

Safely-limited Position with Rollover via a GuardLogix Controller Safety Function

Products: 843ES CIP Safety Encoder, Compact GuardLogix 5380 or GuardLogix 5580 Controller, 5069 Compact I/O Safety Module, Kinetix 5300 Servo Drive

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



Topic	Page
Important User Information	2
General Safety Information	3
Introduction	3
Use Sample Project Files	4
Safety Function Realization: Risk Assessment	5
Safely-limited Position Safety Function	5
Safety Function Requirements	5
Functional Safety Description	6
Bill of Material	10
Setup and Wiring	11
Configuration	13
Programming	16
Calculation of the Performance Level	24
Verification and Validation Plan	25
Additional Resources	25

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 Compact GuardLogix® 5380 controller (logic), an 843ES CIP Safety™ encoder (input), and a Kinetix® 5300 servo drive (output) with hardwired Safe Torque Off (STO) to perform the Safely-limited Position (SLP) safety function, which helps prevent the motor shaft from exceeding the specified position limits.

In the GuardLogix safety task, the Safety Feedback Interface (SFX) Drive Safety instruction is used to provide the actual position of the motor to the SLP instruction.

The SLP instruction monitors the position of a motor to help ensure that the position does not deviate above or below defined limits. The SLP instruction signals when the motor moves outside of the specified limits and the signal can be used to initiate an application-specific stopping action such as STO, Safe Stop 1 (SS1), or Safe Stop 2 (SS2).

The example in this document also shows in detail how to manage the SLP instruction when the motor moves through the encoder rollover position.

A Safe Stop 1 time controlled (SS1-t) event, as per IEC 61800-5-2 4.2.3.3, provides the ability to stop the motor if the SLP limit is exceeded while the SLP instruction is active. Then an STO request is made from the safety task to help prevent hazardous motion after the SS1-t Stop Timer completes.

Because the Kinetix 5300 servo drive doesn't have advanced safety capabilities, the safety actions have to be executed in the GuardLogix safety task. Standard logic is executed when SLP mode or SS1 are requested. If the standard logic is not executed properly, the drive safety instructions detect this condition and maintain a safe machine state. It is important to note that the safety function, by itself, does not control the motor. The standard motion control program is used to manage control of the motor based on the safety function executing.



This example assumes the use of an 843ES CIP Safety encoder as a sensor that provides single-feedback position monitoring.

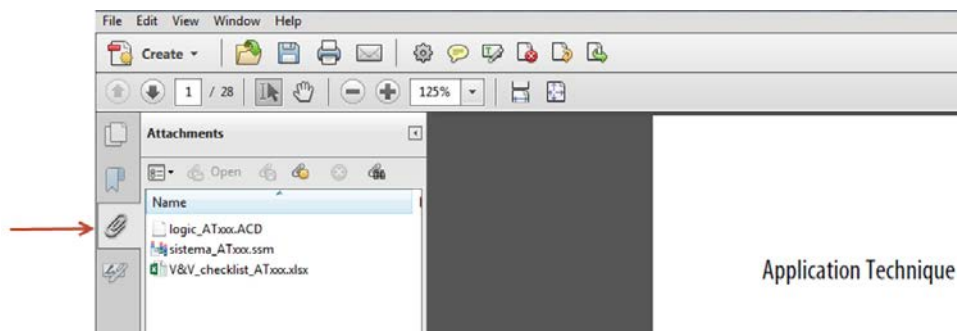
This example uses a 5069-L3100ERMS2 Compact GuardLogix controller, but you can substitute a GuardLogix controller that supports the safety rating that is demonstrated in this safety function application technique. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA)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

Use Sample Project Files

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

To access these files, follow these steps.

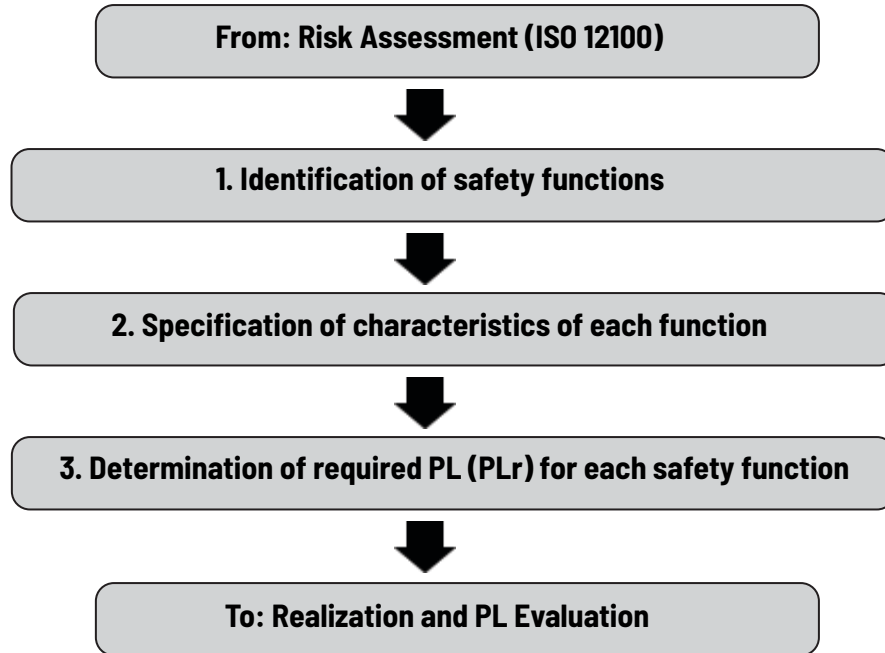
1. If you are viewing the PDF file in a browser and do not see the Attachments link , download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link .
3. Right-click and save the desired file.



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.



Safely-limited Position Safety Function

This application technique includes one safety function: Safely-limited position.

Safety Function Requirements

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 values for the motor.

If the motor position moves outside of the specified limits, after the Check Delay time expires, an SS1-t is generated to stop the motor. When the SS1-1 Stop Timer expires, an STO function 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 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](#).

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

Functional Safety Description

For tasks that require hazardous motion, a safety function to monitor the position of a motor to help ensure that the position does not deviate above or below defined limits can be used so that harm can be avoided, or at least reduced.

An SLP instruction is used with a CIP safety encoder that supplies the position of a motor and an SFX instruction is used to scale the feedback.

The SLP function begins if it has been previously reset and the Request input is set to high (1). At this point, the Check Delay Timer begins. When the Check Delay Timer expires, position monitoring begins. The Actual Position, provided by an SFX instruction, is compared to the Positive and Negative Position Limits. If the Actual Position is not within these limits, then the SLP_Limit output is set to high (1) and remains set until the SLP function is reset. The SFX instruction must be homed before the SLP function operates.

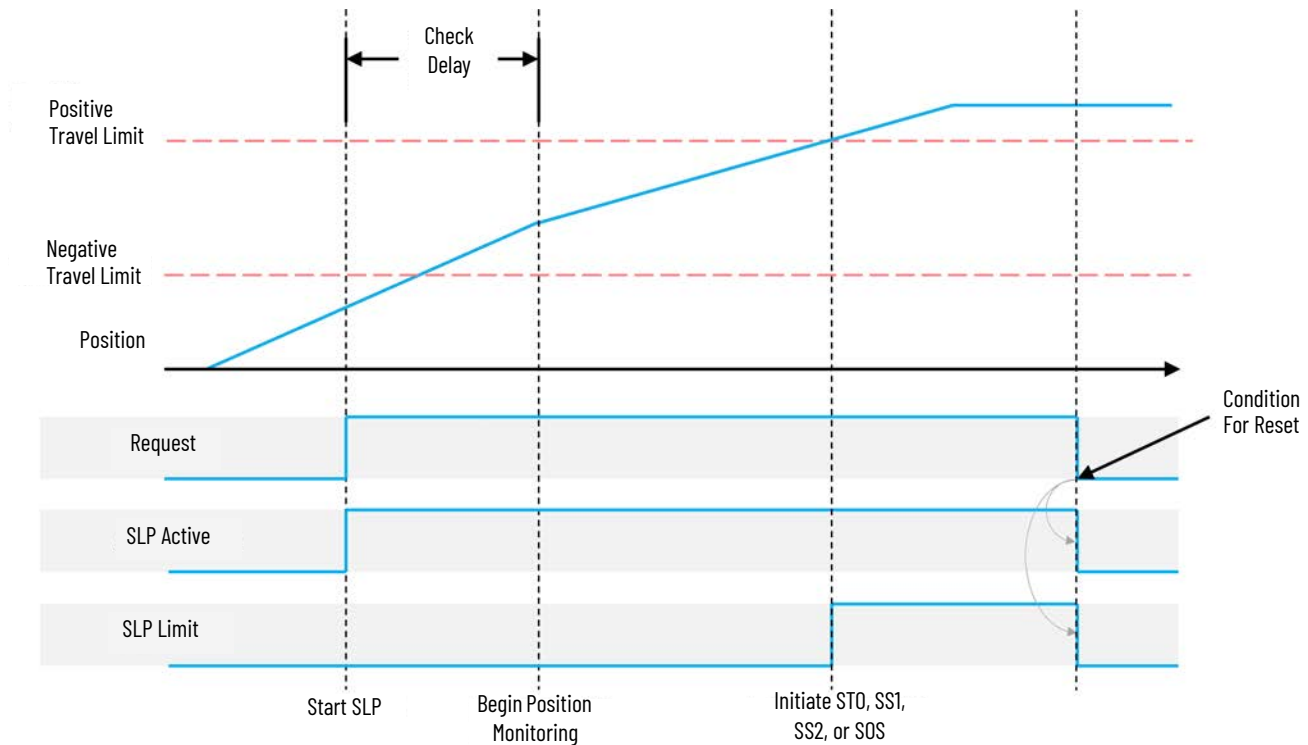
Position values used in the SLP instruction are in Position Units. A position unit is user-defined according to the specific application and is configured in the SFX instruction.

During operation, the Position Limits can be programmatically changed. If the limits are changed while the function is operating, then the new limits take effect immediately.

If the motor moves outside the specified limits when the SLP instruction is active, the instruction SLP_Limit output can be used to initiate an application-specific action, in our example an SS1-t.

Normal Operation, Automatic Restart

The following diagram shows normal operation with Automatic Restart. After the Check Delay expires, the Position is shown to be within the Positive and Negative Travel Limits. The diagram then shows the position moving outside of the limits and the Limit Output is set to high (1). For automatic restart operation, the SLP function is reset when the Request is removed, low (0), provided no SLP faults have occurred.



SLP Operation

To operate the SLP function, follow these steps.

1. While the motor is energized, the SLP request is set high (1) when there are no faults with the Drive Safety Instructions (SFX/SLP). The SLP request must remain high (1) throughout the SLP procedure. After SLP is requested, the motion application program is signaled by using the SLP_instruction. The SLP_Active output bit indicates that an SLP instruction is active. 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 ST0 when SLS is Exceeded

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

If the SLP Active Limit is exceeded after the programmable delay expires, an SS1-t request is initiated. When the SS1-t Stop Timer expires, an ST0 request is automatically initiated and, when completed, removes the ability to produce motor torque. To recover, follow these steps.

1. Remove the SLP request.
2. To remove the ST0 condition so that the motor can be enabled, press the Safety Circuit Reset button.

Rollover Considerations

The 843ES CIP safety encoder has a zero-crossing rollover, which the SLP instruction interprets as a move outside the programmed Positive and Negative Position limits, which can cause nuisance machine stops.

The Kinetix 5700-ERS4 drive and PowerFlex® 755 drive with a 20-750-S4 safety card deliver position data to the GuardLogix input as a value from - 2,147,483,648 to 2,147,483,648. A rollover is seen as a 4.29 billion count change in position.

The 843ES CIP safety encoder delivers position data to the GuardLogix controller input as a value from 0 to 134,217,728 for a maximum turn configured multi-turn, or 0 to 32,768 value for a single-turn encoder.

Kinetix 5700-ERS4 Drive or PowerFlex 755-S4 Drive	
Tag	SI.FeedbackPosition
Type	DINT
Low Value	-2,147,483,648
Upper Value	2,147,483,648
Rollover Limit	4,294,967,296

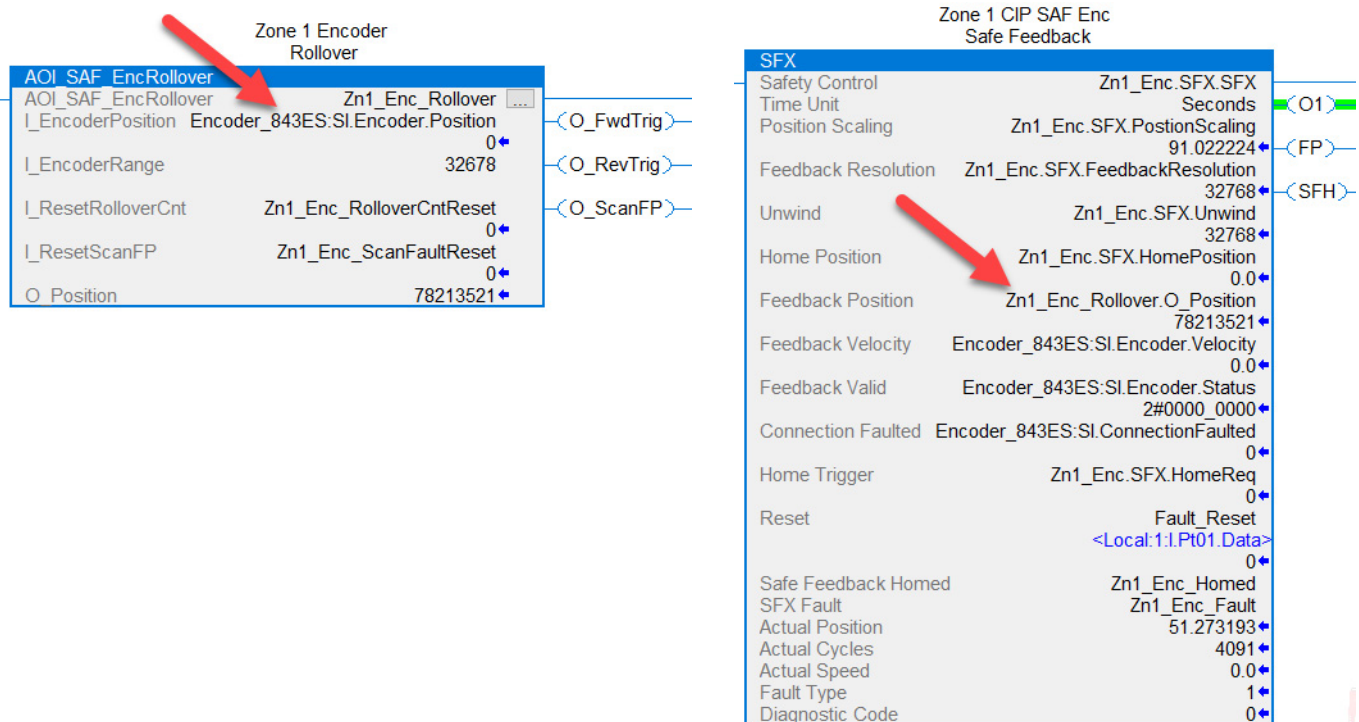
843ES Multi Turn Encoder	
Tag	SI.Encoder.Position
Type	DINT
Low Value	0
Upper Value	134,217,728
Rollover Limit	134,217,728

843ES Single Turn Encoder	
Tag	SI.Encoder.Position
Type	DINT
Low Value	0
Upper Value	32,768
Rollover Limit	32,768

AOI_SAF_EncRollover Add-on Instruction

The AOI_SAF_EncRollover Add-on Instruction (AOI) was developed for converting a safety encoder signal with a zero-position rollover (example: 0...32768) to continuous position DINT (-2,147,483,648 to 2,147,483,648).

The safety encoder position is an AOI input, I_EncoderPosition, and the O_Position output is used as input for the SFX Feedback Position instruction.



The O_Position output is designed to accumulate positive and negative position and handle position rollover in a manner that is supported by safety instructions.

IMPORTANT Encoder input Requested Packet Interval (RPI) and Safety task period have implications on encoder input data reliability. The input RPI must be faster than the safety task to help ensure fresh data is available. (Input RPI is typically ½ safety task period.) Multiple scans of the safety task are required between encoder rollovers to accurately interpret the position of the encoder. The O_ScanFP bit indicates fewer than three scans were executed per rollover. During active monitoring, the O_ScanFP going high (1) must take the application to a safe state. If three scans are unobtainable with a single-turn encoder, a multi-turn encoder is required.

IMPORTANT Final validation of functionality and proper fault reaction must be conducted and documented at the point of application.

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

If a malfunction occurs, it is possible that stop category 0 may occur. 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. The nature of a malfunction that causes this condition could be if a hardwired STO input to the drive were to go low (that is, a wire falls off) before the drive has a chance to completely stop the motor. 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
843ES-SIP14BA7	843ES CIP Safety encoder, single-turn (1 turn), solid shaft 10 mm (0.39 in.), M12 connector, 32,768 (15 bit) safety and 262,144 (18 bit) standard steps per revolution, 58 mm (2.28 in.) square flange	1
1585D-M4UBJM-2	M12 to RJ45 Ethernet patchcord, shielded, 2 m (6.56 ft)	1
889D-F4EC-2	DC Micro (M12) 4-pin straight female, shielded, 22 AWG, 2 m (6.56 ft)	1
800FM-KM22MX02	Two-position key selector switch, metal, maintained, right key removal, two normally closed contacts	1
800FP-R611	800F Reset, round plastic (Type 4/4X/13, IP66), blue, R, standard pack (quantity 1)	2
5069-IB8S	5069 Compact I/O™ 8 channel safety sink input module	1
5069-OBV8S	5069 Compact I/O 8 channel configurable safety output module	1
5069-RTB18-SCREW	5069 Compact I/O 18-pin screw type terminal block	2
2198-C1004-ERS	Kinetix 5300 servo drive with hard-wired STO	1

Choose one of the following safety-controller hardware groups.

Controller	Cat. No.	Description	Quantity
Compact GuardLogix 5380-SIL 2	5069-L306ERS2	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory	1
	5069-L306ERMS2		
	5069-L310ERMS	Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory	
	5069-L310ERMS2		
	5069-L320ERS2	Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory	
	5069-L320ERMS2		
	5069-L330ERS2	Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory	
	5069-L330ERMS2		
	5069-L340ERS2	Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory	
	5069-L340ERMS2		
	5069-L350ERS2	Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory	
	5069-L350ERMS2		
	5069-L380ERS2	Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory	
	5069-L380ERMS2		
	5069-L3100ERS2	Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	
	5069-L3100ERMS2		
	5069-RTB64-SCREW	Compact I/O power terminal RTB kit for both 4- and 6-pin screw type	1
	1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 120/240V AC input	1
Compact GuardLogix 5380 - SIL 3	5069-L306ERMS3	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory	1
	5069-L310ERMS3	Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory	
	5069-L320ERMS3	Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory	
	5069-L330ERMS3	Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory	
	5069-L340ERMS3	Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory	
	5069-L350ERMS3	Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory	
	5069-L380ERMS3	Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory	
	5069-L3100ERMS3	Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	
	5069-RTB64-SCREW	Compact I/O power terminal RTB kit for both 4- and 6-pin screw type	1
	1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 120/240V AC input	1

Controller	Cat. No.	Description	Quantity
GuardLogix 5580 ⁽¹⁾	1756-L81ES	GuardLogix Processor, 3 MB standard memory, 1.5 MB safety memory	1
	1756-L82ES	GuardLogix Processor, 5 MB standard memory, 2.5 MB safety memory	
	1756-L83ES	GuardLogix Processor, 10 MB standard memory, 5 MB safety memory	
	1756-L84ES	GuardLogix Processor, 20 MB standard memory, 6 MB safety memory	
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A7	Seven-slot ControlLogix [®] chassis	1

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

Setup and Wiring

For detailed information on how to install and wire the products in this application technique, refer to the publications that are listed in the [Additional Resources](#).

System Overview

In this example, SLP mode is requested via the two-position maintained key selector switch (Key-Switch). The SLP mode request selector switch is wired to the 5069-IB8S safety input module. Test Outputs 0 and 1 are used to source the 24V DC for the SLP mode key selector switch.

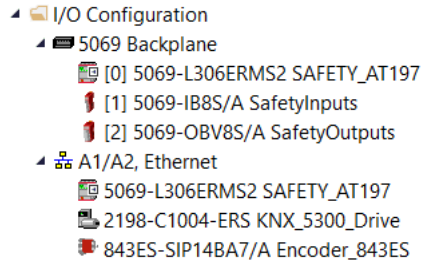
The GuardLogix controller, by using the integrated Ethernet port, uses safety connections to the 843ES encoder over an EtherNet/IP[™] network. The CIP Safety[™] protocol makes the network architecture a black channel, and thus not part of the safety (PL) calculation.

The Safety Reset and Fault Reset push buttons are wired to the 5069-IB8S input module in this example. This configuration is not required for functional safety; the reset inputs could be wired to a standard input module.

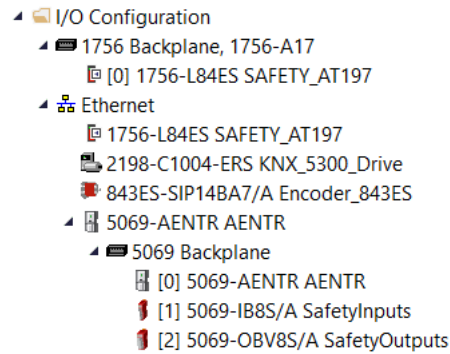
Two 5069-OBV8S safety output modules are wired to the Kinetix 5300 drive STO hardwired inputs.



Network Architecture



Compact GuardLogix 5380 Controller



GuardLogix 5580 Controller with Embedded Ethernet Connection⁽¹⁾

(1) 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 Compact GuardLogix controller is configured by using the Studio 5000 Logix Designer® application, version 33 or later. You must create a project and add the 843ES encoder, the Kinetix 5300 drive with hardwired STO, and appropriate safety and standard I/O modules. 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 5380 controller, but if you choose a 5580 controller, you can change the controller in the Logix Designer program.

Minimum Logix Designer Application Version	Product
31	843ES CIP Safety encoder
32	Compact 5000™ safety I/O: 5069-IB8S, 5069-OBV8S
31	GuardLogix 5580 or Compact GuardLogix 5380 controller
33	Kinetix 5300 drive ⁽¹⁾

⁽¹⁾ The Kinetix 5300 drive uses an Add-On Profile that requires a minimum version 33 of Logix Designer.

IMPORTANT Only the GuardLogix controller, the safety I/O modules, and the 843ES encoder configuration options that are related to safety and SLP are shown in the example.

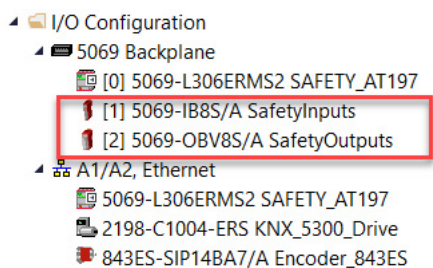
Create a Project with a GuardLogix Controller

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](#).

- In the Logix Designer application, create a project with a GuardLogix controller that includes the following:
 - A connection to an Ethernet network—GuardLogix 5580 and Compact GuardLogix 5380 controllers have Ethernet ports
 - Time Synchronization enabled on the controller and any Ethernet communication modules, if used

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

2. Set the IP address for the controller or any Ethernet communication modules, if used.
3. Add a Compact 5000 Ethernet adapter to your project, if you are using a GuardLogix 5580 controller.
4. Add the 5069-IB8S and 5069-OBV8S Compact 5000 I/O safety input modules to your project. In our application, we have the I/O installed as shown.



5. Configure the 5069-IB8S safety input module properly for your application as shown in the graphics:
 - Configure Input 0 and 1 to be Safety.
 - Configure Input 2 to be Safety Pulse Test from Test Source 1.
 - Configure Input 3 to be Safety Pulse Test from Test Source 0.

General

Type: 5069-IB8S 8 Point 24V DC Safety Input, Sink

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name:

Description:

Module Definition

Series: A Change ...

Revision: 2.001

Electronic Keying: Compatible Module

Configured By: This Controller

Input Data: Safety Data

Muting Lamp Points: None

Input Points

Point	Point Mode	Test Source	Input Delay Time(ms)		Transition Time Limit (ms)	Diagnostics
			Off->On	On->Off		
0	Safety	None	0 ms	0 ms	100 ms	...
1	Safety	None	0 ms	0 ms	100 ms	...
2	Safety Pulse Test	Test Source 1	5 ms	5 ms	100 ms	...
3	Safety Pulse Test	Test Source 0	5 ms	5 ms	100 ms	...
4	Not Used	None	0 ms	0 ms	100 ms	...
5	Not Used	None	0 ms	0 ms	100 ms	...
6	Not Used	None	0 ms	0 ms	100 ms	...
7	Not Used	None	0 ms	0 ms	100 ms	...

See the [Additional Resources](#) for information on your 5069-IB8S safety input module.

6. Configure the 5069-OBV8S safety output module properly for your application as shown in the following graphics.
 - Configure Outputs 0 and 1 to be Single and Safety.

General

Type: 5069-OBV8S 8 Point 24V DC Bipolar/Sourcing Safety Output

Vendor: Rockwell Automation/Allen-Bradley

Parent: Local

Name:

Description:

Module Definition

Series: A Change ...

Revision: 2.001

Electronic Keying: Compatible Module

Configured By: This Controller

Input Data: Safety Data

Output Data: Safety Data

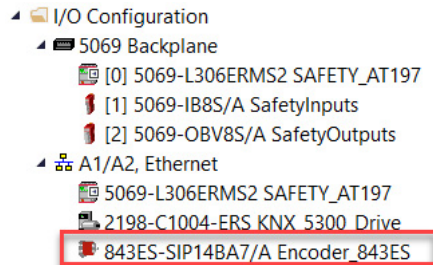
Output Mode: Sourcing

Points

Point	Point Operation		Point Mode	Enable No Load Diagnostic	Diagnostics
	Type				
0	Single	Safety	<input type="checkbox"/>	...	
1	Single	Safety	<input type="checkbox"/>	...	
2	Dual	Not Used	<input type="checkbox"/>	...	
3	Dual	Not Used	<input type="checkbox"/>	...	
4	Dual	Not Used	<input type="checkbox"/>	...	
5	Dual	Not Used	<input type="checkbox"/>	...	
6	Dual	Not Used	<input type="checkbox"/>	...	
7	Dual	Not Used	<input type="checkbox"/>	...	

See the [Additional Resources](#) for information on your product.

7. Add the 843ES CIP Safety encoder to the I/O configuration.



8. Configure the safety properties of the 843ES CIP Safety encoder as shown in the Encoder Safety Configuration dialog box.

General	Encoder Safety Configuration
Type: 843ES-SIP14BA7 10mm Solid Shaft Single-turn Safety E	<input checked="" type="checkbox"/> Monitor Input Voltage
Vendor: Rockwell Automation/Allen-Bradley	<input checked="" type="checkbox"/> Enable Position Scaling
Parent: Local	<input type="checkbox"/> Enable Endless Shaft Functionality
Name: Encoder_843ES	Numerator: 1
Description:	Denominator: 1
Module Definition	Resolution: 32768 Counts/Revolution
Series: A	Revolutions: 1
Revision: 1.001	Range: 32768 Counts
Electronic Keying: Compatible Module	Direction: Counter Clockwise
Connection: Safety Only	Velocity Units: Counts/s
Safety Input Data: Data	
Safety Output Data: Data	
Standard Data: None	

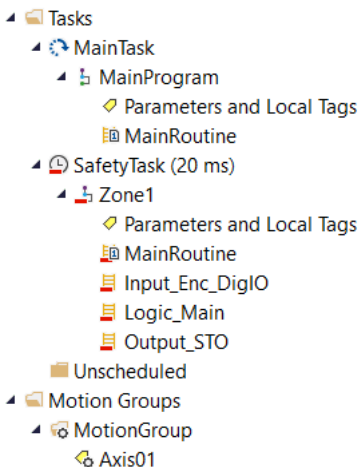
The 843ES-SIP14BA7 is a single-turn encoder capable of 32,768 (15 bit) safety counts per revolution. In our application, it is configured as Counter Clockwise for ease of comparison to the motor position in the trend. See the [Additional Resources](#) for information on your product.

9. Add the Kinetix 5300 drive to your project.
10. Configure the Kinetix 5300 drive properly for your application.
See the [Additional Resources](#) for information on your product.

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](#).

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.



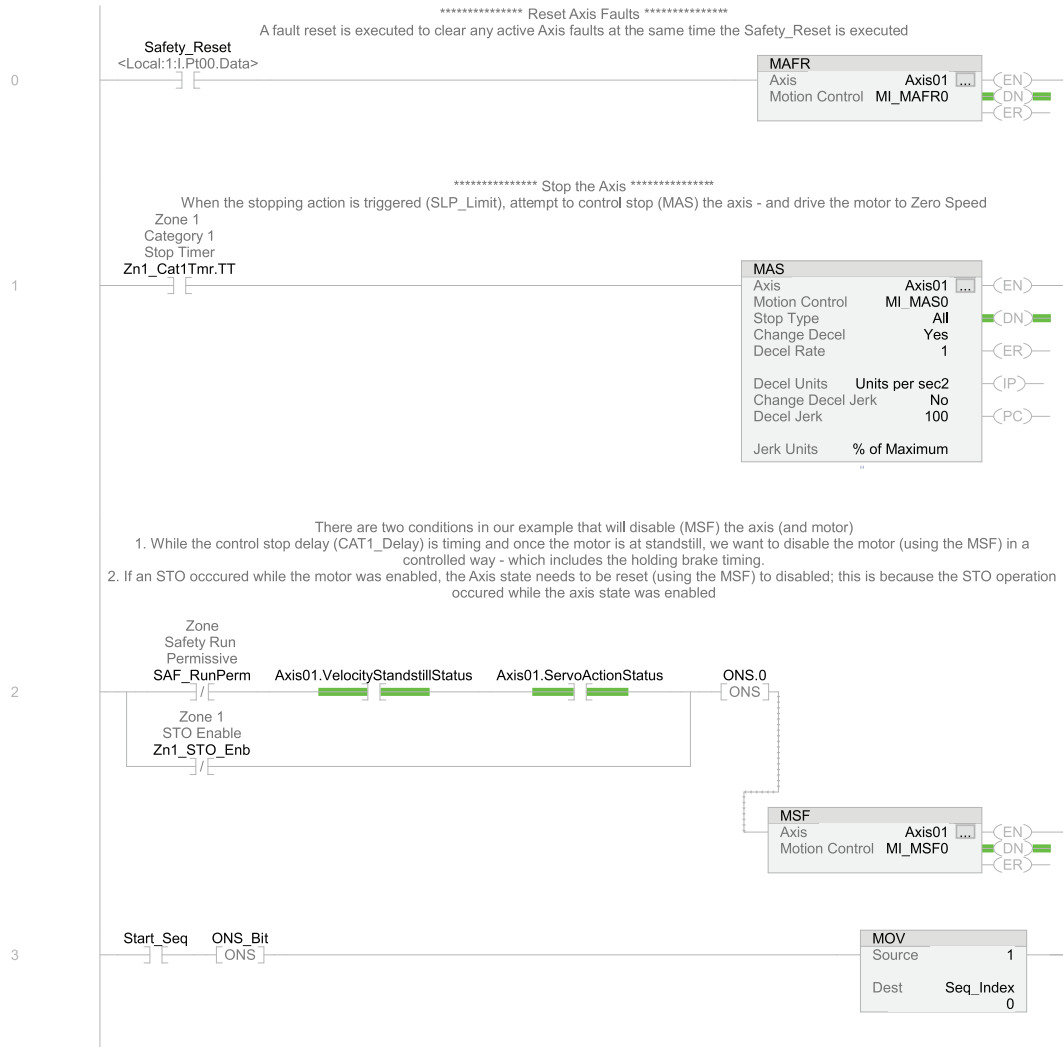
Standard Logic Considerations

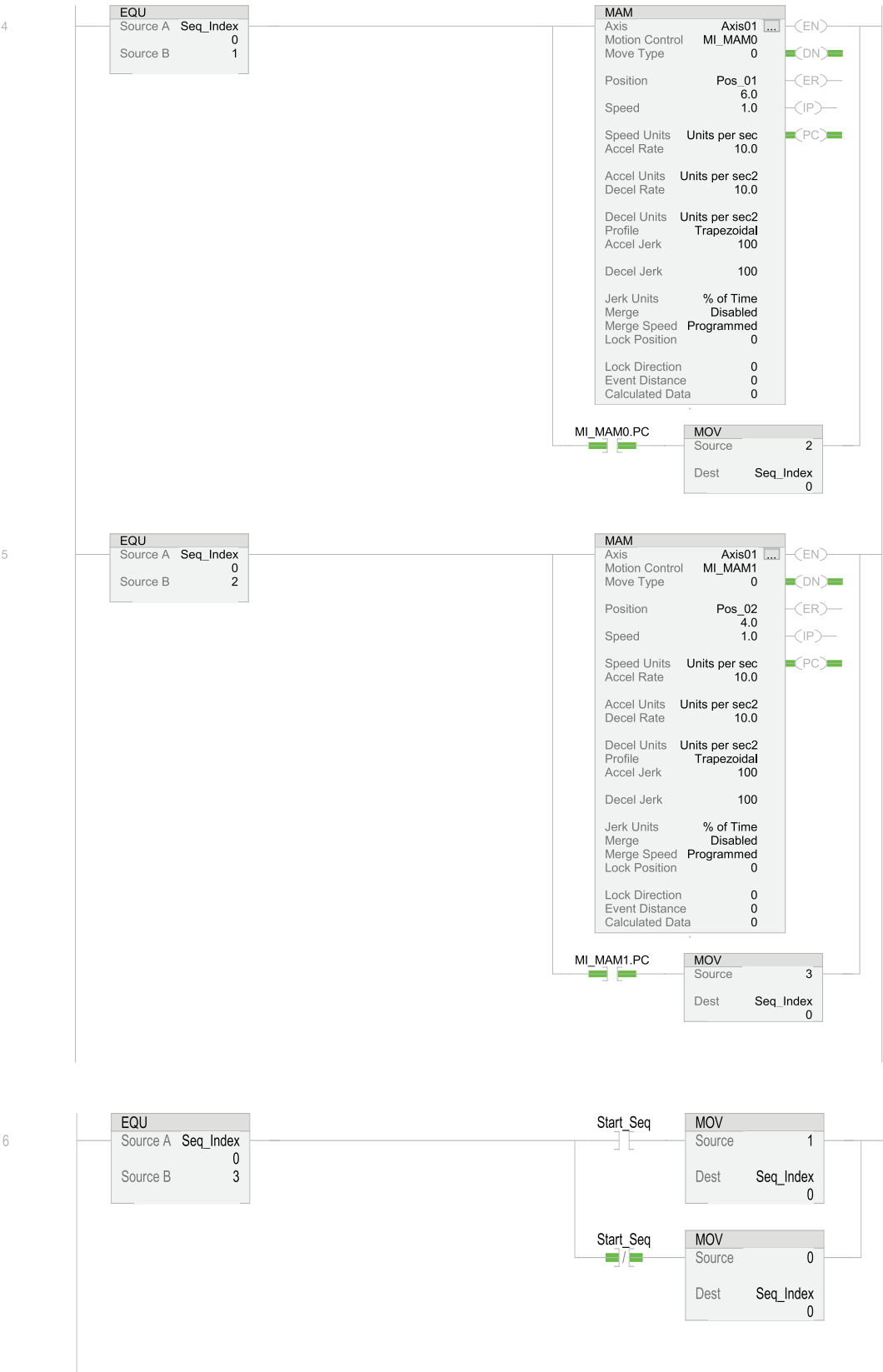
When the Kinetix 5300 STO inputs are de-energized, the drive disables its output power transistors and lets hazardous motion coast to a stop. When the input device is returned to its safe state and the Safety Reset button is pressed and released properly, the 5069-0BV8S outputs 0 and 1 are on, and the STO inputs of the drive are energized. Hazardous motion can then be restarted by an additional, separate action such as a start button.

IMPORTANT For more information on how to configure and program the Kinetix 5300 drive for a coast-to-stop (stop category 0) or a controlled stop (stop category 1), see Actuator Subsystems – Stop Category 0 or 1 via an Integrated Safety Controller and Kinetix 5300 Servo Drive with Hardwired Safe Torque Off Safety Function Application Technique, publication [SAFETY-AT196](#).

MainRoutine (Standard) Logic

This standard logic includes disabling and reset conditions that are required to disable and reset from a stop category 0 or 1 request. It includes a motion sequence example that is used just for validation. For more information, see [Verification and Validation Plan on page 25](#). You must include logic to enable the motor and perform your application-specific motion.



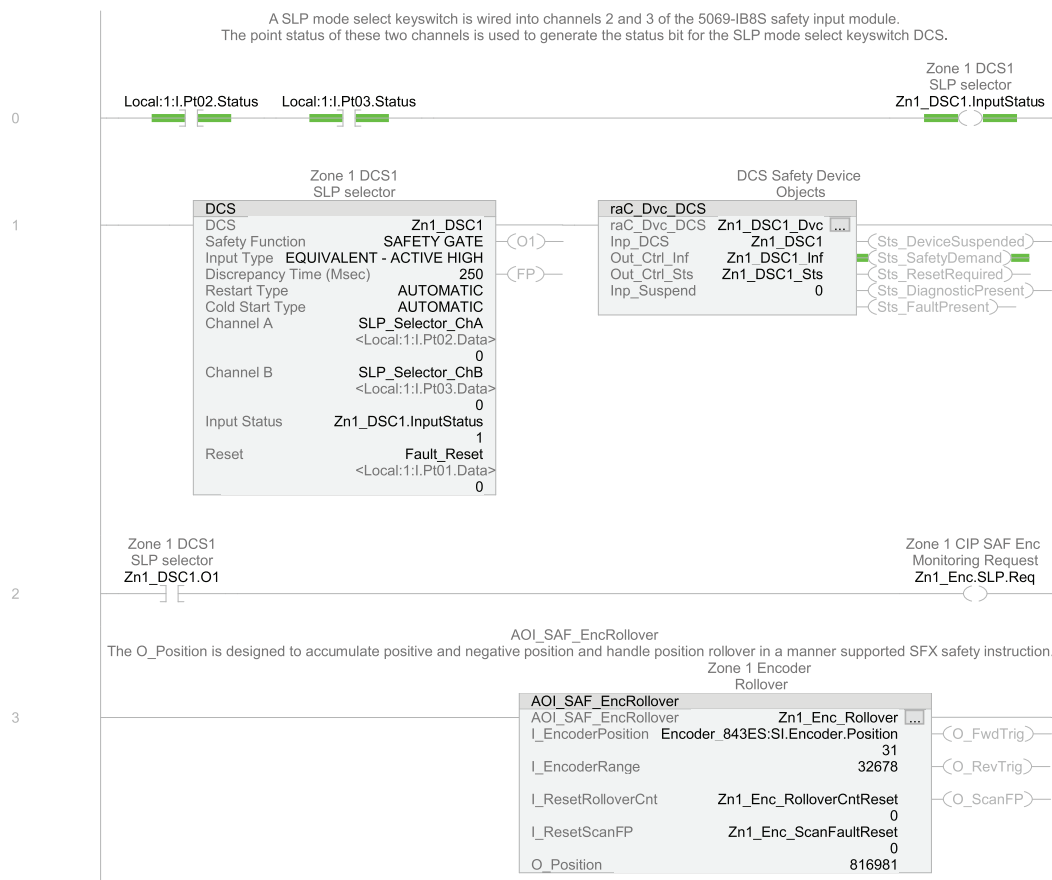


Safety Program Logic

The safety logic consists of the Safety Task, which contains the Zone1 program. The Zone1 program contains three subroutines that perform logic control.

Zone1 – Input_Enc_DigI/O

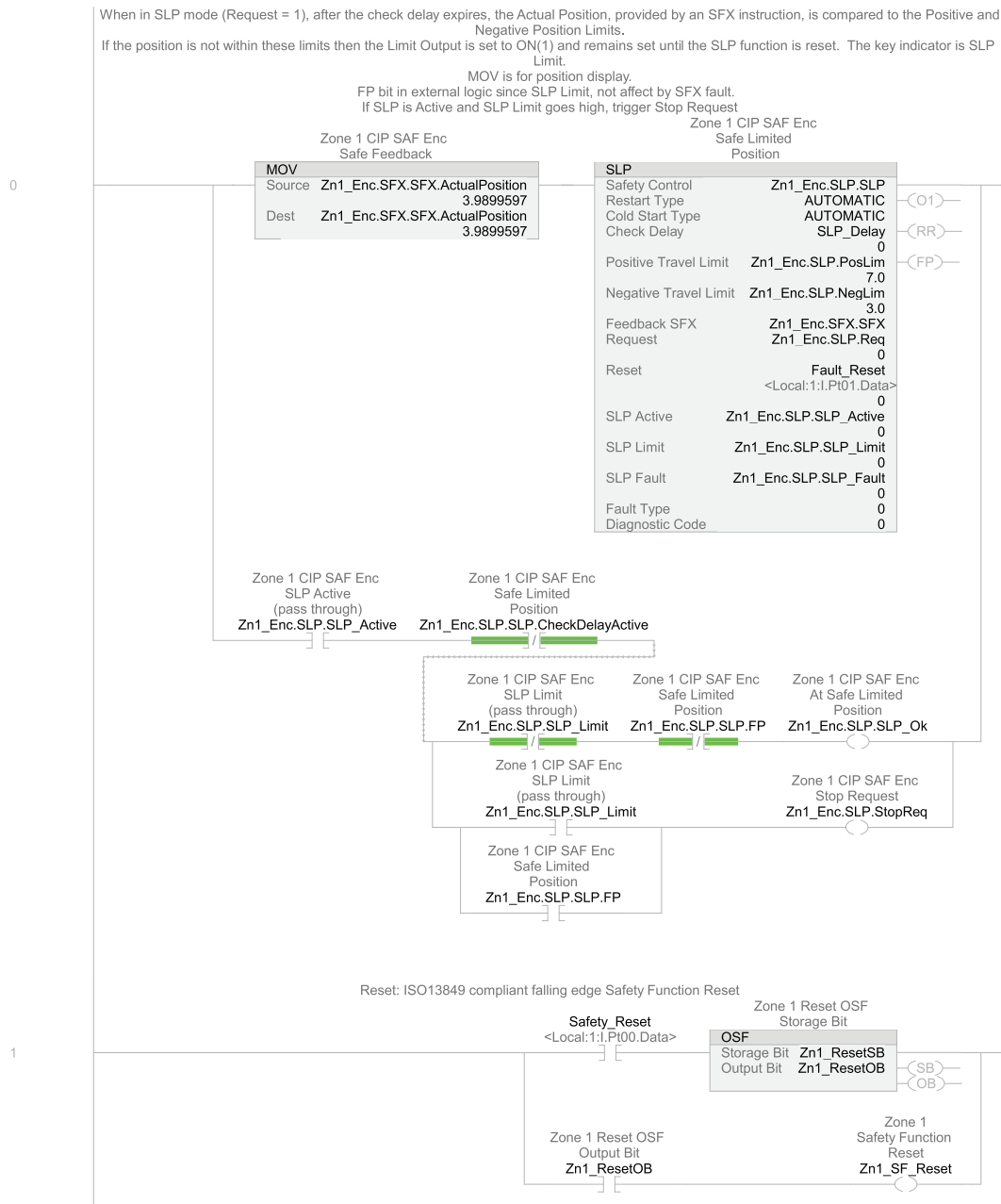
This subroutine contains the Dual Channel Input Stop (DCS) instruction that monitors dual-input safety devices whose main function is, in our example, to select the Safely-limited Position. This instruction can only energize Output 1 (O1) when both safety inputs, Channel A and Channel B, are in the active state as determined by the Input Type parameter, and the correct reset actions are implemented. The DCS instruction monitors dual-input channels for consistency (Equivalent - Active High) and detects and traps faults when the inconsistency is detected for longer than the configured Discrepancy Time (ms). The optional raC_Dvc_DCS Add-On Instruction (AOI) connects the DCS to an HMI Faceplate for use in FactoryTalk® View Machine Edition (ME), FactoryTalk View Site Edition (SE), or Studio 5000 View Designer software. The AOI_SAF_EncRollover.O_Position instruction output is designed to accumulate positive and negative position and handle position rollover in a manner supported by the SFX safety instruction. The SFX instruction output is used as input by the Drive Safety instructions, in our example, the SLP instruction. The Dual Channel Input Monitor (DCM) instruction is used to simulate a Home Prox Input physical Home position switch; the SLP requires the SLX instruction to be home before triggering the SLP execution.

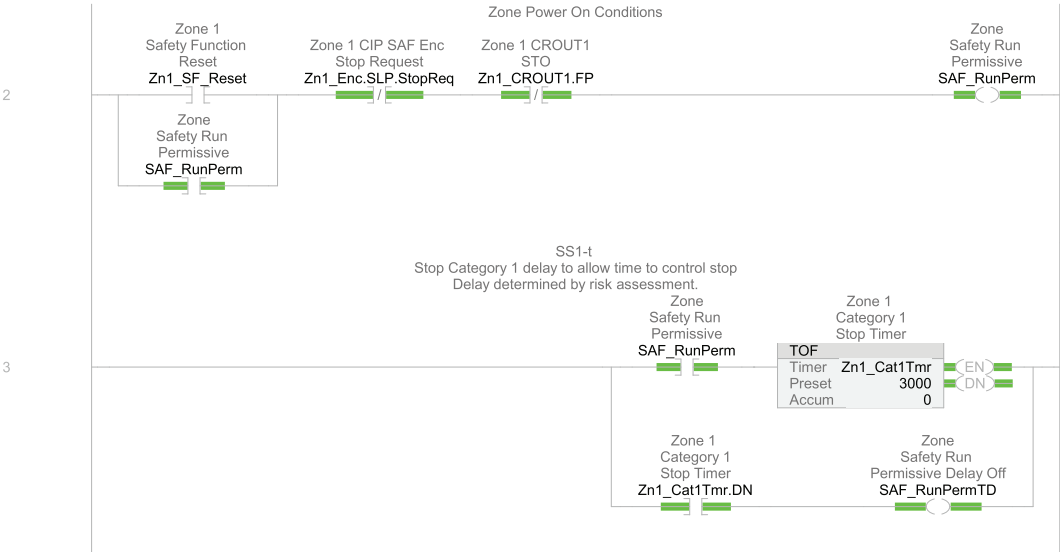




Zone1 - Logic_Main

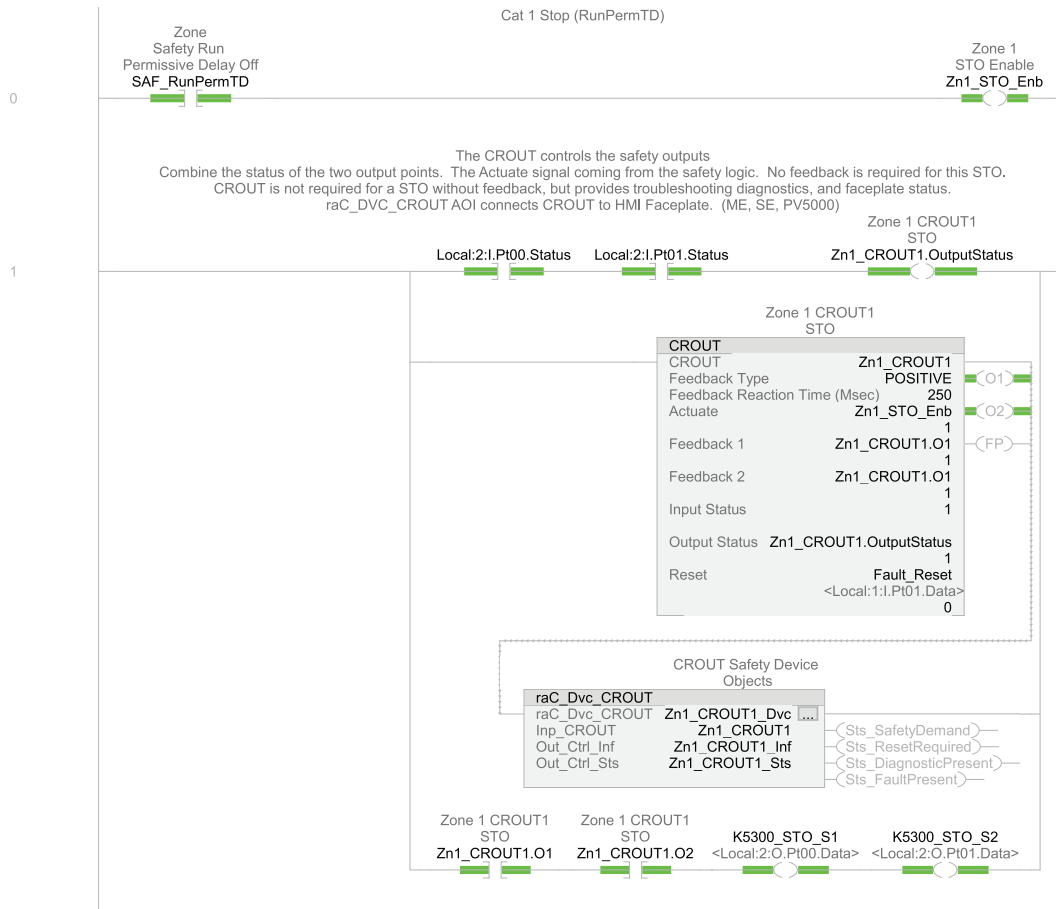
This subroutine contains the SLP instruction. When in SLP mode (Request = 1), after the Check Delay expires, the Actual Position, provided by an SFX instruction, is compared to the Positive and Negative Position Limits. If the position is not within these limits, then the Limit Output is set to high (1) and remains set until the SLP function is reset. The SLP.StopReq tag is used to generate a Safe Stop request. Rung 1 is used to manage the falling edge of the reset button signal that is compliant with the ISO 13849 standard. Rung 2 is the safe run permissive to enable the drive power. Rung 3 is used to manage a three-second time delay when a Category 1 stop (SS1-t) is requested.





Zone1 – Output_STO

This subroutine contains the Configurable Redundant Output (CROUT) instruction, which controls the safety outputs. The output Status combines the status of the two output points. The Actuate signal comes from the safety logic. No feedback is required for this STO and generally CROUT is not required for an STO without feedback, but nevertheless it provides troubleshooting diagnostics, and faceplate status. The raC_DVC_CROUT AOI connects the CROUT instruction to an HMI Faceplate for use in FactoryTalk View Machine Edition (ME), FactoryTalk View Site Edition (SE), or Studio 5000 View Designer software.



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, this safety function 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 will be different.

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

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

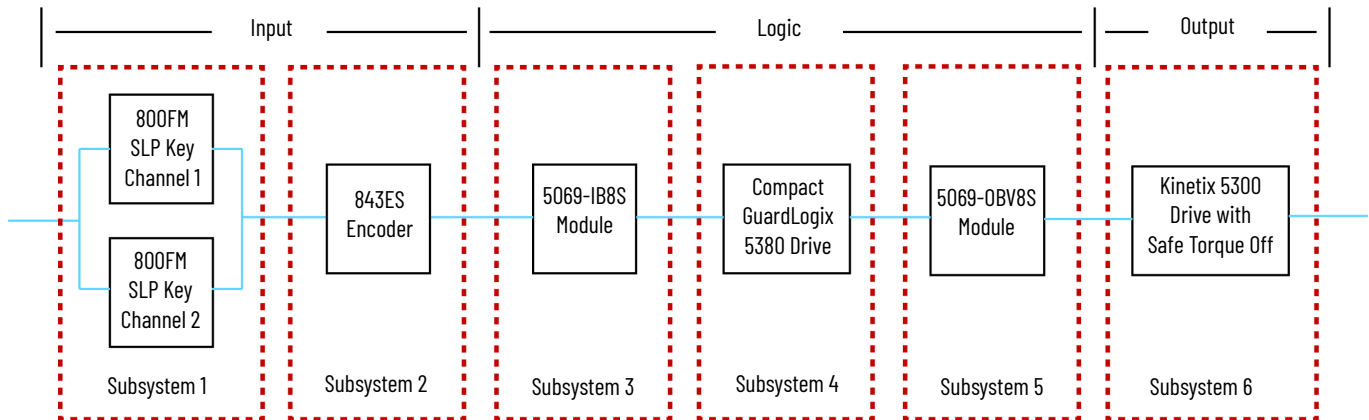
The PFHd values for the GuardLogix 5580 and Compact GuardLogix 5380 safety controllers are shown in the following graphic.

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

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	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✓SB	SLS Mode Select Key Switch	01	e	9.9E-10	80 (fulfilled)	99 (High)	2,283.1 (High)	4	fulfilled
✓SB	843ES CIP Safety Encoder	02	e	8E-9	not relevant	not relevant	not relevant	3	fulfilled
✓SB	Compact GuardLogix Safety I/O	03	e	2.5E-10	not relevant	not relevant	not relevant	4	fulfilled
✓SB	Compact GuardLogix 5380, SIL 2, Category 3	04	d	7.2E-9	not relevant	not relevant	not relevant	3	fulfilled
✓SB	Compact GuardLogix Safety I/O	05	e	3.1E-10	not relevant	not relevant	not relevant	4	fulfilled
✓SB	Motion Control: Kinetix 5300 with Safe Torque Off "Hardwired Safety"	06	d	2.1E-11	not relevant	not relevant	not relevant	3	fulfilled

The Safely-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 1.7E-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](#) 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.
EtherNet/IP Absolute Encoders: Standard and CIP Safety Models User Manual, publication 843-UM001	Provides information on how to install, configure, and program the encoder with the Studio 5000 Logix Designer application to integrate the encoder with a Logix 5000® controller-based system.
Kinetix 5300 Single-axis EtherNet/IP Servo Drives User Manual, publication 2198-UM005	Provides detailed installation instructions to mount, wire, and troubleshoot the Kinetix 5300 servo drives, and system integration for your drive and motor/actuator combination with a Logix 5000 controller.
Kinetix 5300 Single-axis EtherNet/IP Servo Drives Installation Instructions, publication 2198-IN021	Provides detailed installation instructions to mount, wire, and troubleshoot the Kinetix 5300 servo drives.
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.
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](#).





Allen-Bradley, Compact 5000, Compact I/O, CompactLogix, ControlLogix, expanding human possibility, FactoryTalk, GuardLogix, Kinetix, Logix 5000, PowerFlex, Rockwell Automation, Safety Automation Builder, SensaGuard, Studio 5000 Logix Designer, and Studio 5000 View Designer are trademarks of Rockwell Automation, Inc.

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

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

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

UNITED KINGDOM: Rockwell Automation Ltd. Pitfield, Kiln Farm Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917