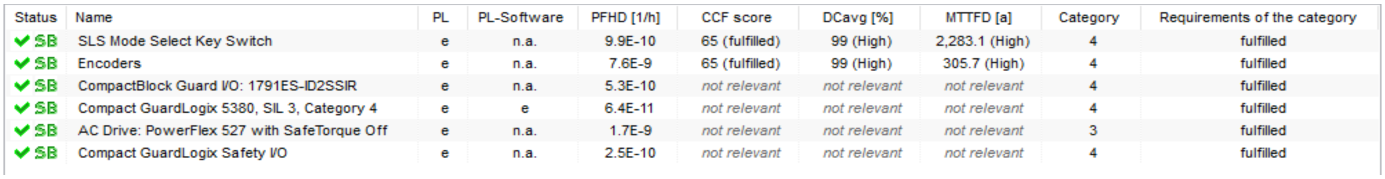
The PFHd values for the PowerFlex 527 and the Kinetix 5500 “Integrated Safety” architectures are shown in the following graphic.



Status	Name	PL	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✓ SB	AC Drive: PowerFlex 527 with SafeTorque Off	e	1.7E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✓ SB	Motion Control: Kinetix 5500 with Safe Torque Off "Integrated Safety"	e	1.5E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled

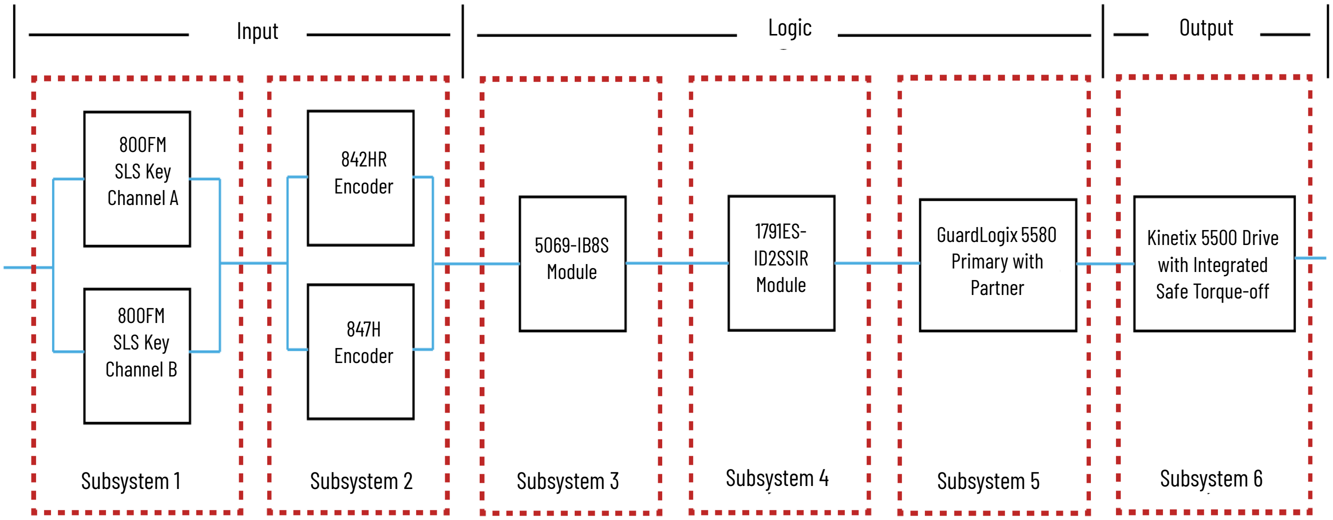
Stop Category 1 (SS1) Stop Function Initiated by Safely-limited Speed (SLS) Monitoring

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

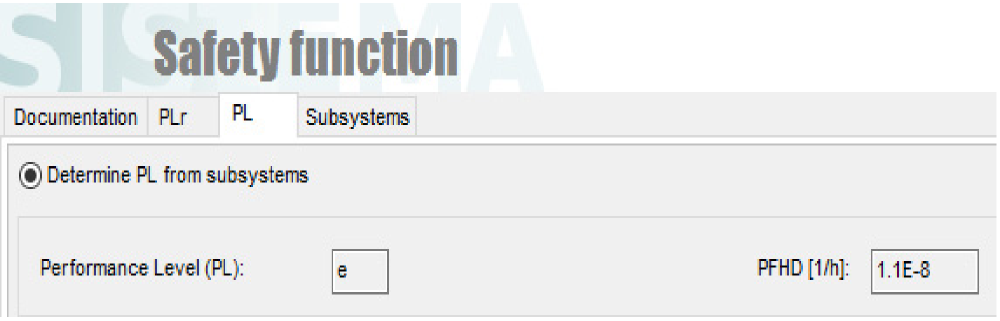


Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✓ SB	SLS Mode Select Key Switch	e	n.a.	9.9E-10	65 (fulfilled)	99 (High)	2,283.1 (High)	4	fulfilled
✓ SB	Encoders	e	n.a.	7.6E-9	65 (fulfilled)	99 (High)	305.7 (High)	4	fulfilled
✓ SB	CompactBlock Guard I/O: 1791ES-ID2SSIR	e	n.a.	5.3E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✓ SB	Compact GuardLogix 5380, SIL 3, Category 4	e	e	6.4E-11	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✓ SB	AC Drive: PowerFlex 527 with SafeTorque Off	e	n.a.	1.7E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✓ SB	Compact GuardLogix Safety I/O	e	n.a.	2.5E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

This safety function can be modeled as follows.



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 1.1E-8. The PL for the complete safety function is PLe.



Safety function

Documentation | PLr | PL | Subsystems

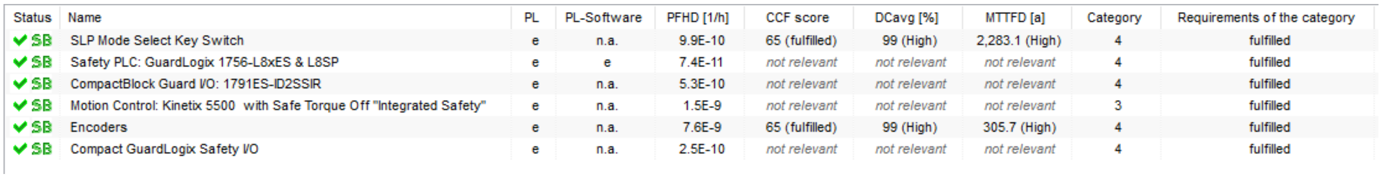
● Determine PL from subsystems

Performance Level (PL): e

PFHD [1/h]: 1.1E-8

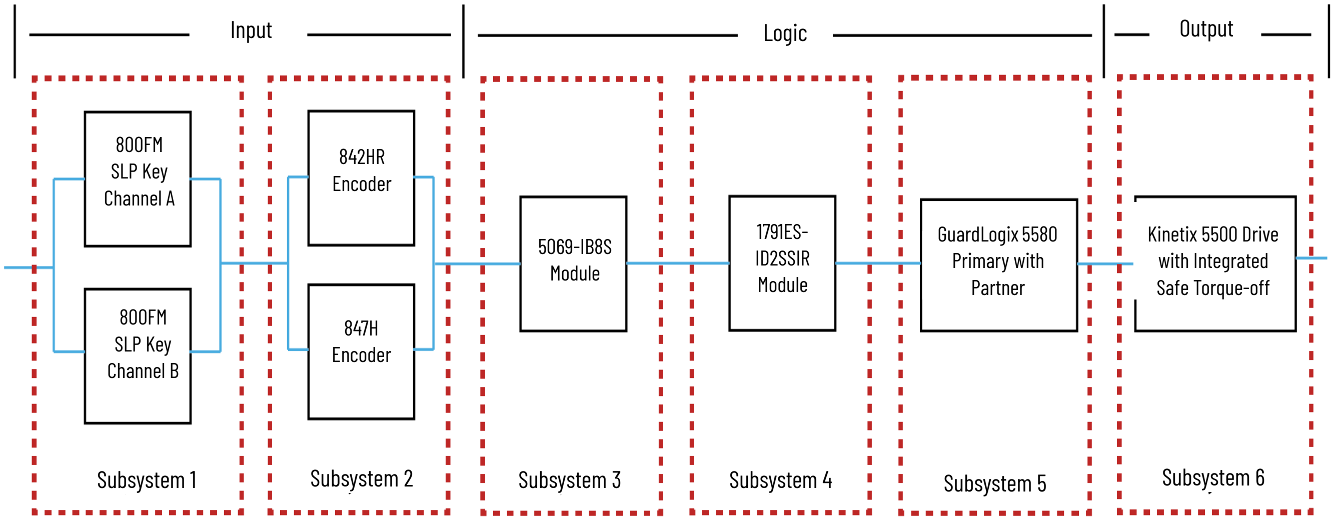
Safely-limited Position

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

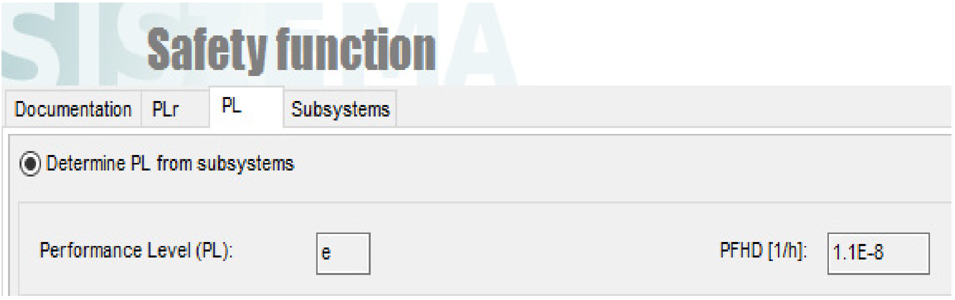


Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✓ SB	SLP Mode Select Key Switch	e	n.a.	9.9E-10	65 (fulfilled)	99 (High)	2,283.1 (High)	4	fulfilled
✓ SB	Safety PLC: GuardLogix 1756-L8xES & L8SP	e	e	7.4E-11	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✓ SB	CompactBlock Guard I/O: 1791ES-ID2SSIR	e	n.a.	5.3E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✓ SB	Motion Control: Kinetix 5500 with Safe Torque Off "Integrated Safety"	e	n.a.	1.5E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✓ SB	Encoders	e	n.a.	7.6E-9	65 (fulfilled)	99 (High)	305.7 (High)	4	fulfilled
✓ SB	Compact GuardLogix Safety I/O	e	n.a.	2.5E-10	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

The Safety-limited Position safety function can be modeled as follows.



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 1.1E-8. The PL for the complete safety function is PLe.



● Determine PL from subsystems

Performance Level (PL): e

PFHD [1/h]: 1.1E-8

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

Because the SLS and SLP key-selector switches 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 B10d (2,000,000 cycles) of the key selector switches are provided by the vendor.

The DCavg (99%) for the key selector switch is selected from the Output Device table of ISO 13849-1 Annex E, Cross monitoring of input signals and intermediate results within the logic (L), and detection of static faults and short circuits.

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.

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 Application Instruction Safety Reference Manual, publication 1756-RM095.

For a validation checklist, see the attached spreadsheet.

Additional Resources

These documents contain additional information concerning 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 5380 and Compact GuardLogix 5380 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.
CompactBlock Guard I/O 2-Channel Incremental Synchronous Serial Interface Encoder Module User Manual, publication 1791ES-UM002	Provides information on how to configure, and program the 1791ES-ID2SSIR CompactBlock Guard I/O module in the Logix Designer application.
CompactBlock Guard I/O 2-Channel Incremental Encoder Synchronous Serial Interface Module Installation Manual, publication 1791ES-IN002	Provides information on how to install the GuardLogix 5570 controllers in the Logix Designer application.
Kinetix 5500 Servo Drives User Manual, publication 2198-UM001	Provides detailed instructions on how to install, mount, wire, maintain, and troubleshoot the Kinetix 5500 servo drives. Also provides information on how to integrate the drive with a Logix 5000™ controller.
PowerFlex 527 Adjustable Frequency AC Drive User Manual, publication 520-UM002	Provides instructions on how to install, start up, and troubleshoot the PowerFlex® 527 adjustable frequency AC drive.
GuardLogix Application Instruction Safety 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.
842HR Sine Cosine/Serial Encoders Installation Instructions, publication 842HR-IN001	Provides detailed instructions on how to install, mount, and wire the 842HR Sine Cosine/Serial encoders.
847H 2.5 in. Diameter Solid Shaft Incremental Encoders Installation Instructions, publication 847H-IN001	Provides detailed instructions on how to install, mount, and wire the 847H Sine incremental encoders.
Safe Homing for Position Safety Function Application Technique, publication SAFETY-AT183	Provides information on how to perform safe homing by using the SFX instruction with the Kinetix 5700 drive, the 843ES CIP Safety Encoder and the 1791ES-IDSSIR Universal Feedback module.
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.
Safety Automation Builder® and SISTEMA Library website, rok.auto/sistema	Download Safety Automation Builder to help simplify machine safety design and validation, and reduce time and costs. Integration with our risk assessment software provides you with consistent, reliable, and documented management of the Functional Safety Lifecycle. The SISTEMA tool, also available for download from the Safety Automation Builder page, automates calculation of the attained Performance Level from the safety-related parts of a machine's control system to (EN) ISO 13849-1.

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) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846