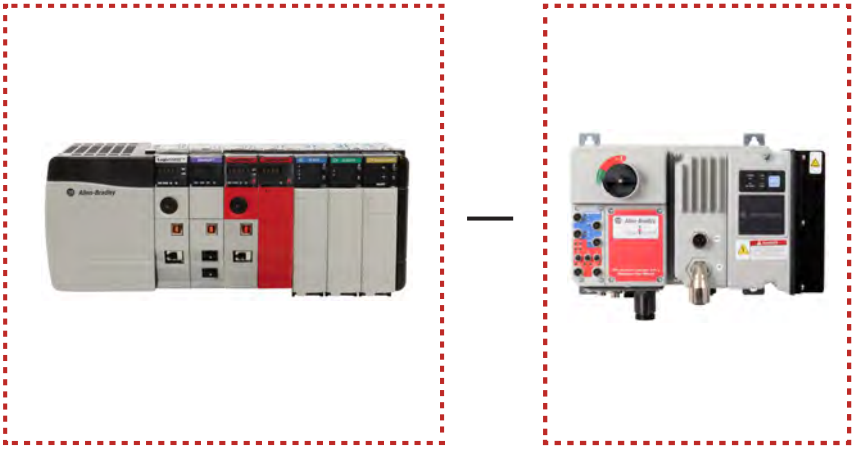
Application Technique

Allen-Bradley

Actuator Subsystems - Stop Category 0 or 1 Safety Function via an Integrated Safety Controller and an ArmorStart ST Controller with Integrated Safety

Products: GuardLogix 5580 Controller, ArmorStart ST Controller with Integrated Safety Variable Frequency Drive

Safety Rating: Cat. 4, PLe to ISO 13849-1: 2015



LISTEN. THINK. SOLVE.®

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.

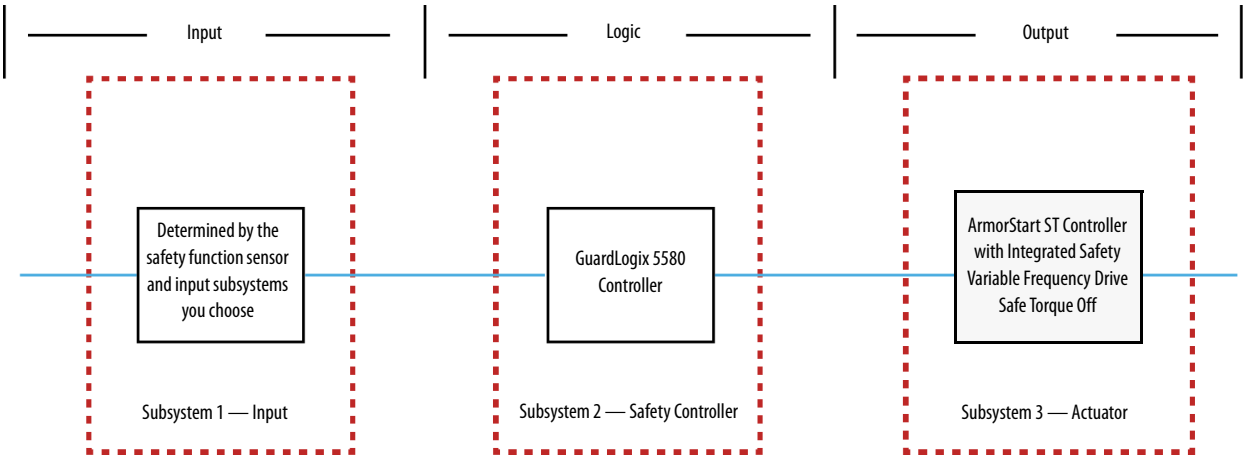
Introduction

This partial safety function application technique describes the logic and output subsystems of an overall safety system. The document illustrates how to combine a GuardLogix® safety controller with an ArmorStart® ST controller that includes an integrated safety variable-frequency drive and Safe Torque Off (STO). This combination of controllers can provide an actuator motor stop safety function with stop category 0 coast-to-stop STO, or stop category 1 controlled stop followed by STO.

Although not shown in this document, the ArmorStart ST controller with integrated safety full-voltage and reversing safety starter versions can also be applied to this safety function to provide an actuator motor stop safety function with stop category 0 coast-to-stop.

This example uses a GuardLogix 5580 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 this application technique with the sensor subsystems from any other GuardLogix safety function application technique. For example, you can use sensor subsystems 1 and 2 from Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function Application Technique, publication SAFETY-AT034, along with the actuator subsystems from this application technique, to create the following overall safety function.



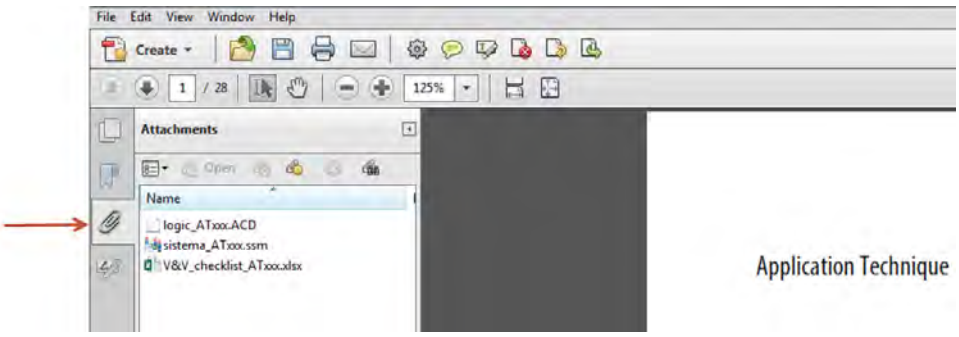
IMPORTANT You must add the PFH values for each subsystem together to create a PFH for the overall safety function. Depending on the sensor subsystems and devices you choose, the overall safety rating of your system could be reduced. The results of an example calculation for a complete safety function are shown in the section titled Calculation of the Performance Level on page 14.

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.

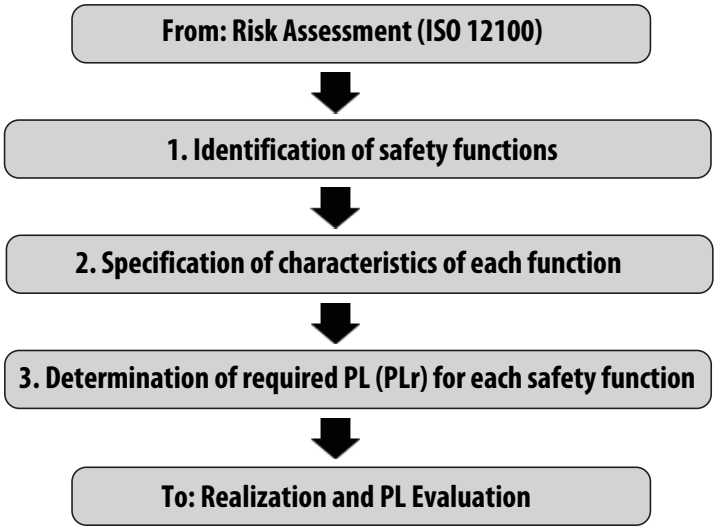
1. If you are viewing the PDF file in a browser and do not see the Attachments link, download the PDF file and open it in the Adobe Acrobat Reader application.
2. Right-click the Attachments link, and save the desired file.



3. 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 that is 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.



Actuator Stop Safety Function

This application technique includes one partial safety function: the stopping of the actuator motor when the safety system detects that one or more sensor subsystems have placed a demand on the safety function. The stopping of the motor removes the hazard. The actuator stop safety function is stop category 0, uncontrolled coasting of the actuator motor.

Safety Function Requirements

When the safety system detects that one or more sensor input subsystems have placed a demand on the safety function, stopping of the AC drive removes the hazard by preventing the motor from producing rotational torque. The STO stopping method is stop category 0, which is an uncontrolled coasting of the motor. If the risk assessment determines that coasting of the motor is dangerous, then a stop category 1 must be implemented.

The safety system cannot be reset, and hazardous motion cannot be restarted while the input subsystem places a demand on the safety system. Once the input subsystem is placed in a safe state and the safety function is successfully reset, it is possible to resume hazardous motion.

Although not included in this safety function application technique, the overall risk assessment results must be used to define the method for resuming motion of the hazard. Typically, a second action is required, such as pressing a drive Start button or toggling the drive Run selector, before hazardous motion can resume.

IMPORTANT The vendor must provide probability of failure per hour (PFH) and all relevant functional safety data for all subsystems of this safety system necessary to prove that the overall safety functions meet the requirements of this safety function.

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

Considerations for Safety Distance and Stopping Performance

Based on the selection of a sensor subsystem, the risk assessment determines if a safety distance calculation is required. Typically, a safety distance calculation is required if a non-separating sensor subsystem (such as a light curtain) is selected for the safety function. If a safety distance calculation is required for this safety function, the following documents can be referenced:

- GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication1756-RM099
- GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1856-RM012
- Machinery SafeBook 5 – Safety-related control systems for machinery, publication SAFEBK-RM002
- Safety Function: Light Curtain Products: Light Curtain GuardLogix Controller, publication SAFETY-AT056

Functional Safety Description

This safety function is a partial safety function that describes the logic and output actuator subsystems of an overall actuator stop safety function. The GuardLogix controller and ArmorStart ST controller with integrated safety are connected via an EtherNet/IP network. The GuardLogix controller and ArmorStart ST controller with integrated safety use a 1oo2 architecture to achieve the PFH values that are used in the Performance Level calculation verification section of this document.

Input Subsystem

The input subsystem can be a valid safety sensor or combination of sensors that are wired to Guard I/O™ safety inputs.

Logix Subsystem

The GuardLogix safety controller monitors its internal circuitry for proper operation and faults. The GuardLogix controller safety task and associated safety instructions are programmed to monitor the status of the safety input subsystem. When the GuardLogix controller receives a safety demand from the input subsystem or an invalid status or fault is detected, the controller logic deactivates the ArmorStart ST controller with integrated safety STO outputs, which initiates a stop category 0 coast-to-stop. An example of delaying deactivation of the ArmorStart ST controller with integrated safety variable-frequency drive STO to allow a stop category 1 controlled stop function is also provided. Depending on the result of the risk assessment, it may be necessary to use a stop category 1 controlled stop to reduce the time the motor actuator coasts to stop in applications with high inertia or vertical loads.

Actuator Subsystem

The ArmorStart ST controller with integrated safety function monitors its internal safety circuits for valid status and faults. When the GuardLogix controller de-energizes the ArmorStart ST controller with integrated safety STO outputs or the motor controller detects an invalid state or fault, a stop category 0 coast-to-stop is initiated by forcing the AC drive output inverter power devices to a disabled state. The hazardous motion of the motor that is controlled by the AC drive coasts to a stop.

ATTENTION: The ArmorStart ST controller with integrated safety function does not eliminate dangerous voltages at the drive output. Input power to the drive must be turned off and safety procedures must be followed before performing any electrical work on the drive or motor.

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

If a malfunction occurs, the most likely stop category is 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 communication 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
	Additional components depend on your input subsystems.	

Choose one of the following safety-controller hardware groups.

Controller	Cat. No.	Description	Quantity
GuardLogix 5570	1756-L71S 1756-L72S 1756-L73S	GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory, or GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory, or GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory	1
	1756-L7SP	GuardLogix Safety Partner	1
	1756-EN2TR	ControlLogix® EtherNet/IP bridge, 10/100 Mbps, two-port, twisted-pair media	1
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A7	Seven-slot ControlLogix chassis	1
Compact GuardLogix 5370	1769-L30ERMS 1769-L33ERMS 1769-L36ERMS 1769-L37ERMS 1769-L38ERMS	Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory, or Compact GuardLogix processor, 2.0 MB standard memory,1.0 MB safety memory, or Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory, or Compact GuardLogix processor, 4.0 MB standard memory, 1.5 MB safety memory, or Compact GuardLogix processor, 5.0 MB standard memory, 1.5 MB safety memory	1
	1769-PA4	Power supply, 120V/240V AC input, 2.0 A @ 24V DC	1
	1769-ECR	Right-end cap and terminator	1
GuardLogix 5580[1]	1756-L81ES 1756-L82ES 1756-L83ES 1756-L84ES	GuardLogix Processor, 3 MB standard memory, 1.5 MB safety memory, or GuardLogix Processor, 5 MB standard memory, 2.5 MB safety memory, or GuardLogix Processor, 10 MB standard memory, 5 MB safety memory, or GuardLogix Processor, 20 MB standard memory, 6 MB safety memory	1
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A7	Seven-slot ControlLogix chassis	1
Compact GuardLogix 5380–SIL 2	5069-L306ERS2 5069-L306ERMS2 5069-L310ERMS 5069-L310ERMS2 5069-L320ERS2 5069-L320ERMS2 5069-L330ERS2 5069-L330ERMS2 5069-L340ERS2 5069-L340ERMS2 5069-L350ERS2 5069-L350ERMS2 5069-L380ERS2 5069-L380ERMS2 5069-L3100ERS2 5069-L3100ERMS2	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory, or Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory, or Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory, or Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory, or Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory, or Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory, or Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory, or Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	1
	1606-XLB120E	Power supply, 24…28V DC, 120 W, 85…132V/170…264V AC input voltage	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 an ArmorStart ST controller with integrated safety.

Cat. No.	Description	Quantity
284ES/GS-FVDxPxS-xxx (284ES-FVD2P3S-10-RRG-SBG-DB1-EMI-00)	ArmorStart ST controller with integrated safety variable-frequency drive, any rating	1
281ES/GS-FxxS-xxx	ArmorStart ST controller with integrated safety full-voltage reversing motor, any rating	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

The final control device is the ArmorStart ST controller with integrated safety variable-frequency drive. Because these motor controllers use CIP Safety communication STO inputs, rather than hard-wired safety inputs, a safety output module is not needed in this safety function.

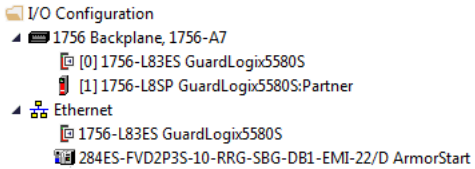
The GuardLogix controller and the ArmorStart ST controller with integrated safety variable-frequency drive must have a direct connection to one another on an EtherNet/IP network. The use of CIP Safety protocol makes the EtherNet/IP hardware between these two end devices a black channel. Therefore, any EtherNet/IP hardware can be used. Star, linear, or device level ring (DLR) EtherNet cable topologies are acceptable methods of connecting network cable media.

The overall safety function must have individual reset buttons for resetting faults and for resetting safety outputs. These reset buttons can be wired to any input module (safety or standard) in your system. The safety rating of the reset button must not diminish the rating of the relevant safety function. This condition is accomplished by the trailing edge or falling edge of the button that generates the reset command, which tolerates faults in the reset circuit.

Network Architecture

A schematic for this actuator subsystem is not needed, because the ArmorStart controller and the GuardLogix controller are connected on an EtherNet/IP network. The following I/O configuration depicts the partial safety function that uses a GuardLogix 5580 controller and safety partner via the embedded Ethernet port on the controller.

Partial Safety Function - GuardLogix 5580S Controller with Embedded Ethernet Connection



Slot 1 of the GuardLogix 5580 controller is reserved for the safety partner, which is required for SIL 3, PLe applications.

Configuration

The GuardLogix 5580 controller is configured by using the Studio 5000 Logix Designer® application, version 31 or later. You must create a project and add the products (I/O or drive, and so on). 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
30	GuardLogix 5570 controller or Compact GuardLogix 5370 controller (1769-L30ERMS, 1769-L33ERMS, 1769-L36ERMS)
31	GuardLogix 5580 controller or Compact GuardLogix 5380 controller

IMPORTANT The required versions of the Studio 5000® Add-on Profile (AOP) are:

- ArmorStart ST controller with integrated safety variable-frequency drive, AOP version 1.05 (and later)
- ArmorStart ST controller with integrated safety full-voltage reversing motor, AOP version 1.05 (and later)

ArmorStart ST controller with integrated safety firmware required versions are:

- ArmorStart ST controller with integrated safety variable-frequency drive, AOP version 1.01 (and later)
- ArmorStart ST controller with integrated safety full-voltage reversing motor, AOP version 1.01 (and later).

The latest version of the AOP can be downloaded from the Product Compatibility and Download Center (PCDC) website, rok.auto/pcdc

Create a Project with a GuardLogix Controller

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

1. In the Logix Designer application, create a project with a GuardLogix controller that includes the following:
   - A connection to an Ethernet network
     GuardLogix 5570 controllers require the use of an Ethernet communication module, but GuardLogix 5580 and Compact GuardLogix 5370 and 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.
   If you are using the embedded EtherNet/IP port on the GuardLogix 5580 module or Compact GuardLogix controllers, you must be online with the controller to set the IP address. If you are offline, the Internet Protocol tab in the Controller Properties dialog box is grayed out.
3. Configure the modules properly for your application.
   See the Additional Resources for information on your I/O modules.
4. Add the ArmorStart ST controller with integrated safety variable frequency drive to your project.
5. Set the IP address for the ArmorStart ST controller with integrated safety variable frequency drive.
   In this example, the IP address is set to 192.168.1.20. Your IP address can differ.

6. Configure the ArmorStart ST controller with integrated safety variable frequency drive properly for your application.

   See the Additional Resources for information on your product.

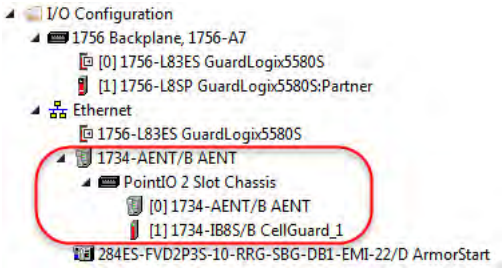
Configure the Input Subsystem

The overall safety function requires a sensor input subsystem. Create a valid input subsystem that can be used with this partial safety function.

The Complete Safety Function PL Calculation Example on page 15 is based on the input subsystems shown in the Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function, publication SAFETY-AT034, combined with the logic and actuator output safety subsystems described in this application technique. Publication SAFETY-AT034 describes input and sensor subsystems that use a SensaGuard non-contact interlock sensor and POINT Guard I/O 1734-IB8S safety input module with a POINT I/O™ 1734-AENT EtherNet/IP communication adapter for the input subsystem. The input sensor circuits can be wired to the safety input module shown in this application technique or added as a separate node on this safety function parent network.

Here is an example of a GuardLogix 5580 complete safety system network architecture including the input subsystem that is used in publication SAFETY-AT034 with a separate 1734-AENT communication adapter node AENT on this safety function parent network.

Example, Overall Safety Function



Configure the ArmorStart ST Controller with Integrated Safety

The ArmorStart ST motor controller with integrated safety is created and configured using the Studio 5000 Logix Designer® Add-on Profile (AOP) module. A detailed description of how to fully configure the ArmorStart ST controller is beyond the scope of this document. See the ArmorStart ST Motor Controller with Integrated Safety User Manual, publication 280ES-UM002, for further details.

Programming

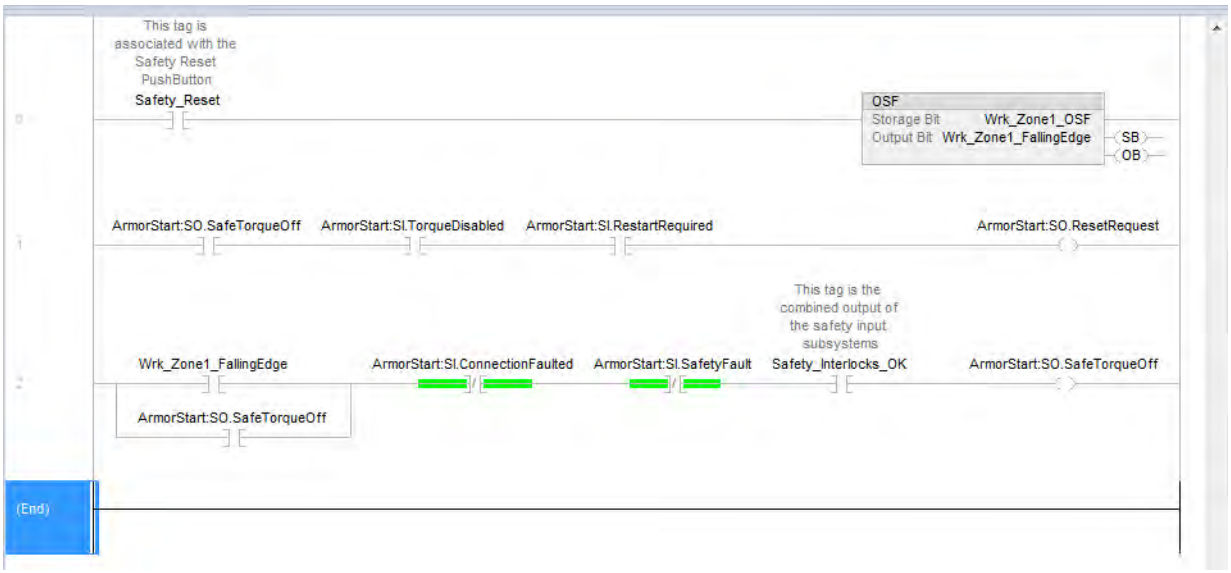
The accumulated Safety_Interlocks_OK tag is the resultant output from the safety input and logic subsystems. It is used as a permissive in the Safety Torque Off (STO) logic. Rung 2 in the following safety program logic screen captures shows this tag. If the Safety_Interlocks_OK tag goes false (0), it initiates the STO function. The STO function remains false (0) until a manual reset action is conducted after the Safety_Interlocks_OK tag goes true (1).

The ArmorStart ST controller with integrated safety STO function requires a reset after the STO function is initially energized. Rung 1 in the following application logic screen captures accomplishes this reset. For details on the reset function, see the STO Reset topic in the appropriate PowerFlex® drive manual, which is listed in the Additional Resources on page 18.

Safety Task Logic – Stop Category 0, Coast-to-stop

The following code is an example for a category 0 coast-to-stop. When a demand is placed on safety interlocks, and the accumulated Safety_Interlocks_OK tag goes to false (0), then the ArmorStart:SO.SafeTorqueOff output immediately goes to false (0) as well.

For controller logic that you can download to your controller, see the attached ACD file.



Safety Task Logic – Stop Category 1, Controlled Stop

The following code is an example for a category 1 stop that can be used with the ArmorStart ST controller with integrated safety variable-frequency drive. When a demand is placed on the safety interlocks, and the accumulated Safety_Interlocks_OK tag goes to false (0), the STO_enable tag goes false (0) immediately.

This action initiates the CAT1_delay Timer Off Delay (TOF). The Drive_Stop tag goes false (0) immediately and is used to initiate a controlled stop of the drive. The Drive_Stop tag is used to initiate a drive ramp stop by controlling the ArmorStart:O.RunForward and ArmorStart:O.RunReverse tags. The method that is used for a stop category 1 controlled stop is application-specific and determined by the risk assessment. A normal ramp deceleration or torque limit fast stop may be required.

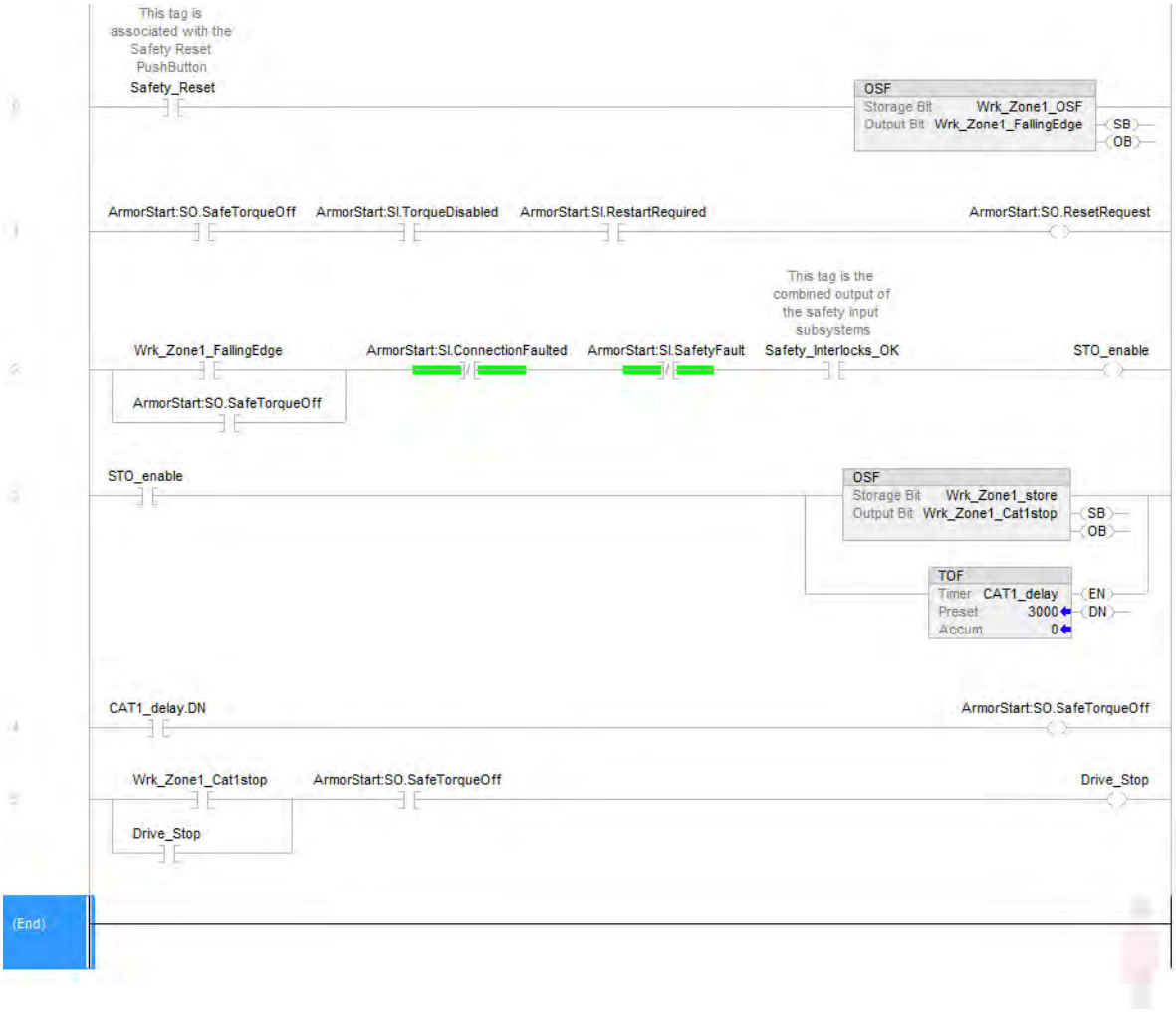
After the CAT1-delay timer times out, the CAT1_delay.DN bit goes false (0), which then causes the ArmorStart:SO.SafetTorqueOff output to go false (0). This action initiates the drive STO.

Even if the motor has not reached zero speed, when the CAT1_delay timer expires, the drive STO is initiated and if the motor is still rotating, it coasts to stop.

The CAT1_delay timer preset is determined in the risk assessment. In this example, the delay time is three seconds.

Reset of the STO logic is the same as described for the stop category 0 logic shown earlier.

For controller logic that you can download to your controller, see the attached ACD file.



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, the ArmorStart ST controller with integrated safety subsystem can be used in a safety function that achieves a safety rating of category 4, Performance Level e (cat. 4, 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 sensor subsystems along with the logic and actuator subsystems that are shown here. Depending on the sensor subsystems and devices you choose, the overall safety rating of your system could be reduced. An example that describes how to calculate the safety rating for a complete safety function appears in the section titled Complete Safety Function PL Calculation Example on page 15.

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

The PFH for electromechanical subsystems 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.

Logic and Actuator Subsystem Calculation

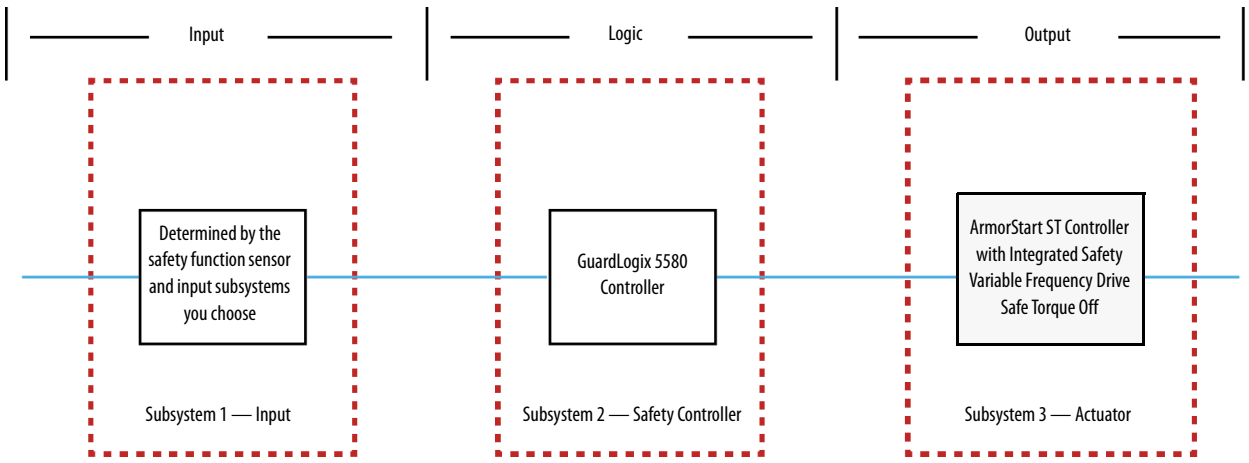
The calculations for the logic subsystem are shown in the following graphic.

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category	Use case
✔ SB	Safety PLC: Compact GuardLogix 5370	e	n.a.	1.5E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled	[Standard Use Case]
✔ SB	Safety PLC: GuardLogix 1756-L7xS & L7SP	e	n.a.	1.2E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled	[Standard Use Case]
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	n.a.	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled	[Standard Use Case]
✔ SB	Safety PLC: GuardLogix 1756-L8xES & L8SP	e	n.a.	7.4E-11	*not relevant*	*not relevant*	*not relevant*	4	fulfilled	[Standard Use Case]

The calculations for the actuator subsystem are shown in the following graphic.

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔ SB	ArmorStart ST 284ES/GS VFD	e	n.a.	3.6E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	ArmorStart ST 281ES/GS Starter	e	n.a.	3.6E-9	*not relevant*	*not relevant*	*not relevant*	4	fulfilled

The Actuator Stop safety function can be modeled as follows:



Complete Safety Function PL Calculation Example

This example takes one of the logic subsystems and one of the actuator subsystems from this document and combines them with the sensor subsystems from Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function Application Technique, publication SAFETY-AT034, to illustrate how any sensor subsystems can be added to the output subsystems within this publication. If you choose different products, you will need new calculations.

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	Safety PLC: GuardLogix 1756-L8xES & L8SP	e	n.a.	7.4E-11	not relevant	not relevant	not relevant	4	fulfilled
SB	ArmorStart ST 284ES/GS VFD	e	n.a.	3.6E-9	not relevant	not relevant	not relevant	4	fulfilled

Here are the subsystems from Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function Application Technique, publication SAFETY-AT034.

Safety function

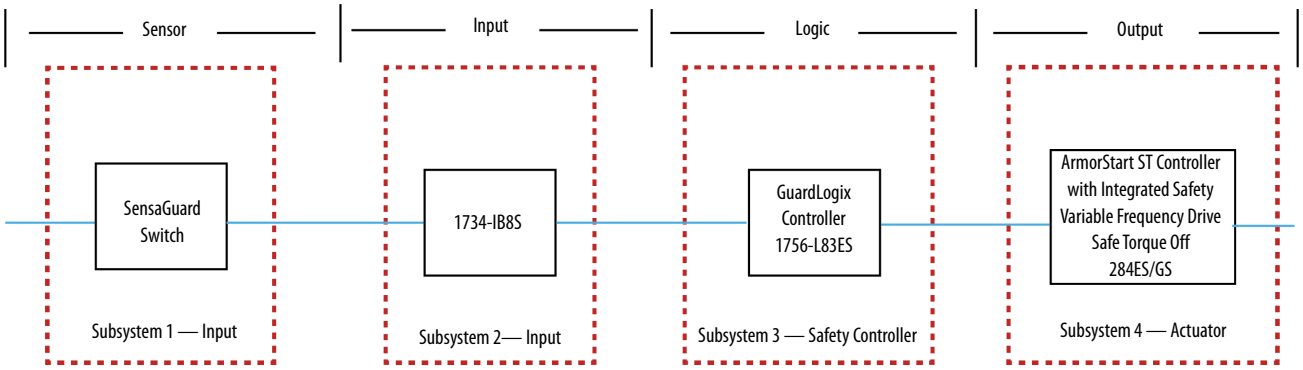
IFA

Documentation | PLr | PL | Subsystems

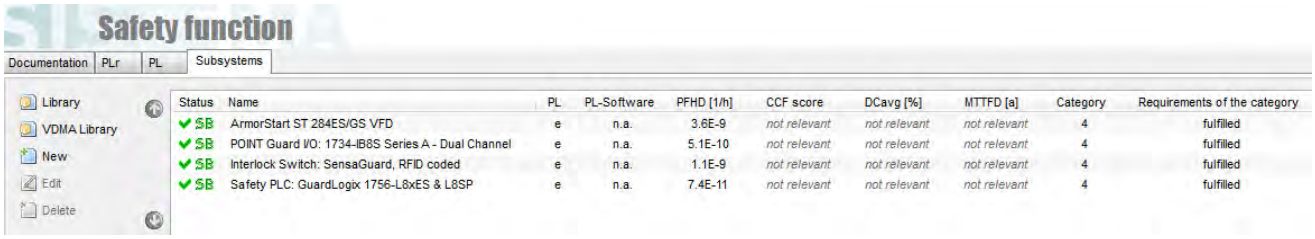
Library
New
Edit
Delete

	Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
SB	Interlock Switch: SensaGuard	e	1.12E-9	not relevant	not relevant	not relevant	4	fulfilled
SB	POINT Guard I/O: 1734-IB8S	e	5.1E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	Safety PLC: Compact GuardLogix 1...	e	2.1E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	POINT Guard I/O: 1734-OB8S	e	5.14E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	Contactors 100S	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled

The sensor subsystems from Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function Application Technique, publication SAFETY-AT034, are the SensaGuard Interlock Switch and the 1734-IB8S POINT Guard I/O™ input module. The overall safety function is shown here. It combines those sensor subsystems from publication SAFETY-AT034, and the logic and actuator subsystems from this document.



The PFH values for each subsystem in the safety function that is modeled in the graphic are taken from their respective publications and combined.



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 5.3E-09. The PL for the complete safety function is PLe.

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 Safety Reference Manual, publication 1756-RM095.

For a validation checklist, see the attached spreadsheet.

IMPORTANT In addition to using the verification and validation steps that are provided in the spreadsheet, consult the application technique for your input subsystem for the steps that are required to validate the input device. For the input subsystem example used in this safety function application technique, we reference Door-monitoring Interlock Switch with an Integrated Safety Controller Safety Function Application Technique, publication SAFETY-AT034.

Additional Resources

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

Resource	Description
ArmorStart ST Motor Controller with Integrated Safety User Manual, publication 280ES-UM002	Describes the ArmorStart ST controller with integrated safety. Provides instructions on how to install, wire, and configure the ArmorStart controller.
ArmorStart ST Distributed Motor Controller Specifications Technical Data, publication 280ES-TD001	Describes important specifications and technical data for the ArmorStart ST controller with integrated safety.
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 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information on how to install, configure, and program the ControlLogix 5580 and 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 CompactLogix 5380 and Compact GuardLogix 5380 controllers in the Logix Designer application.
GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099	Describes the GuardLogix 5570 controller and Compact GuardLogix 5370 controller system. Provides instructions on how to develop, operate, or maintain a controller-based safety system that uses the Studio 5000 Logix Designer application.
GuardLogix 5570 Controllers User Manual, publication 1756-UM022	Provides information on how to install, configure, and program the GuardLogix 5570 controllers in the Logix Designer application.
Compact GuardLogix 5370 Controllers User Manual, publication 1769-UM022	Provides information on how to install, configure, and program the Compact GuardLogix 5370 controllers in the Logix Designer application.
GuardLogix Safety Application Instruction Set 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.
Rockwell Automation Functional Safety Data Sheet, publication SAFETY-SR001	Provides functional safety data for Rockwell Automation products.
Industrial Automation Wiring and Grounding Guidelines, publication1770-4.1	Provides general guidelines on how to install 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 control system to (EN) ISO 13849-1.

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

Notes:

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	www.rockwellautomation.com/knowledgebase
Local Technical Support Phone Numbers	Locate the phone number for your country.	www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	www.rockwellautomation.com/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

Publication SAFETY-AT177A-EN-P - January 2020