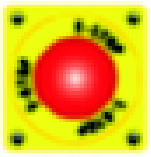
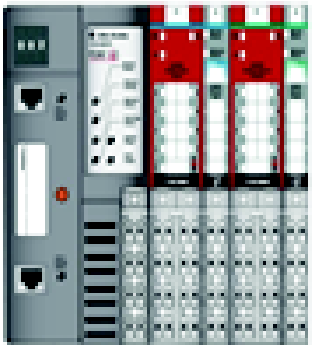
Application Technique





Safety Function: Pneumatic Safety Valves

Products: GuardLogix Controller, E-stop, Safety I/O Module, DM^2 Safety Valve
Safety Rating: CAT. 3, PLd to EN ISO 13849-1: 2008

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

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 PPE.

General Safety Information

Contact Rockwell Automation to find out 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 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 take into consideration safety distance calculations, which are not part of the scope of this document.

Table of Contents

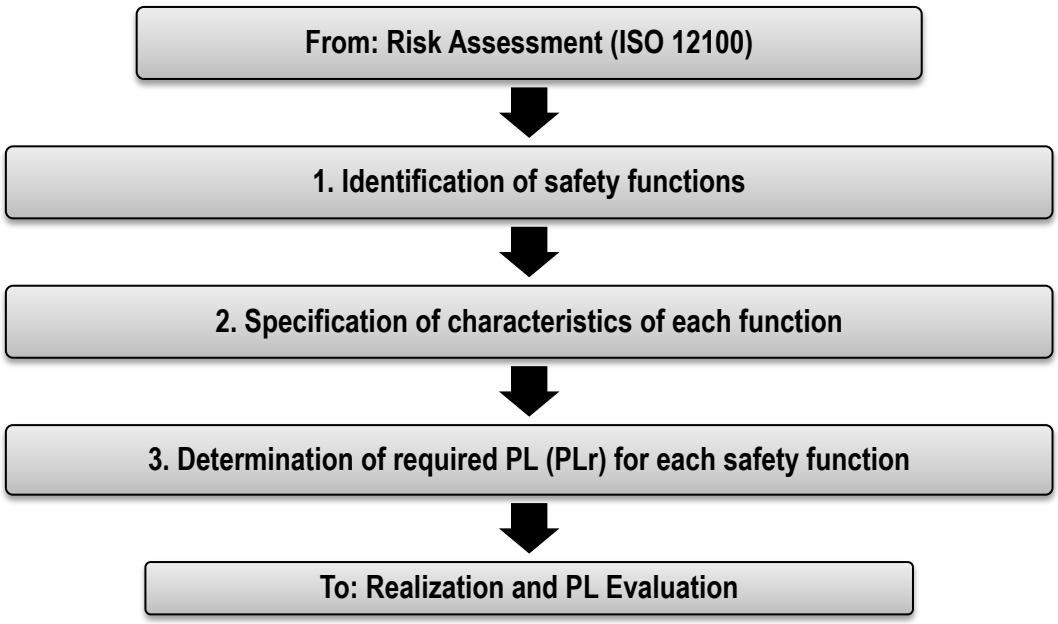
Introduction

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 safety valve from ROSS Controls.

This example uses a Compact GuardLogix controller, but is applicable to any GuardLogix controller. The SISTEMA software calculations 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 carried out 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 includes one safety function: the removal of power/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 safety valve. Upon resetting the E-stop button, the hazardous motion and power to the safety valve do not resume until a secondary action occurs (the Reset button is pressed and released). 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 EN ISO 13849-1 and control reliable operation per ANSI B11.19.

Functional Safety Description

Hazardous motion is interrupted or prevented by actuation of any the emergency stop push button (ES1, ES2, or ES3). Each E-stop is considered a separate safety function. The E-stop push buttons are connected in series to a pair of safety inputs of a safety input module (SI1). The 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 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 safety valve.

Bill of Material

This application uses these products.

Cat. No.	Description	Quantity
800FM-G611MX10	800F reset push button - metal, guarded, blue, R, metal latch mount, 1 N.O. contact, standard	1
800FM-MT44MX02	800F non-illuminated mushroom operators, twist-to-release, 40 mm, round metal (type 4/13, IP66), red, metal latch mount, 0 N.O. contacts, 2 N.C. contacts, standard, standard pack (quantity 1)	1
800F-15YSE112	800F legend plate, 60 mm round, universal: EMERGENCY STOP, yellow with black legend text, 22.5 mm opening	3
DM^2 Series	DM^2 series safety valve – contact ROSS Controls for 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	
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 installing and wiring, 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 short 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 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 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 safety valve that is controlled by a 1734-OB8S output module. A feedback circuit is wired through the N.O. contact and back to an input of the 1734-IB8S module to monitor the safety valve for proper operation. The safety valve cannot restart if the feedback circuit is not in the correct state.

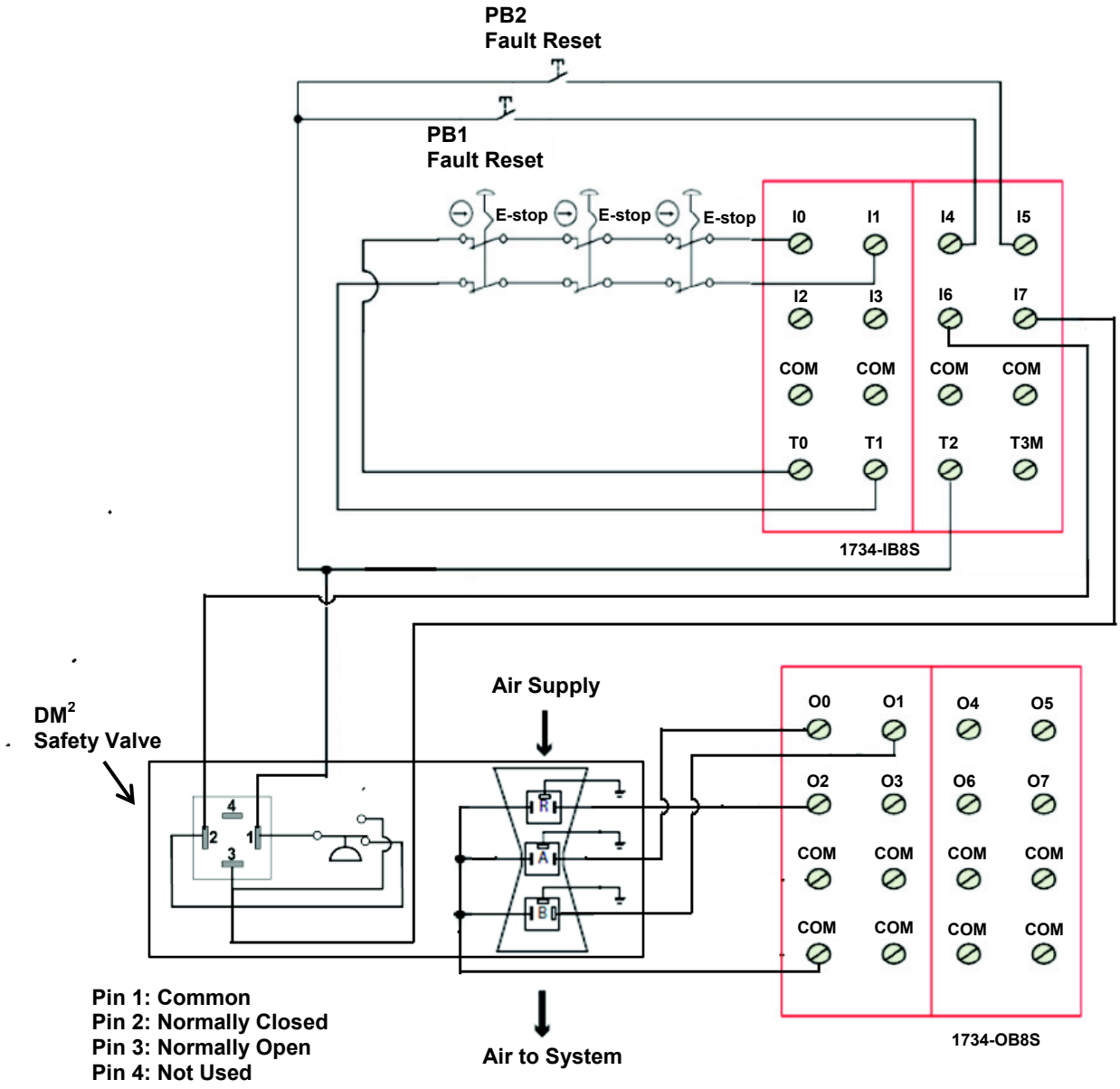
The maximum output current is 1 A for each output point of the 1734-OB8S module.

Primary power consumption for each solenoid is as follows:

- 15.8VA inrush
- 12.8VA holding on 50 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 safety valve Ready to Run N.O. and Fault Indicate N.C. contacts are all wired to the 1734-IB8S module in this example. This 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.

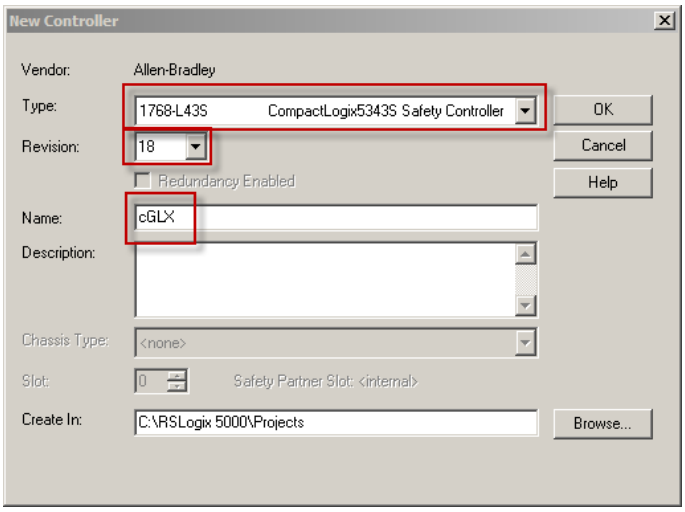
In the event of a fault, remove power from the pilot solenoids (A and B) momentarily, apply power to the Reset solenoid to return the valve to Return To Run state. Wait at least 250 ms after removing power from the reset solenoid before trying to re-energize the pilot solenoids.

Configuration

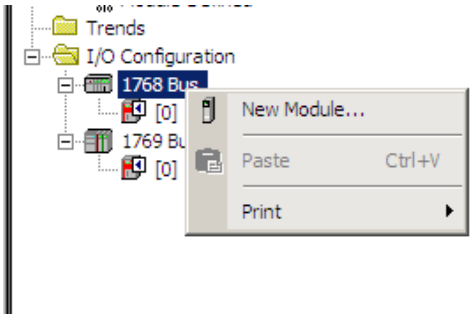
The Compact GuardLogix controller is configured by using RSLogix™ 5000 software, version 17 or later. First, you must create a new project and add the I/O modules, then configure the I/O modules for the correct input and output types. A detailed description of each step is beyond the scope of this document. Knowledge of the RSLogix programming environment is assumed.

Follow these steps.

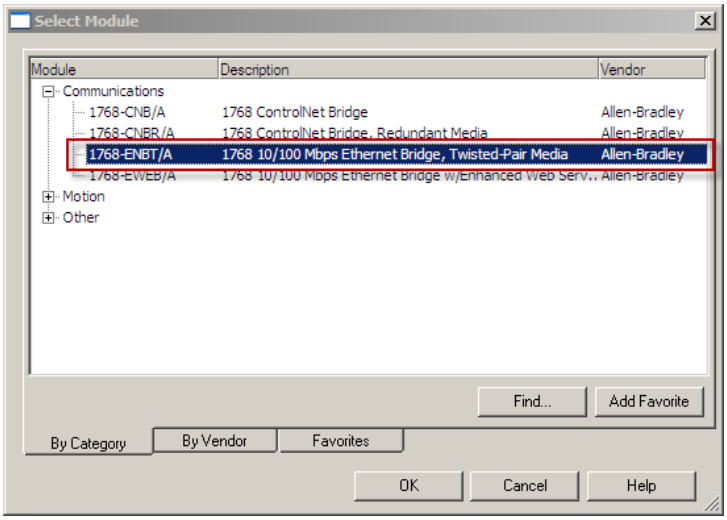
1. In RSLogix 5000 software, create a new project.
   a. Choose a controller.
   b. From the Type pull-down menu, choose 1768-L43S CompactLogix 5343S Safety Controller.
   c. From the Revision pull-down menu, choose the appropriate revision for the controller.
   d. In the Name box, type an appropriate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



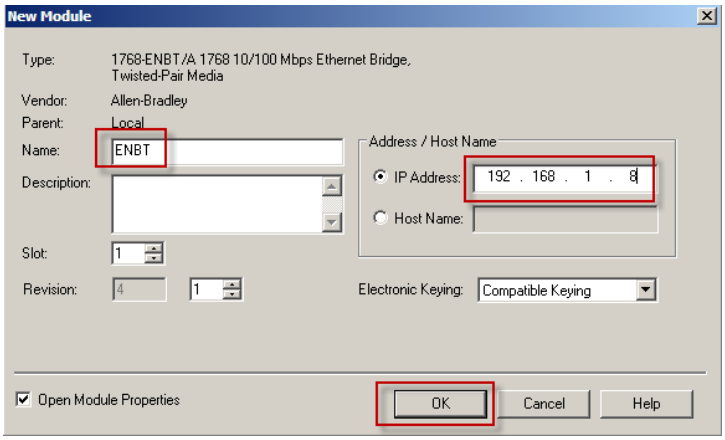
2. In the Controller Organizer, add the 1768-ENBT module to the 1768 bus.



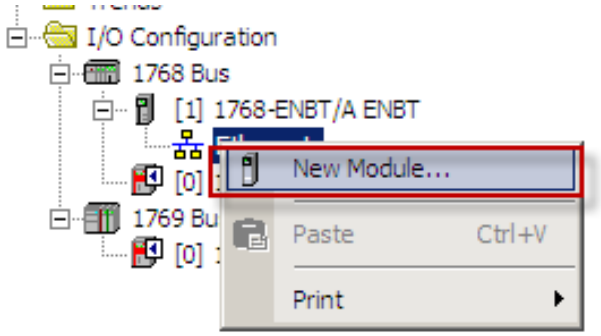
3. Select the 1768-ENBT module and click OK.



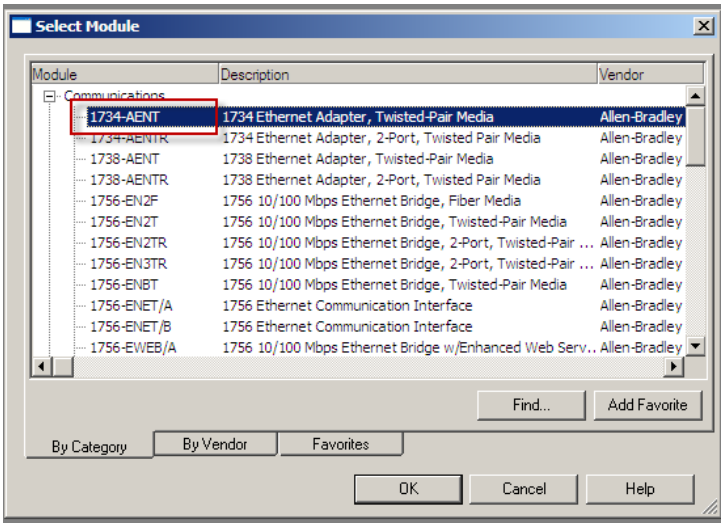
4. Name the module, type its IP address, and click OK.
We used 192.168.1.8 for this application example. Yours can be different.



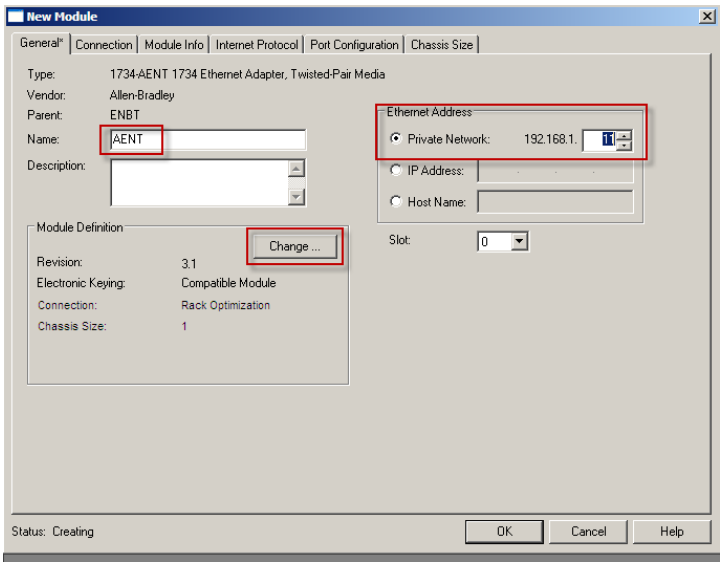
5. In the Controller Organizer, right-click 1768-ENBT module and choose New Module.



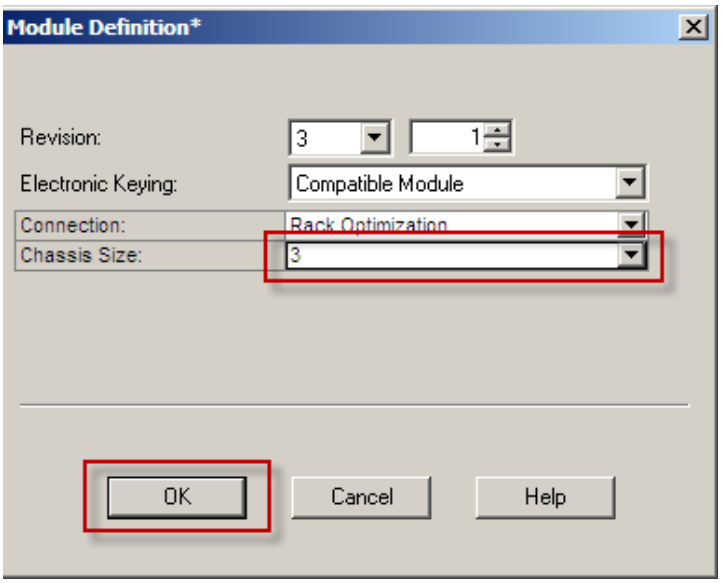
6. Select the 1734-AENT adapter and click OK.



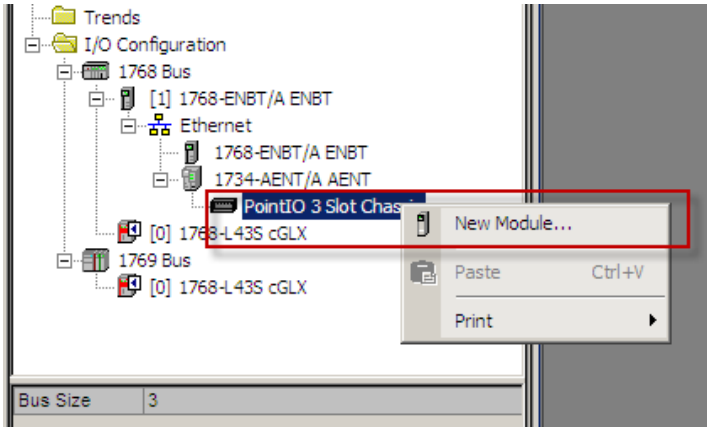
7. Name the module, type its IP address, and click OK.
   We used 192.168.1.11 for this application example. Yours may be different.
8. Click Change.



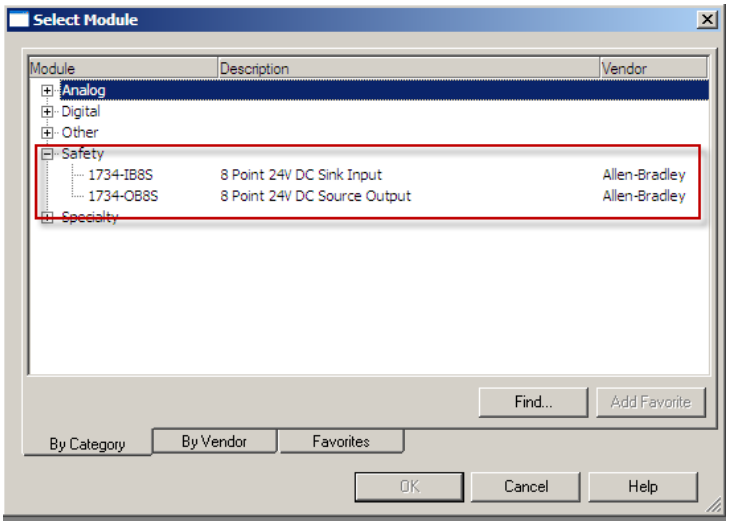
9. From the Chassis Size pull-down menu, choose 3 and click OK.
   Chassis size is the number of modules that are inserted in the chassis. The 1734-AENT adapter is considered to be in slot 0, so for one input and one output module, the chassis size is 3.



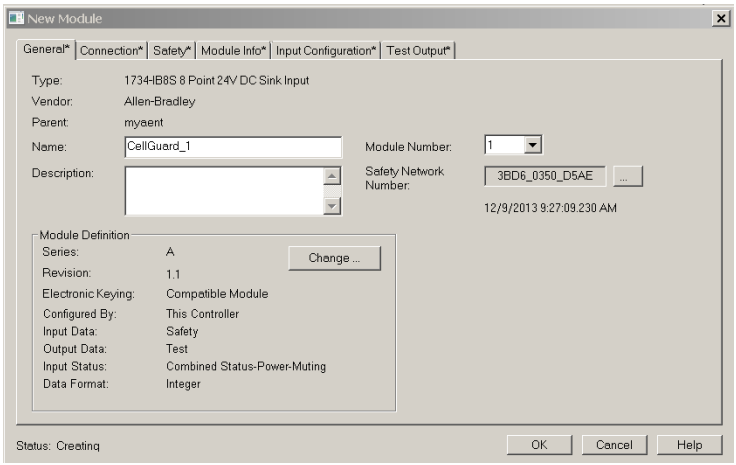
10. In the Controller Organizer, right-click the PointIO Slot Classis adapter and choose New Module.



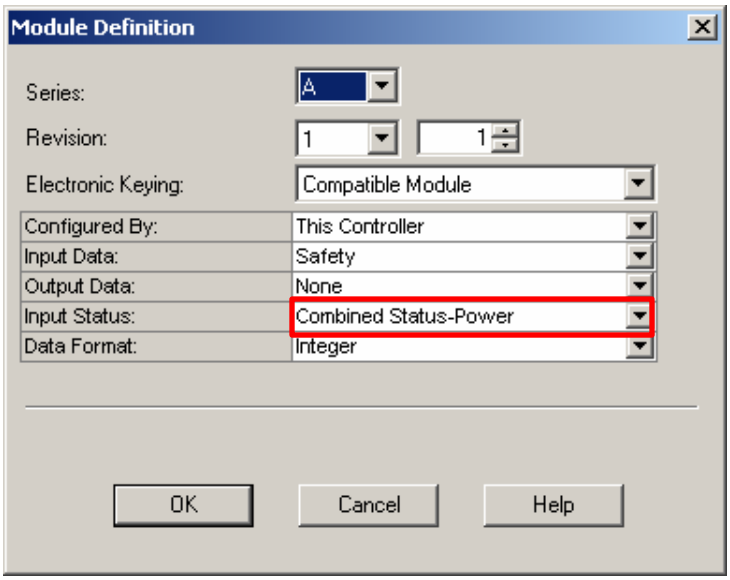
11. Expand Safety, select the 1734-IB8S module, and click OK.



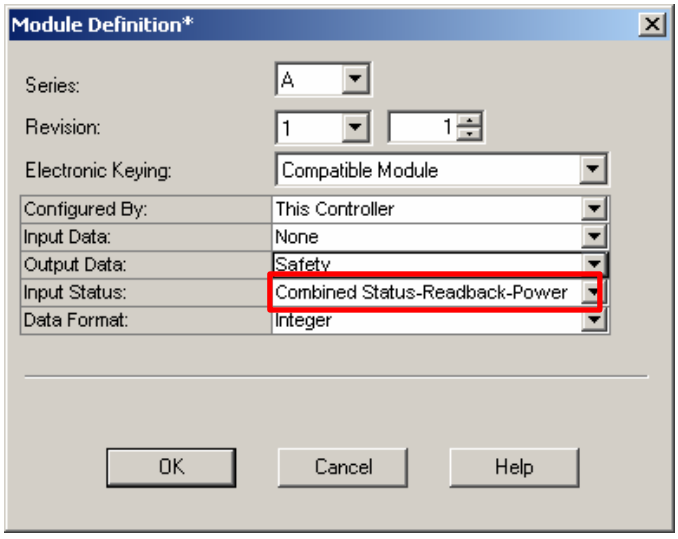
12. In the New Module dialog box, name the device CellGuard_1 and click Change.



13. When the Module Definition dialog box opens, change the Output Data to ‘None’, verify 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 saves one controller connection because we are using only the input connection.



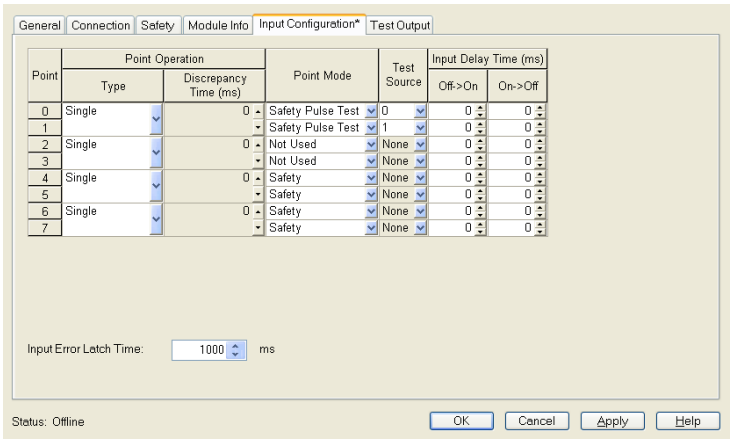
14. Close the Module Properties dialog box by clicking OK.
15. Repeat steps 10…14 to add the 1734-OB8S safety output module.
    a. Name the module OB8S.
    b. Choose slot 2.
    c. Set the Input Status to Combined Status-Readback-Power.



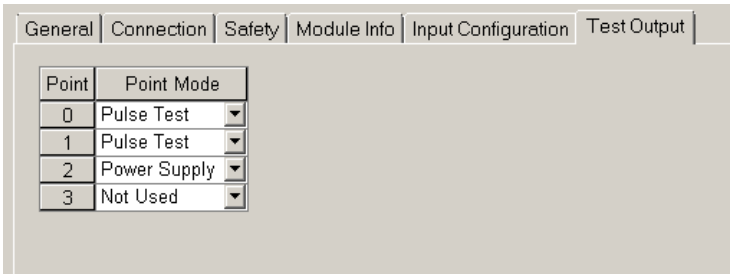
Configure the I/O Modules

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

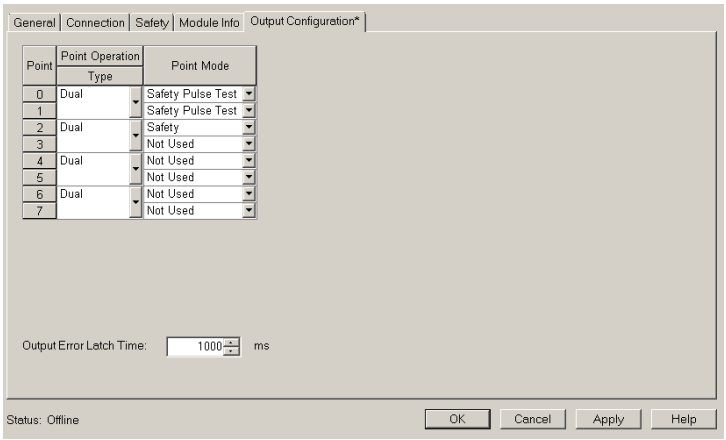
1. In the Controller Organizer, right-click the 1734-IB8S module and choose Properties.
2. Click Input Configuration and configure the module as shown.



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.

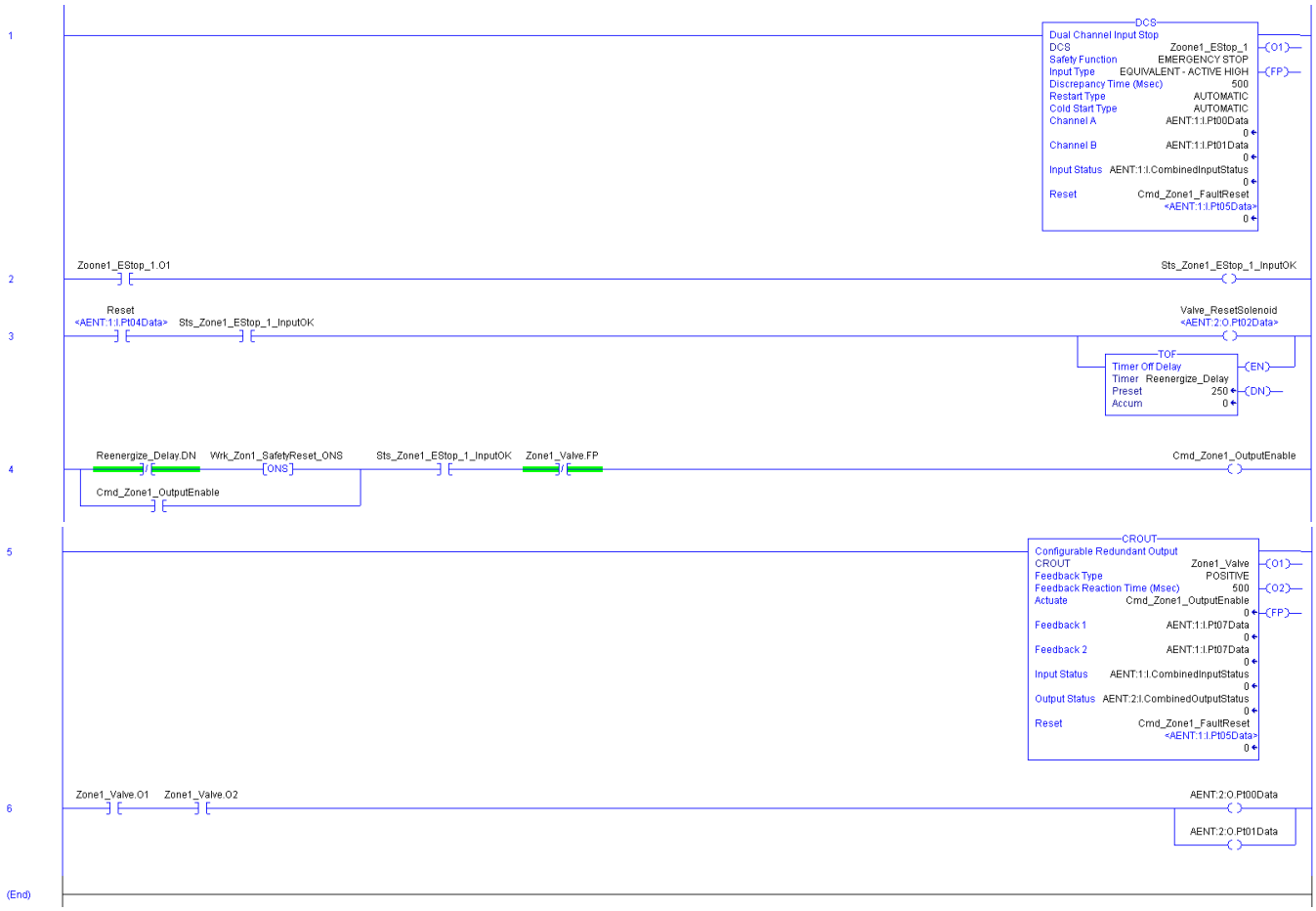
Programming

The Dual Channel Input Stop (DCS) instruction monitors dual-input safety devices whose main function is to stop a machine safely, for example, an E-stop, light curtain, or safety gate. This instruction can energize only the output 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 carried out. 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, providing anti-tiedown functionality for the circuit reset.

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

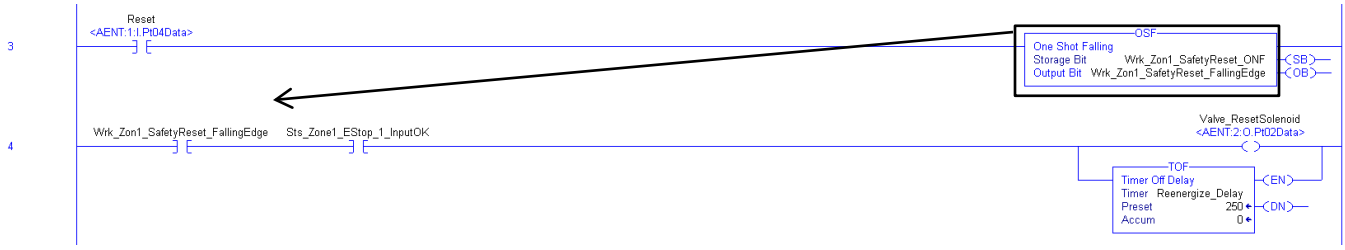


Falling Edge Reset

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 below.

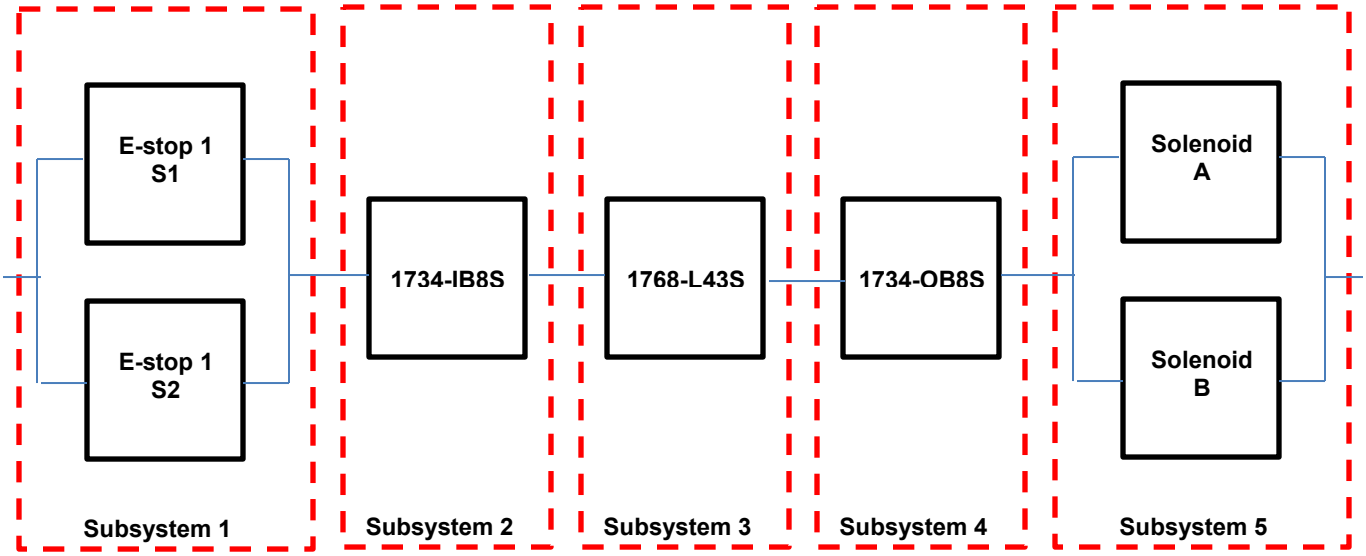


Calculation of the Performance Level

When configured correctly, the safety system can achieve the safety rating of Category 3, Performance Level d (CAT. 3, PLd) according to EN ISO13849-1: 2008.

PLr	d
PL	d
PFH [1/h]	1.26E-7

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 a single E-stop safety function.



Calculations are based on one operation of the E-stop per month, therefore, 12 operations of the safety valve per year.

E-stop Safety Function Subsystem 1

SB Estop 1	
PL	d
PFH [1/h]	1.01E-7
Cat.	3
MTTFd [...	100 (High)
DCavg [...	60 (Low)
CCF	65 (fulfilled)

E-stop Safety Function Subsystem 2

SB POINT Guard I/O: 1734-IB8S	
PL	e
PFH [1/h]	1.34E-10
Cat.	4
MTTFd [...	*not relevant*
DCavg [...	*not relevant*
CCF	*not relevant*

E-stop Safety Function Subsystem 3

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [...	*not relevant*
DCavg [...	*not relevant*
CCF	*not relevant*

E-stop Safety Function Subsystem 4

SB POINT Guard I/O: 1734-OB8S	
PL	e
PFH [1/h]	1.38E-10
Cat.	4
MTTFd [...	*not relevant*
DCavg [...	*not relevant*
CCF	*not relevant*

E-stop Safety Function Subsystem 5

SB ROSS DM2C BG certification to ISO 13849-1: 2006	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [...	100 (High)
DCavg [...	99 (High)
CCF	80 (fulfilled)

Because these are electro-mechanical devices, the safety data includes the following:

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

Electro-mechanical devices' functional safety evaluations include the following:

- How frequently they are operated
- Whether they are effectively monitored for faults
- Whether they are properly specified and installed

SISTEMA software calculates the MTTFd by using B10d data provided for the safety valves along with the estimated frequency of use, entered during the creation of the SISTEMA project.

The DCavg is reduced to 60% for E-stops because they are connected in series.

The measures against CCF are qualified by using the scoring process outlined in Annex F of ISO 13849-1. For the purpose of the PL calculation, the required score of 65 needed to fulfill the CCF requirement is considered to be met. The complete CCF scoring process must be done when implementing this example.

Verification and Validation Plan

Verification and validation play important roles in the avoidance of faults throughout the safety system design and development process. EN ISO 13849-2 sets the requirements for verification and validation. The standard calls for a documented plan to confirm all of the 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 EN 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 of the safety-related outputs respond appropriately to their corresponding safety-related inputs. The functional test includes normal operating conditions in addition to 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 created through poor software development processes and procedures are systemic in nature rather than faults associated with hardware, which are considered as random.

Prior to validating the GuardLogix Safety System, it is necessary to confirm that the safety system and safety application program have been designed in accordance with the GuardLogix System Safety Reference Manuals, publication 1756-RM093 (GuardLogix 5560 and Compact GuardLogix controllers) and 1756-RM099 (GuardLogix 5570 controllers), and the GuardLogix Application Instruction Safety Reference Manual, publication 1756-RM095.

E-stop Safety Function Verification and Validation Checklist

General Machinery Information		
Machine Name/Model Number		
Machine Serial Number		
Customer Name		
Test Date		
Tester Name(s)		
Schematic Drawing Number		
Controller Name		
Safety Signature ID		
Safety Network Number(s)		
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	

GuardLogix Safety System Configuration and Wiring Verification			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
	Verify that the safety system has been designed in accordance with the GuardLogix System Safety Reference Manual listed under Additional Resources.		
	Verify that the safety application program has been designed in accordance with the GuardLogix Application Instruction Safety Reference Manual listed under Additional Resources.		
	Visually inspect the safety system network and I/O to verify that it is wired as documented in the schematics.		
	Visually inspect the RSLogix 5000 program to verify that the safety system network and I/O module configuration is configured as documented.		
	Visually inspect the RSLogix 5000 application program to verify that suitable safety-certified instructions are used. The logic is readable, understandable, and testable with the aid of clear comments.		
	All input devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags dialog box.		
	All output devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags dialog box.		

E-stop Safety Function Verification and Validation Checklist (continued)

Normal Operation Verification The GuardLogix safety system properly responds to all normal Start, Stop, and Reset commands.			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
	Initiate a Start command. The safety valve energizes for a normal machine run condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	Initiate a Stop command. The safety valve de-energizes for a normal machine Stop condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	While the system is running, press any E-stop button. The safety valve immediately de-energizes. Verify proper machine-status indication and RSLogix 5000 safety application program indication. Repeat for all E-stops.		
	Initiate a Reset command. The safety valve remains de-energized.		
Abnormal Operation Validation **The GuardLogix safety system properly responds to all foreseeable faults with corresponding diagnostics.**			
Door Monitoring Input Tests			
Test Step	**Verification and Validation**	**Pass/Fail**	**Changes/Modifications**
	While the system is running, remove the channel 1 wire from the safety I/O. The safety valve de-energizes. Verify proper machine-status indication and RSLogix 5000 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.		
	While the system is running, short channel 1 of the safety I/O to 24V DC. The safety valve de-energizes. Verify proper machine-status indication and RSLogix 5000 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		
	While the system is running, short channel 1 of the safety I/O to 0V DC. The safety valve de-energizes. Verify proper machine-status indication and RSLogix 5000 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.		
	While the system is running, short channels 1 and 2 of the safety I/O. The safety valve de-energizes. Verify proper machine-status indication and RSLogix 5000 safety application program indication. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and 2 wiring.		
	While the system is running, short channel 1 and 2 of the safety I/O. The safety valve de-energizes. Verify proper machine-status indication and RSLogix 5000 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.		

E-stop Safety Function Verification and Validation Checklist (continued)

GuardLogix Controller and Network Tests			
Test Step	**Verification and Validation**	**Pass/Fail**	**Changes/Modifications**
	While the system is running, remove the Ethernet network connection between the safety I/O and the controller. The safety valve de-energizes. Verify proper machine-status indication and I/O connection status in the RSLogix 5000 safety application program.		
	Restore the safety I/O module network connection and allow time to re-establish communication. Verify the connection status bit in the RSLogix 5000 safety application program. Repeat for all safety I/O connections.		
	While the system is running, switch the controller out of Run mode. The safety valve de-energizes. Return the controller keyswitch back to Run mode. The safety valve remains de-energized. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
Safety Valve Output Tests			
Test Step	**Verification and Validation**	**Pass/Fail**	**Changes/Modifications**
	Initiate a Start command. The safety valve energizes for a normal machine run condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	While the system is running, remove the valve feedback from the safety I/O. The 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 RSLogix 5000 safety application program indication. Restore feedback signal.		
	While the system is running, 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 RSLogix 5000 safety application program indication. Remove the short.		

Additional Resources

These publications contain additional information concerning related products from Rockwell Automation.

Resource	Description
Compact GuardLogix Controllers User Manual, publication 1768-UM002	Provides information on configuring, operating, and maintain Compact GuardLogix controllers
Point Guard I/O Safety Modules Installation and User Manual, publication 1734-UM013	Provides information on installing, configuring, and operating POINT Guard I/O modules
GuardLogix Controller Systems Safety Reference Manual, Publication 1756-RM093	Contains detailed requirements for achieving and maintaining safety ratings with the GuardLogix controller system
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides detailed information on the GuardLogix Safety Application Instruction Set.
Safety Accelerator Toolkit for GuardLogix Systems Quick Start Guide, publication IASIMP-QS005	Provides a step-by-step guide to using the design, programming, and diagnostic tools in the Safety Accelerator Toolkit.
Safety Products Catalog, publication S117-CA001	Provides an overview of products, product specifications, and application examples.

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.

For more information on
Safety Function Capabilities, visit:

discover.rockwellautomation.com/safety

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-AT128A-EN-P – February 2014