Allen-Bradley

Pneumatic Safety Valves Safety Function

Products: GuardLogix Controller, E-stop Button, Safety I/O Module, DM^2 Pneumatic Safety Valve

Safety Rating: CAT. 3, PLd to ISO 13849-1: 2008

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.

Safety Distance Calculations

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 reduce the risk to a tolerable level. Safety circuits must consider safety distance calculations, which are not part of the scope of this document.

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 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 prevent hazardous zones being reached by upper and lower limbs

ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

Separating safeguards monitor a moveable, 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 assure compliance.

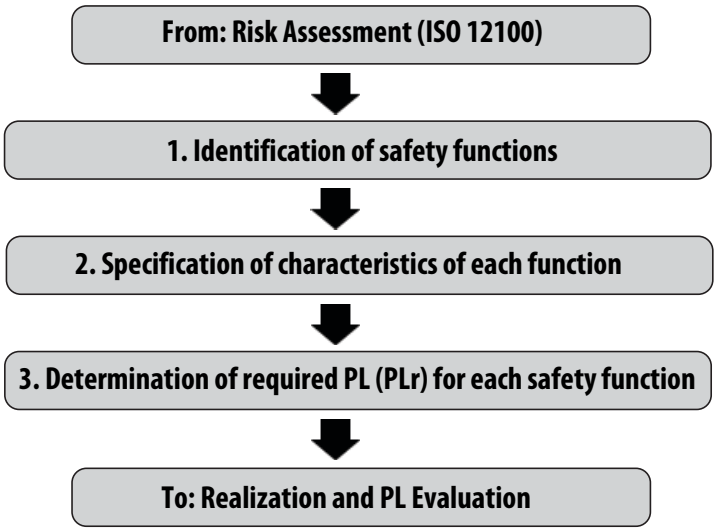
Introduction

This safety application technique explains how to wire, configure, and program a Compact GuardLogix controller and POINT Guard I/O™ module to monitor a dual-channel E-stop device. If the E-stop is actuated, or a fault is detected in the monitoring circuit, the GuardLogix® controller de-energizes the final control device, in this case, a DM$^{2®}$ pneumatic safety valve from ROSS Controls.

This example uses a Compact GuardLogix controller, but is applicable to any GuardLogix controller. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) software calculations that are shown later in this document must be recalculated if different products are used.

Safety Function Realization: Risk Assessment

The required performance level 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 (PLr) 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.



Pneumatic Safety Valves Safety Function

This application technique includes one safety function: the removal of power or energy from the hazard by actuation of any of the emergency stop push buttons.

Safety Function Requirements

Pressing any one of the series-wired E-stop buttons stops and prevents hazardous motion by removing power to the pneumatic safety valve. When the E-stop button is reset, the hazardous motion and power to the pneumatic safety valve do not resume until a secondary action (the Reset button is pressed and released) occurs. Faults at the E-stop button, wiring terminals, or safety controller are detected before the next safety demand. This emergency stop function is complementary to any other safeguards on the machine and does not reduce the performance of other safety-related functions.

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

Hazardous motion is interrupted or prevented by actuation of any of the emergency stop buttons (ES1, ES2, or ES3). Each E-stop is considered a separate safety function. The E-stop buttons are connected in series to a pair of safety inputs of a safety input module (SI1). The pneumatic safety valve is connected to a pair of safety outputs of a safety output module (SO1). The I/O modules are connected via CIP Safety™ through an EtherNet/IP™ network to the safety controller (SC1). The safety code in SC1 monitors the status of the E-stop buttons by using a pre-certified safety instruction named Dual Channel Input Stop (DCS). When all conditions are satisfied, and no faults are detected on the input modules, and a Reset button is pressed and released, a secondary certified function block called Configurable Redundant Output (CROUT) checks the status of the final control device, a pneumatic safety valve. The safety controller then issues an output signal to the safety output module (SO1) to switch on a pair of safety outputs to energize the pneumatic safety valve.

Bill of Material

This application technique uses these products.

Cat. No.	Description	Quantity
800FM-G611MX10	800F reset push button - metal, guarded, blue, R, metal latch mount, one normally-open contact, standard	1
800FM-MT44MX02	800F non-illuminated mushroom operators, twist-to-release, 40 mm (1.58 in.), round metal (type 4/13, IP66), red, metal latch mount, 0 normally-open contacts, 2 normally-closed contacts, standard, standard pack	1
800F-15YSE112	800F legend plate, 60 mm (2.36 in.) round, universal emergency stop, yellow with black legend text, 22.5 mm (.89 in.) opening	3
DM^2CNAxxA21	DM^2 series pneumatic safety valve – Contact ROSS Controls for proper valve sizing and a specific part number	1
1768-ENBT	CompactLogix™ EtherNet/IP bridge module	1
1768-L43S	Compact GuardLogix processor, 2.0 MB standard memory, 0.5 MB safety memory	1
1768-PA3	Power supply, 120/240V AC Input, 3.5 A @ 24V DC	1
1769-ECR	Right end cap/terminator	1
1734-AENT	24V DC Ethernet adapter	1
1734-TB	Module base with removable IEC screw terminals	4
1734-IB8S	POINT Guard I/O safety input module	1
1734-OB8S	POINT Guard I/O safety output module	1
1783-US05T	Stratix 2000™ unmanaged Ethernet switch	1

Setup and Wiring

For detailed information on how to install and wire, refer to the publications listed in the Additional Resources.

System Overview

The 1734-IB8S input module monitors the inputs from the E-stops, which are connected in series.

The 1734-IB8S module can source the 24V DC for all input channels to dynamically test the signal wiring for shorts to 24V DC and channel-to-channel shorts. If a fault occurs, either or both channels are set to low (0), and the controller reacts by dropping out the pneumatic safety valve. Only after the fault is cleared and the Reset button is pressed and released does the function block reset.

Shorts to 0V DC (and wire off) are seen as an open circuit by the 1734-IB8S input module, and the controller reacts by dropping out the pneumatic safety valve. If the inputs remain discrepant for longer than the discrepancy time, then the function block in the controller safety task declares a fault. Only after the fault is cleared, and the Reset button is pressed and released, does the function block reset.

The final control device is a pneumatic safety valve that is controlled by a 1734-OB8S output module. A feedback circuit is wired through the normally-open contact and back to an input of the 1734-IB8S module to monitor the pneumatic safety valve for proper operation. The pneumatic safety valve cannot restart if the feedback circuit is not in the correct state.

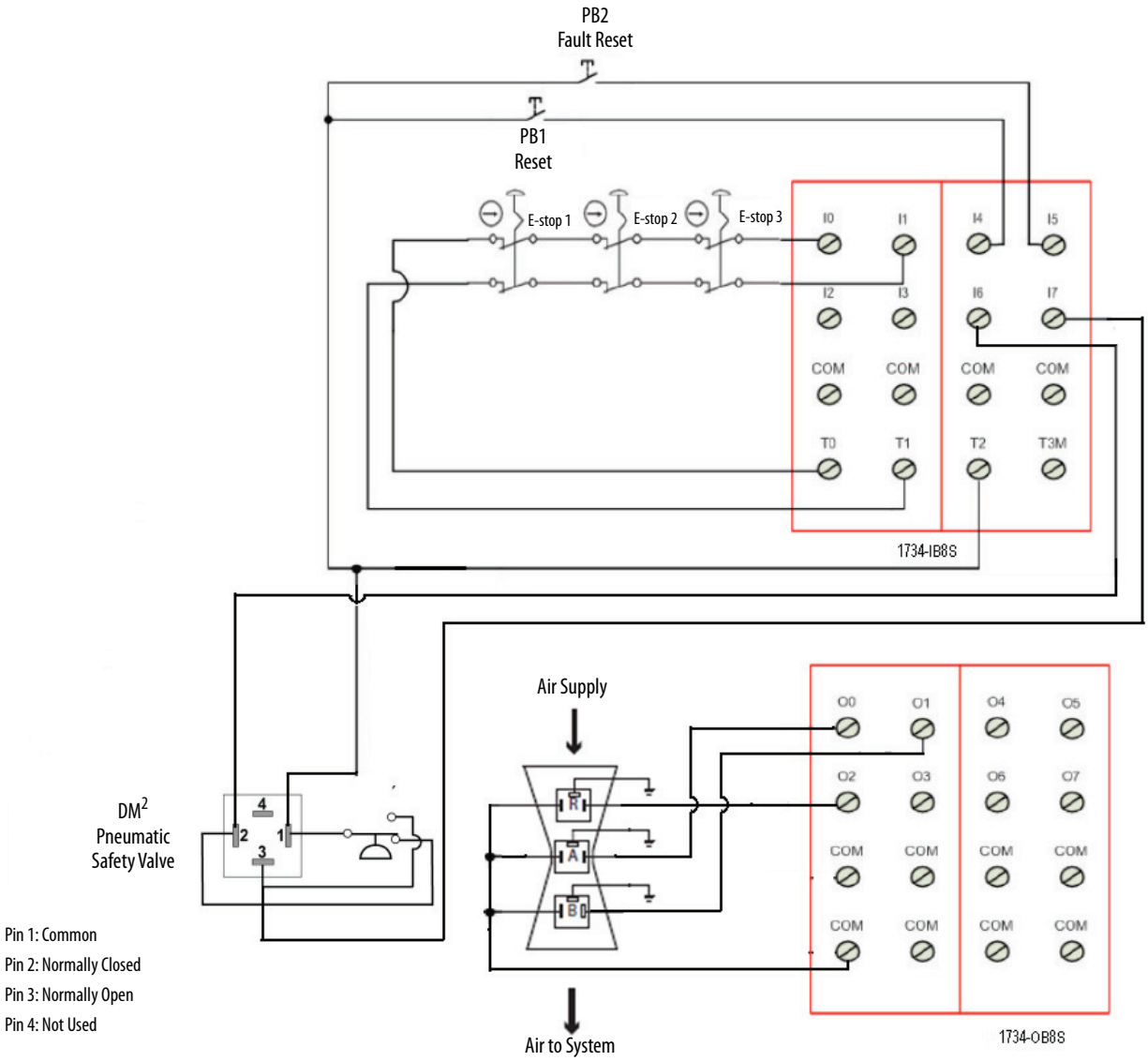
The maximum output current is 1 A for each output point of the 1734-OB8S module.

Primary power consumption for each solenoid is as follows:

- 15.8VA inrush
- 12.8VA holding on 50 Hz or 60 Hz
- 5.8 W on DC

The system has individual Reset buttons for resetting faults and safety outputs. The Reset buttons and the pneumatic safety valve Ready to Run (N.O. Contacts) and Fault Indicator (N.C. Contacts) are all wired to the 1734-IB8S module in this example. This configuration is not required for functional safety. These four inputs can be wired to a standard input module.

Electrical Schematic



Pins 1 and 3 are connected when air pressure is present and the valve is Ready to Run.

If a fault has occurred or pressure is removed from the valve inlet, pins 1 and 2 are connected.

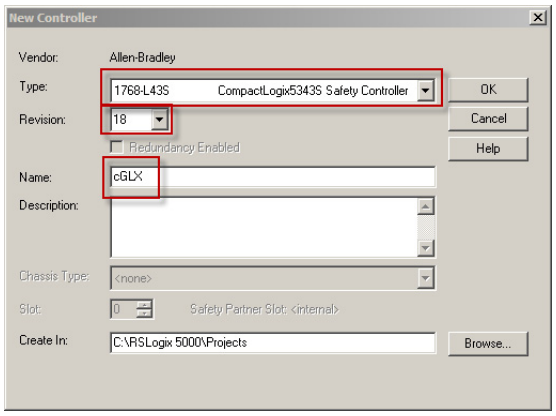
In the event of a fault, remove power from the pilot solenoids (A and B) momentarily, and apply power to the Reset solenoid to return the valve to Return To Run state. Wait at least 250 ms after removing power from the reset solenoid before trying to re-energize the pilot solenoids.

Configuration

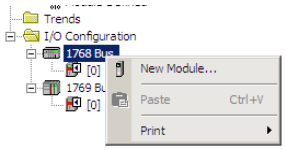
The Compact GuardLogix controller is configured by using RSLogix 5000® software, version 18 or later. You must first create a project and add the I/O modules. Then, configure the I/O modules for the correct input and output types. A detailed description of each step is beyond the scope of this document. Knowledge of the RSLogix™ programming environment is assumed.

Create a Project with a Compact GuardLogix Controller

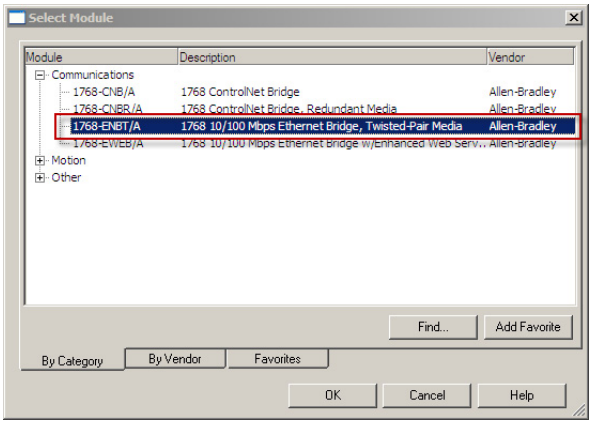
1. In the RSLogix 5000 software, create a project.
2. In the New Controller dialog box, do the following:
   a. From the Type pull-down menu, choose 1768-L43S CompactLogix™ 5343S Safety Controller.
   b. From the Revision pull-down menu, choose the appropriate revision for the controller.
   c. In the Name box, type an appropriate name for the controller.
   d. Click OK.



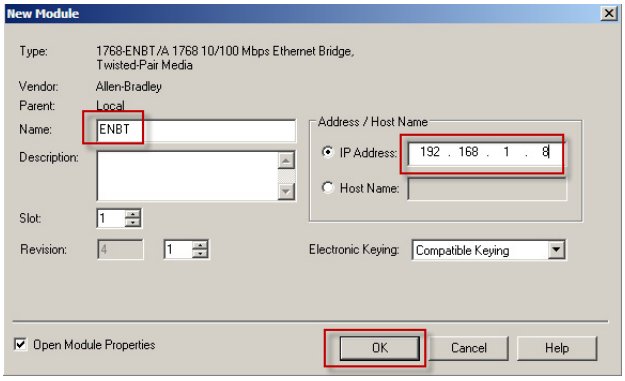
3. In the Controller Organizer, add the 1768-ENBT module to the 1768 bus.



4. In the Select Module dialog box, select the 1768-ENBT module, and click OK.

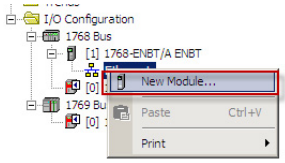


5. In the New Module dialog box, do the following:
   a. Name the module.
   b. Type its IP address.
   c. Click OK.

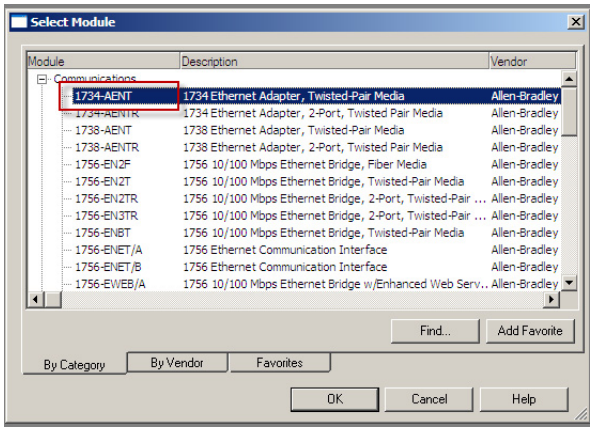


We used 192.168.1.8 for this application example. Yours can be different.

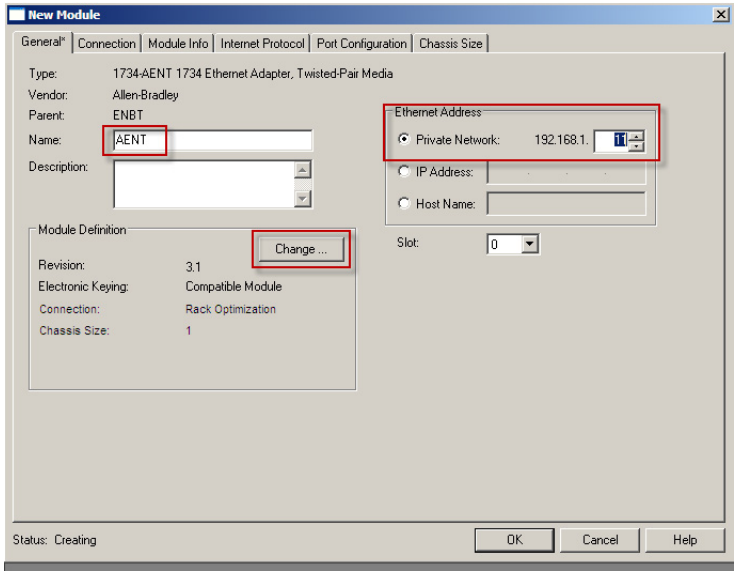
6. In the Controller Organizer, right-click 1768-ENBT module, and choose New Module.



7. In the Select Module dialog box, select the 1734-AENT adapter, and click OK.

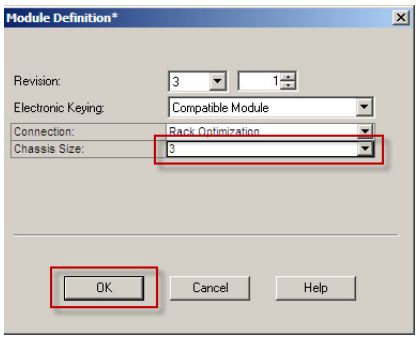


8. In the New Module dialog box, do the following:
   a. Name the module.
   b. Type its IP address.
   c. Click OK.
   d. Click Change.



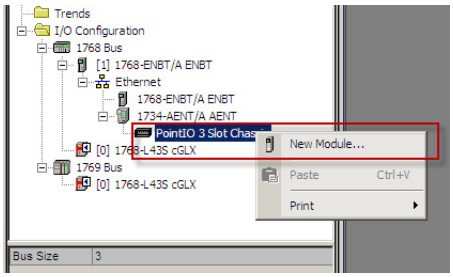
We used 192.168.1.11 for this application example. Yours may be different.

9. From the Chassis Size pull-down menu, choose 3 and click OK.

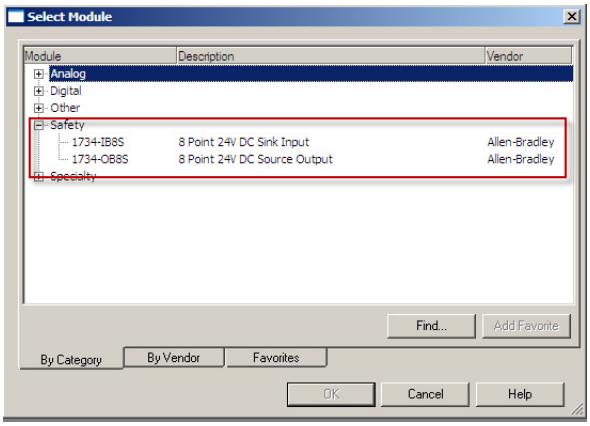


Chassis size is the number of modules that are inserted in the chassis. The 1734-AENT adapter is considered to be in slot 0, so for one input and one output module, the chassis size is 3.

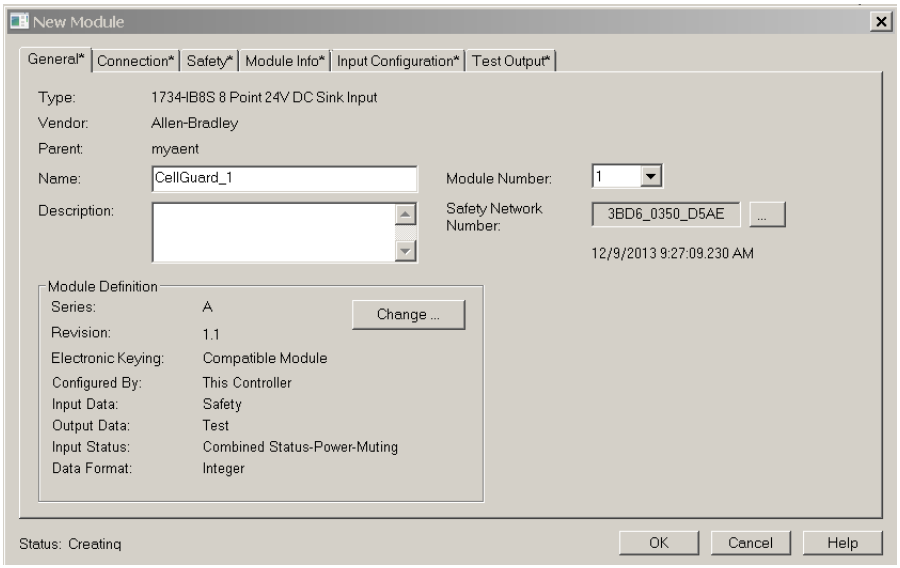
10. In the Controller Organizer, right-click the PointIO 3 Slot Chassis adapter and choose New Module.



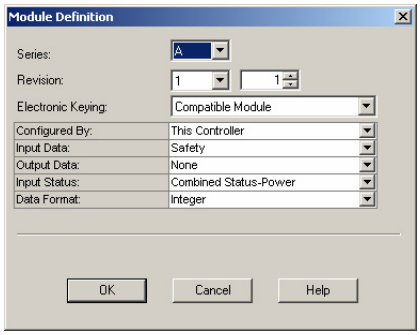
11. Expand Safety, select the 1734-IB8S module, and click OK.



12. In the New Module dialog box, name the device CellGuard_1 and click Change.



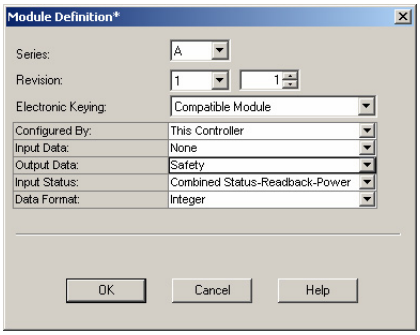
13. When the Module Definition dialog box opens, change the Output Data to None verify that the Input Status is Combined Status-Power, and click OK.



Setting the output data to None means that you cannot use the Test Outputs as standard outputs, which is appropriate in this example. This configuration saves one controller connection, because we are using only the input connection.

14. Close the Module Properties dialog box by clicking OK.

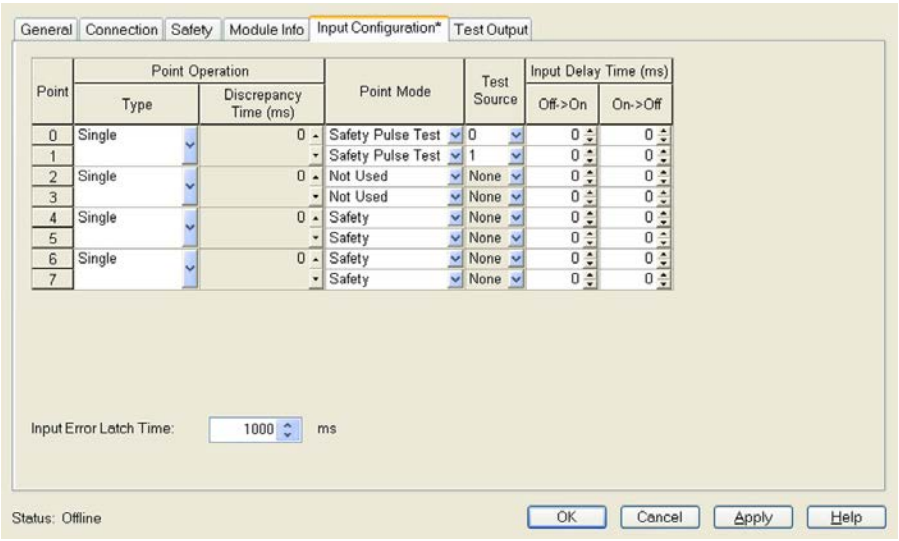
15. Repeat steps 10...14 to add the 1734-OB8S safety output module.
16. Name the module OB8S.
17. Choose slot 2.
18. In the Module Definition dialog box, set the Input Status to Combined Status-Readback-Power.



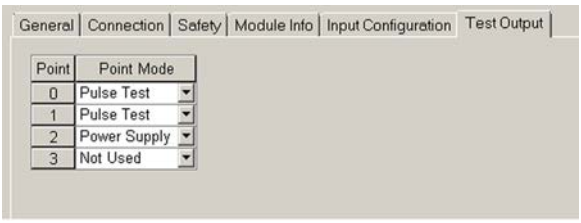
Configure the I/O Modules

Follow these steps to configure the POINT Guard I/O modules.

1. In the Controller Organizer, right-click the 1734-IB8S module and choose Properties.
2. Click Input Configuration and configure the module as shown.

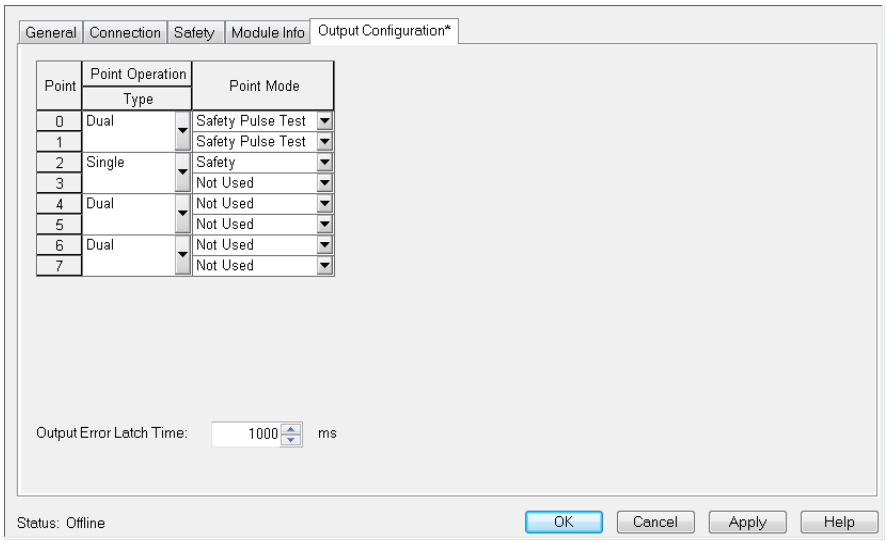


3. Click Test Output and configure the module as shown.



4. Click OK.
5. In the Controller Organizer, right-click the 1734-OB8S module and choose Properties.

6. Click Output Configuration and configure the module as shown.



7. Click OK.

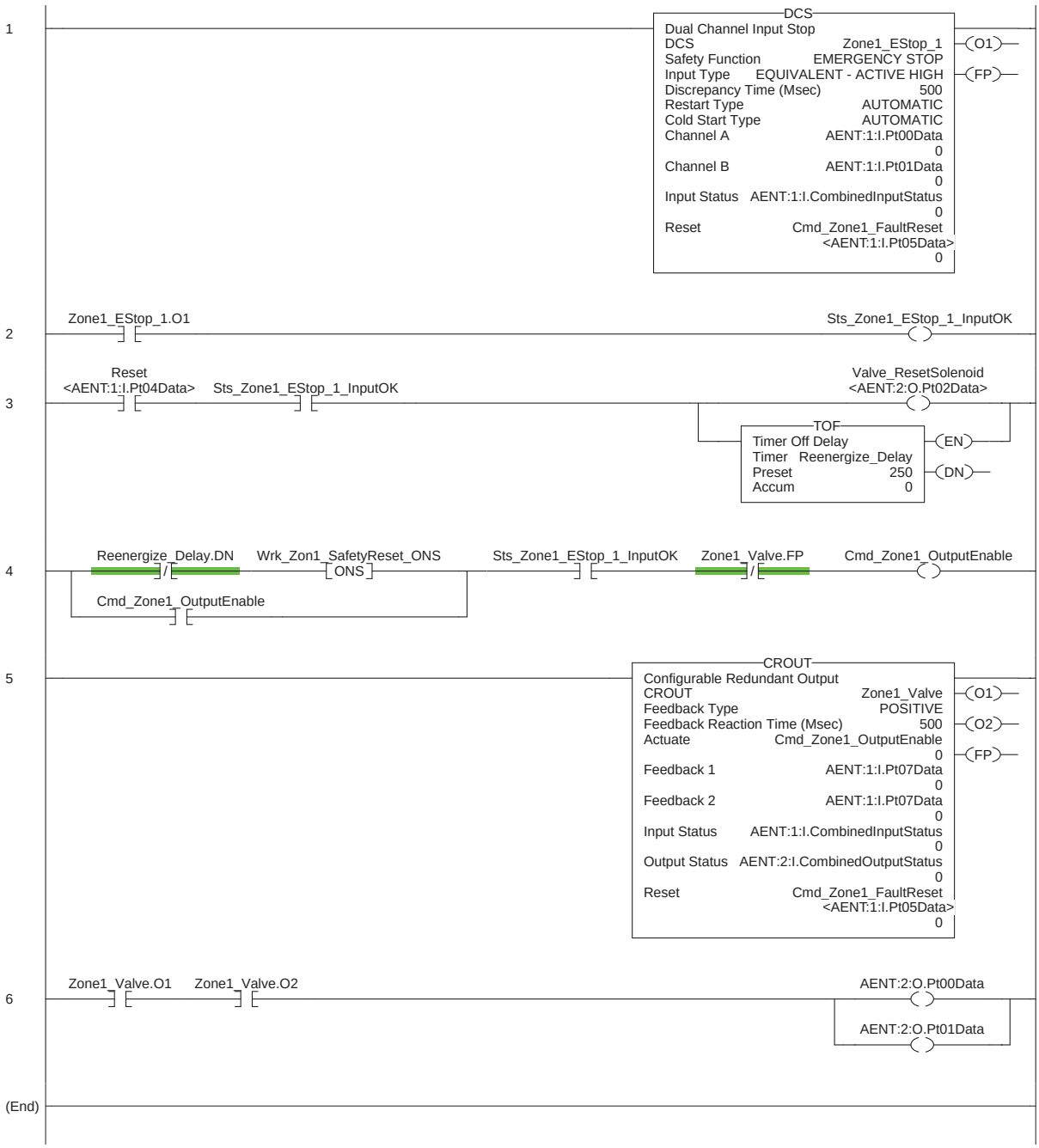
Programming

The Dual Channel Input Stop (DCS) instruction monitors dual-input safety devices, for example, an E-stop, light curtain, or safety gate, whose main function is to stop a machine safely. This instruction can energize the output only when both safety inputs (Channels A and B) are in the active state, as determined by the input type parameter, and the correct reset actions are implemented. The DCS instruction monitors the 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 Configurable Redundant Output (CROUT) instruction controls and monitors redundant outputs. The reaction time for output feedback is configurable. The instruction supports positive and negative feedback signals.

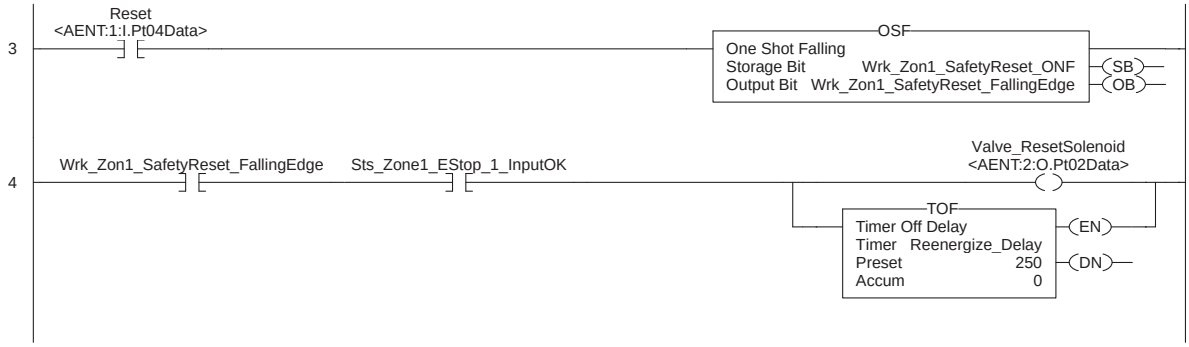
The safety application code in the safety output routine prevents outputs from restarting if the input channel resets automatically, which provides anti-tiedown functionality for the circuit reset.

The input OK status is used as a permissive in the safety output routines.


1
DCS
Dual Channel Input Stop
DCS Zone1_EStop_1
Safety Function EMERGENCY STOP
Input Type EQUIVALENT - ACTIVE HIGH
Discrepancy Time (Msec) 500
Restart Type AUTOMATIC
Cold Start Type AUTOMATIC
Channel A AENT:1:I.Pt00Data
0
Channel B AENT:1:I.Pt01Data
0
Input Status AENT:1:I.CombinedInputStatus
0
Reset Cmd_Zone1_FaultReset
<AENT:1:I.Pt05Data>
0
O1
FP
2
Zone1_EStop_1.O1
Sts_Zone1_EStop_1_InputOK
3
Reset
<AENT:1:I.Pt04Data>
Sts_Zone1_EStop_1_InputOK
Valve_ResetSolenoid
<AENT:2:O.Pt02Data>
TOF
Timer Off Delay
Timer Reenergize_Delay
Preset 250
Accum 0
EN
DN
4
Reenergize_Delay.DN
Wrk_Zon1_SafetyReset_ONS
ONS
Sts_Zone1_EStop_1_InputOK
Zone1_Valve.FP
Cmd_Zone1_OutputEnable
Cmd_Zone1_OutputEnable
5
CROUT
Configurable Redundant Output
CROUT Zone1_Valve
Feedback Type POSITIVE
Feedback Reaction Time (Msec) 500
Actuate Cmd_Zone1_OutputEnable
0
Feedback 1 AENT:1:I.Pt07Data
0
Feedback 2 AENT:1:I.Pt07Data
0
Input Status AENT:1:I.CombinedInputStatus
0
Output Status AENT:2:I.CombinedOutputStatus
0
Reset Cmd_Zone1_FaultReset
<AENT:1:I.Pt05Data>
0
O1
O2
FP
6
Zone1_Valve.O1
Zone1_Valve.O2
AENT:2:O.Pt00Data
AENT:2:O.Pt01Data
(End)

Falling Edge Reset

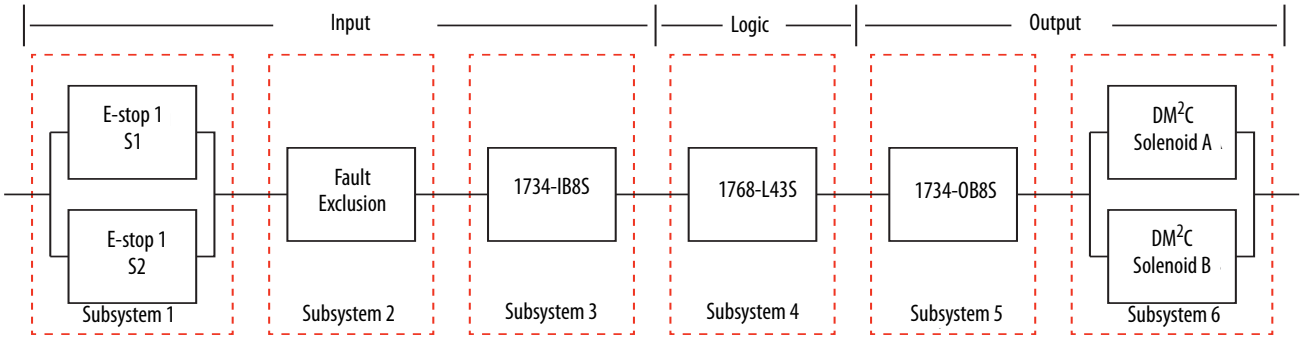
ISO 13849-1 stipulates that instruction reset functions must occur on falling edge signals. To comply with this requirement, add a One Shot Falling (OSF) instruction to the rung immediately preceding the Cmd_Zone1_OutputEnable rung. Then, use the OSF instruction Output Bit tag as the reset bit for the following rung. The Cmd_Zone1_OutputEnable is then used in the Enable the CROUT instruction. Modify the reset code as shown.



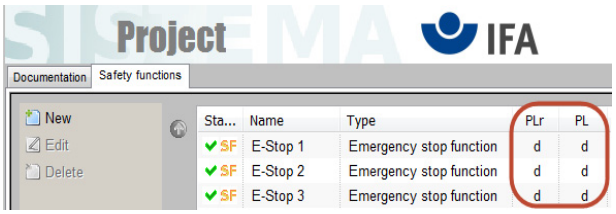
Calculation of the Performance Level

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: 2008, as calculated by using the SISTEMA application. SISTEMA is a software tool that is used to validate that the safety functions in a project can, when properly installed, implemented, and operated, achieve the Performance Level required, the PLr.

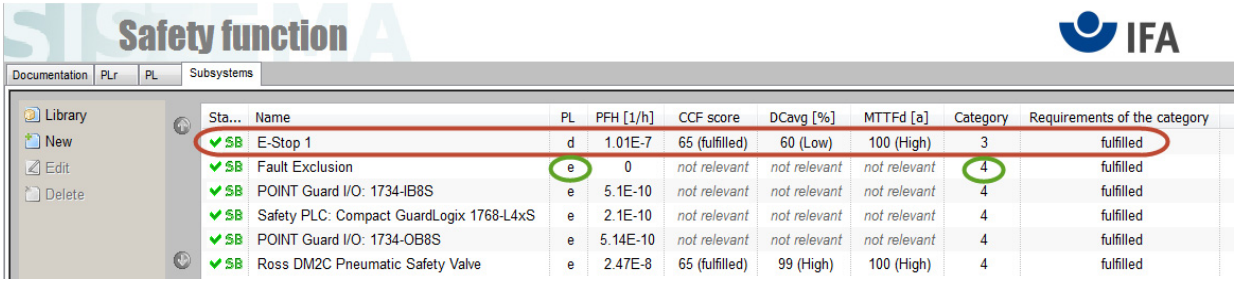
When modeled in SISTEMA software, each safety E-stop string is treated as an individual safety function and can be modeled as follows. This diagram shows one E-stop safety function.



The SISTEMA calculations confirm that the proposed safety functions are capable of achieving the required level of protection CAT. 3, PLd.



The SISTEMA results for the E-stop 1 safety function are shown in the graphic. All three E-stop safety functions are identical.



Sta...	Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
SB	E-Stop 1	d	1.01E-7	65 (fulfilled)	60 (Low)	100 (High)	3	fulfilled
SB	Fault Exclusion	e	0	*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 1768-L4xS	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	Ross DM2C Pneumatic Safety Valve	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled

The Fault Exclusion (green) had no effect on the calculations. The CAT. 3, PL d, and DCavg 60% were manually entered to reflect the effect of the E-stops wired in series.

Because the E-stops are electromechanical devices, certain data must be considered, including the following:

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

The functional safety evaluations of electromechanical devices include the following:

- How frequently they are operated (MTTFd)
- Whether they are effectively monitored for faults (DCavg)
- Whether they are properly specified and installed (CCF)

SISTEMA calculates the MTTFd by using B10d data provided in the Rockwell Automation® SISTEMA library for the E-stops along with the estimated frequency of use, entered during the creation of the SISTEMA project. This example presumes that the E-stops are operated or tested at least once a month, for a total of 12 times a year.

The DCavg (60%) for the E-stops was entered manually to take into account that the E-stops are connected in series. Masking, due to series connection, reduces the ability of the system to detect faults, the Diagnostic Coverage.

Additionally, because the E-stops are electromechanical devices where one mechanical actuator controls two channels, fault exclusion must be considered when calculating the safety ratings. A fault exclusion subsystem is added to SISTEMA to reflect this fact.

EN-ISO 13849-2:2012, Annex D, allows a fault exclusion for mechanical aspects (in this case one actuator operating two channels) of emergency stop devices in accordance with IEC 60947-5-5. The estimated maximum number of E-stop operations (12 per year) is not excessive. Thus the fault exclusion itself must have no effect on the category or performance level that is achieved by the E-stop safety functions, yet must be included. When added to the SISTEMA project, the category and performance level of the fault exclusion subsystem were manually entered as Category 4 and Performance Level e, the highest levels of the other subsystems in the safety function, so that it would have no effect on the overall calculation.

The measures against Common Cause Failure (CCF) are calculated using the scoring process outlined in Annex F of ISO 13849-1. For the purpose of the PL calculation, the required score of 65, that is needed to fulfill the CCF requirement, is entered directly. The complete CCF scoring process must be done when implementing an actual safety system.

The functional safety data for the DM^{2}C Safety solenoid valve is taken from the product literature and is entered directly into the DM^{2}C subsystem of the SISTEMA safety functions:

- PL = PLe
- PFH = 7.7E-9
- CAT. = CAT. 4

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.

Validation of software development is the process in which similar methodologies and techniques that are used in hardware development are deployed. Faults that are created through poor software development processes and procedures are systemic in nature rather than faults associated with hardware, which are considered as random.

Before validating the GuardLogix safety system, confirm that the safety system and safety application program have been designed in accordance with the GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093, and the GuardLogix Safety Application Instruction Set Safety Reference Manual, publication 1756-RM095.

Verification and Validation Checklist

General Machinery Information		
Machine Name/Model Number		
Machine Serial Number		
Customer Name		
Test Date		
Tester Name		
Schematic Drawing Number		
Controller Name		
Safety Signature ID		
Safety Network Number		
RSLogix 5000 Software Version		
Safety Control System Modules	**GuardLogix Modules**	**Firmware Revision**
GuardLogix Safety Controller	1768-L43S	
CompactLogix Ethernet Bridge	1768-ENBT	
POINT I/O™ Ethernet Adapter	1734-AENT	
POINT I/O Input Modules	1734-IB8S	
POINT I/O Output Modules	1734-OB8S	

Safety System Wiring and Configuration Verification			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
1	Verify that the safety system has been designed in accordance with the controller Safety Reference Manual listed under Additional Resources.		
2	Verify that the safety application program has been designed in accordance with the GuardLogix Safety Application Instruction Set Safety Reference Manual, publication 1756-RM095.		
3	Visually inspect the safety system network and I/O to verify that it is wired as documented in the schematics.		
4	Visually inspect the safety application program to verify that the safety system network and I/O module configuration is configured as documented.		
5	Visually inspect the safety application program to verify that suitable safety-certified instructions are used. The logic must be readable, understandable, and testable with the aid of clear comments.		
6	Verify that all input devices are qualified by cycling their respective actuators. Monitor the status in the Controller Tags dialog box.		
7	Verify that all output devices are qualified by cycling their respective actuators. Monitor the status in the Controller Tags dialog box.		

Normal Operation Verification - The safety system responds properly to all normal Start, Stop, and Reset inputs.			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
1	Initiate a Start command. The pneumatic safety valve energizes for a normal machine run condition. Verify proper machine-status indication and safety application program indication.		
2	Initiate a Stop command. The pneumatic safety valve de-energizes for a normal machine Stop condition. Verify proper machine-status indication and safety application program indication.		

Verification and Validation Checklist

3	While the system continues to run, press any E-stop button. The pneumatic safety valve immediately de-energizes. Verify proper machine-status indication and safety application program indication. Repeat for all E-stops.		
4	Initiate a Reset command. The pneumatic safety valve remains de-energized.		
Validation of Safe Response to Abnormal Operation - The safety system responds properly to all foreseeable faults with corresponding diagnostics.			
Door-monitoring Input Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	While the system continues to run, remove the channel 1 wire from the safety I/O. The pneumatic safety valve de-energizes. Verify proper machine-status indication and safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and repeat for channel 2.		
2	While the system continues to run, short channel 1 of the safety I/O to 24V DC. The pneumatic safety valve de-energizes. Verify proper machine-status indication and safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and repeat for channel 2		
3	While the system continues to run, short channel 1 of the safety I/O to 0V DC. The pneumatic safety valve de-energizes. Verify proper machine-status indication and safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and repeat for channel 2.		
4	While the system continues to run, short channels 1 and 2 of the safety I/O. The pneumatic safety valve de-energizes. Verify proper machine-status indication and safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and 2 wiring.		
5	While the system continues to run, short channel 1 and 2 of the safety I/O. The pneumatic safety valve de-energizes. Verify proper machine-status indication and safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 wiring and repeat for channel 2.		
Validation of Safe Response to Abnormal Operation - The safety system responds properly to all foreseeable faults with corresponding diagnostics.			
GuardLogix Controller, Network Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	While the system continues to run, remove the Ethernet network connection between the safety I/O and the controller. The pneumatic safety valve de-energizes. Verify proper machine-status indication and I/O connection status in the safety application program.		
2	Restore the safety I/O module network connection and allow time to re-establish communication. Verify the connection status bit in the safety application program. Repeat for all safety I/O connections.		
3	While the system continues to run, switch the controller out of Run mode. The pneumatic safety valve de-energizes. Return the controller keyswitch back to Run mode. The pneumatic safety valve remains de-energized. Verify proper machine-status indication and safety application program indication.		
Validation of Safe Response to Abnormal Operation - The safety system responds properly to all foreseeable faults with corresponding diagnostics.			
Pneumatic Safety Valve Output Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
1	Initiate a Start command. The pneumatic safety valve energizes for a normal machine run condition. Verify proper machine-status indication and safety application program indication.		
2	While the system continues to run, remove the valve feedback from the safety I/O. The pneumatic safety valve remains energized. Initiate a Stop command and attempt a Reset command. The system does not restart or reset. Verify proper machine-status indication and safety application program indication. Restore feedback signal.		
3	While the system continues to run, short the valve feedback to the 24V DC. All contactors remain energized. Initiate a Stop command and attempt a Reset command. The system does not restart or reset. Verify proper machine-status indication and safety application program indication. Remove the short.		

Additional Resources

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

Resource	Description
Compact GuardLogix Controllers User Manual, publication 1768-UM002	Provides information on how to configure, operate, and maintain Compact GuardLogix controllers.
Point Guard I/O Safety Modules Installation User Manual, publication 1734-UM013	Provides information on how to install, configure, and operate POINT Guard I/O modules.
GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093	Contains detailed requirements for how to achieve and maintain safety ratings with the GuardLogix 5560 or 1768 Compact GuardLogix controller system.
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.
GuardLogix 5570 and Compact GuardLogix 5370 Controller Systems Safety Reference Manual, publication 1756-RM099	Describes the GuardLogix 5570 and Compact GuardLogix 5370 controller systems. Provides instructions on how to develop, operate, or maintain a GuardLogix controller-based safety system that uses the Studio 5000 Logix Designer application.
Safety Accelerator Toolkit Quick Start, publication IASIMP-QS005	Provides a step-by-step guide on how to use the design, programming, and diagnostic tools in the Safety Accelerator Toolkit.
ROSS Controls website, http://www.rosscontrols.com	Provides information about the products and services that are offered by ROSS Controls, along with details about the industries and applications in which the products are used. Also provides access to product support and literature
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines on how to install a Rockwell Automation industrial system.
Safety Products Catalog, publication S117-CA001 Website http://www.rockwellautomation.com/rockwellautomation/catalogs/overview.page	Provides information about Rockwell Automation safety products.
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

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.

For more information on Safety Function Capabilities, visit:

http://marketing.rockwellautomation.com/safety/en/safety_functions

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

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-AT128B-EN-P - July 2016
Supersedes Publication SAFETY-AT128A-EN-P - February 2014