Safety Function: Single-beam Area Access Control (AAC)

Products: Single-beam Area Access Control Sensors, GuardLogix Controllers
Safety Rating: CAT. 4, PLe 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 Personal Protective Equipment (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 function application technique explains how to wire, configure, and program a Compact GuardLogix® controller and POINT Guard I/O™ module to monitor a single-beam area access control sensor. If a demand is placed on the single-beam sensor or a fault is detected in the monitoring circuit, the GuardLogix controller de-energizes the final control devices, in this case, a redundant pair of 100S contactors.

This example uses a Compact GuardLogix controller, but is applicable to any GuardLogix controller. This example uses a single-beam area access control sensor, with the pulse-train output from the POINT Guard I/O module, for monitoring and detection of fault. The SISTEMA Software PL Calculation Tool calculations shown later in this document must be re-calculated 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.

From: Risk Assessment (ISO 12100)

1. Identification of safety functions

2. Specification of characteristics of each function

3. Determination of required PL (PLr) for each safety function

To: Realization and PL Evaluation
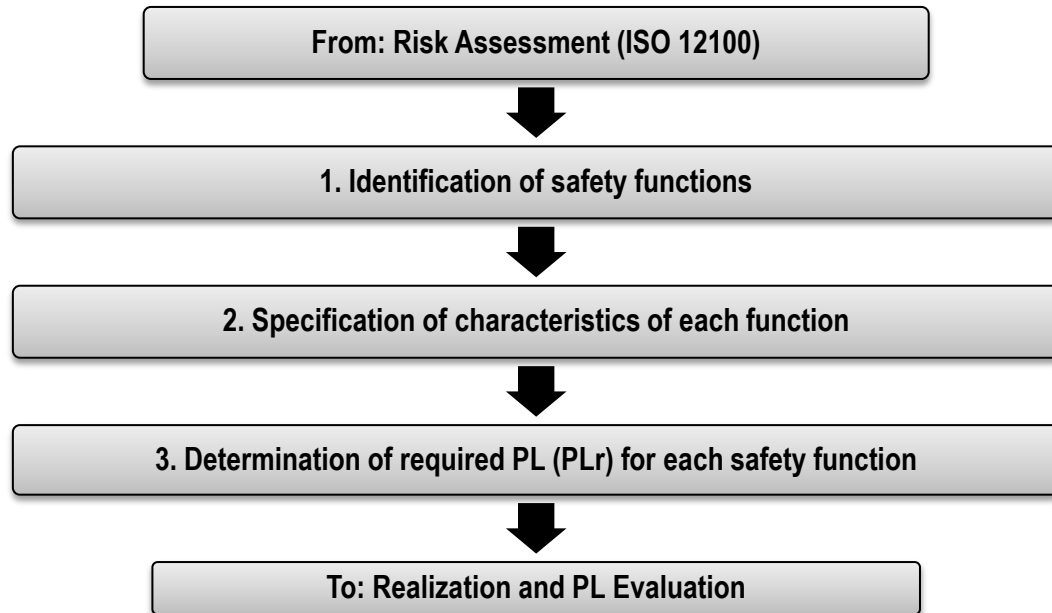
Single-beam Area Access Control Sensor Safety Function

The safety system described in this application has one safety function: safety-related stop by actuation of the single-beam area access control sensor. This system executes a Stop Category 0 stop. Power is immediately removed and motion coasts to a stop.

Safety Function Requirements

The interruption of the single-beam area access control sensor stops and prevents hazardous motion by removing power to the motor. When the sensor is reset, the motor does not resume until a secondary action occurs—the Reset button is pressed and released. A fault at the sensor wiring terminal or safety controller is detected before the next safety demand. The safe distance location of the sensor must be established such that hazardous motion must be stopped before the user can reach the hazard. This distance is called the Safety Distance and is addressed later in this application technique. The safety function in this example is capable of connecting and interrupting power to motors rated up to 9 A, 600V AC. 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

An interruption of the single beam from the transmitter is detected by the receiver and motion is stopped. Hazardous motion is prevented from restarting while the beam is interrupted.

Bill of Material

This application uses these products.

Cat. No.	Description	Quantity
1585J-M4TBJM-2	1585 Ethernet cables, 4 conductors, RJ45, straight male, standard, RJ45, straight male, teal robotic TPE, UL CMB, CMX, CUL, CMG, standard TIA 568-B	2
1783-US05T	Stratix 2000™ switch, unmanaged, 5 copper ports	1
1768-ENBT	EtherNet/IP bridge module	1
1768-L43S	CompactLogix™ L43 safety 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	EtherNet/IP twisted pair media I/O adapter	1
1734-IB8S	POINT Guard I/O safety module – 8-point input module (compatible with terminal bases with 8 terminations)	1
1734-OB8S	POINT Guard I/O safety module - 8 safety sourcing output module (compatible with terminal bases with 8 terminations)	1
1734-TBS	Module bases with removable IEC spring terminals (quantity 10)	4
1794-PS13	85…264V AC to 24V DC 1.3 A power supply	1
440L-T4F2070-Q	Single-beam sensor, 0...70 m range, terminal chamber with cable gland (PG13.5 thread)	1
440L-R4F0020-Q	Single-beam sensor, 0.5...20 m range, 24V DC, terminal chamber with cable gland (PG13.5 thread)	1
440L-AMIRR2	440L-AMIRR2, glass corner mirror, 45° angle 0...30 m	2
100S-C09ZJ23C	MCS 100S-C safety contactor, 9 A, 24V DC	2
800FM-G611MX10	800F push button - metal, guarded, blue, R, metal latch mount, 1 N.O. contact, 0 N.C. contacts, standard, standard pack (quantity 1)	1

Setup and Wiring

For detailed information on installing and wiring, refer to the product manuals listed in the Additional Resources.

System Overview

The 1734-IB8S input module monitors the inputs from the single-beam area access control sensor. The sensor provides two N.C. outputs, which open when an object interrupts the sensor's field of view. These two N.C. contacts are monitored by test pulses (T0 and T1) provided by the input module, which are configured to test the circuit of I0 and I1. These test-pulses are the source of the 24V DC for the circuit. By periodically dropping the 24V DC to 0V DC, it is possible to detect cross-channel faults, shorts to an external 24V DC, and shorts to 0V DC. These faults and shorts are seen as an open circuit by the input and are detected by either the hardware, if configured to detect discrepancy errors, or by the appropriate safety function block in the application code.

Upon detection of an intrusion of the sensor, the pair of 100S safety contractors (K1 and K2) are de-energized. The contactors are controlled by a 1734-OBS output module and a wired-in series. The contactors are tested on start-up for faults. The start-up test is accomplished by using a Configurable Redundant Output (CROUT) instruction to monitor the feedback circuit into input 7 (I7) before the contactors are energized. These de-energized contactors remove power to the motor, causing the motor to coast to a stop (Stop category 0). The contactors are re-energized when the sensor blockage is removed, the sensor resumes its normal state, and the Reset button is pressed and released.

The system is designed so that no single fault results in the safety system failing to perform its safety function. A single fault is detected before the next demand on the safety system. The system cannot be reset until the fault is corrected.

The Reset button and the contactor feedback circuit are wired to the input module. This is not required for functional safety. The Reset button can be wired to a standard input module.

Installation

Refer to the installation instruction and user manuals, listed in the Additional Resources, for guidance on installing and maintaining the different parts of this system.

A single-beam area access control sensor provides no physical barrier between personnel and the hazardous motion. The sensor must be installed at a sufficient distance from the hazardous motion to make sure that an operator putting a hand through the beam cannot reach the hazard before hazardous motion has stopped. This distance is referred to as the Safety Distance.

Safe Distance Calculation

The Safety Distance (Ds) required varies from installation to installation and, therefore, must be calculated for each specific application.

In this application technique, the formula from EN ISO 13855 is used.

Formula: S = (K x T) + C

Symbol	Definition
S	Minimum distance, in millimeters (mm)
K	Parameter, in millimeters per second (mm/s), derived from data on approach speeds of the body or parts of the body.
T	Overall stopping performance in seconds
C	Intrusion distance in millimeters (mm)

In this example, stopping time (T) is a summation of the following.

Variable Value

Single-beam area access control delay time = 22 ms (from product documentation)

1734-IB8S delay = 16 ms (from documentation)

Input Module Connection delay[1]

Safety Controller delay[2]
- Safety Task Watchdog
- Safety Task period

Output Module Connection Delay[3]

1734-OB8S delay = 6 ms (from product documentation)

Contactor response time = 15 ms (from product documentation)

Actual Machine stop time = assume 900 ms for this example

[1] The Input Module connection delay defaults to 4 x requested packet interval (RPI).
   If we assume a RPI of 10 ms, the maximum delay = 40 ms.

[2] The safety controller delay is a combination of the safety task period plus the safety task watchdog. The watchdog accounts for the possibility that the safety code runs right up to, but does not trip the watchdog. The safety task period accounts for the possibility that the asynchronous scan just ended when the input changed state. For this example, the following assumptions were made:
- Safety Task Period = 10 ms
- Safety Task Watchdog = 5 ms
- Therefore the T in this example is 1029 ms

[3] The Output Module connection delay defaults to 3 x RPI.
   If we assume a RPI of 10 ms, the maximum delay = 30 ms.

The worst case reaction time can be calculated by assuming there is only a single fault in the control system. This means that only the higher of the two connection delay values shown above needs to be included in the Time calculation. For this example, 40 ms is used and the 30 ms is excluded. To account for multiple faults occurring at the same time, use both values in the calculation.

In this application technique example, the values are the following.

K	1600 mm/s
T	1029 ms
C	850 mm (with reference to the multi-beam formula)
	S = 1600 x 1.029 + 850 = 2496.4 **Conclusion:** The single-beam area access control sensor must not be mounted closer than 2496.4 mm (98.3 in.) from the hazardous motion being guarded against.

The above calculation is based on the following mounting consideration, with two separate beams, deduced from the risk assessment for reduction of the risk.

T = Transmitter
R = Receiver
M = Mirror
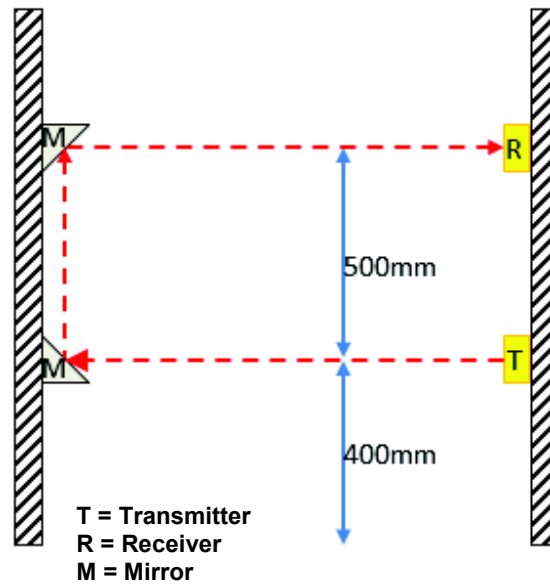
With reference to the EN ISO 13855: 2010, Appendix E standard, for two-beam applications, the mounting heights are 400 mm and 900 mm from the ground or panel level, which correspond to adequate risk reduction and application practice.

Thus, in applying the multiple separated beam, the formula: S = 1600 * T + 850 mm is used.

According to EN ISO 13855:2010, Appendix E, the two-beam application of the lowest height of 400 mm can be used only when the risk assessment allows.

Electrical Schematic

Input Circuit
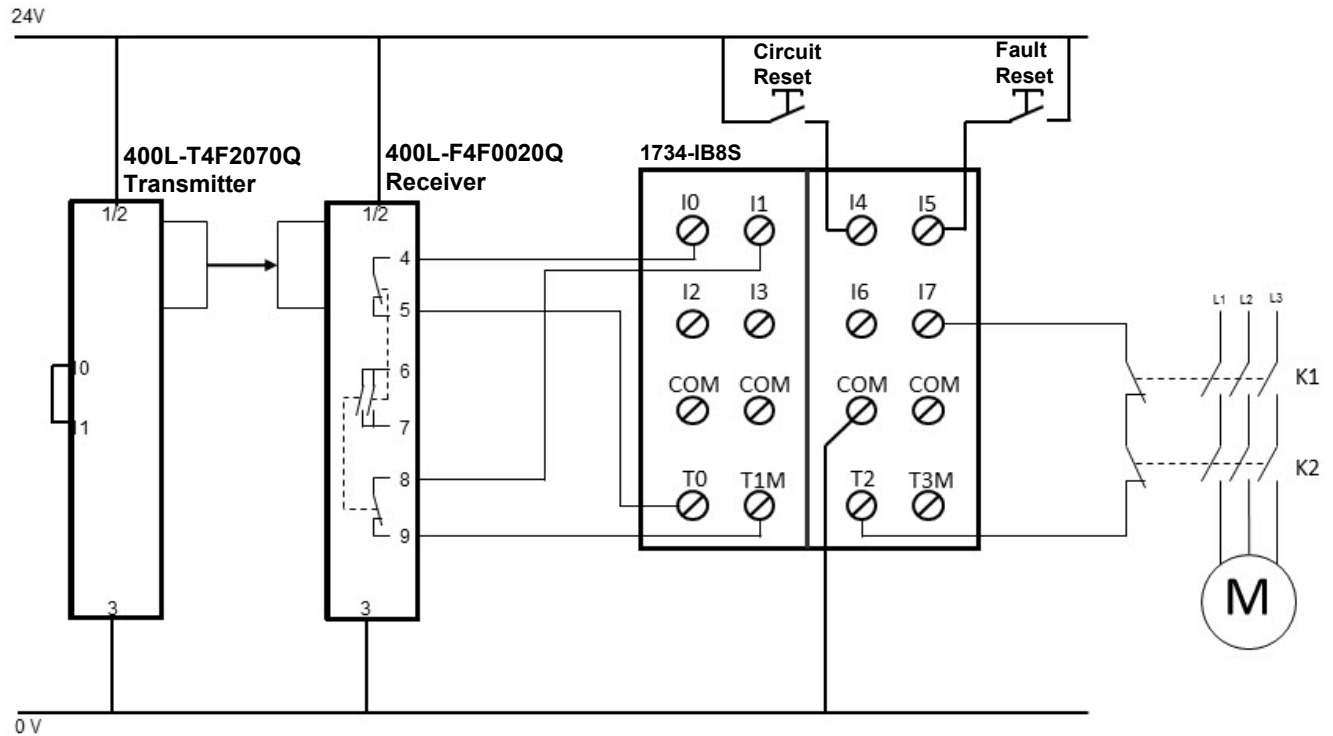
Output Circuit
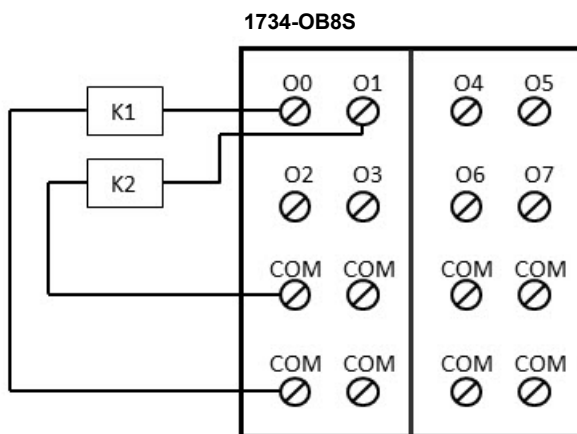
K1 and K2 are the safety contactors.

Configuration

The 440L single-beam area access control sensor needs no settings; only alignment of the transmitter and receiver is necessary.

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.

Configure the Controller and Add I/O Modules

1. In RSLogix 5000 software, create a new project.

2. Choose a controller.

   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.
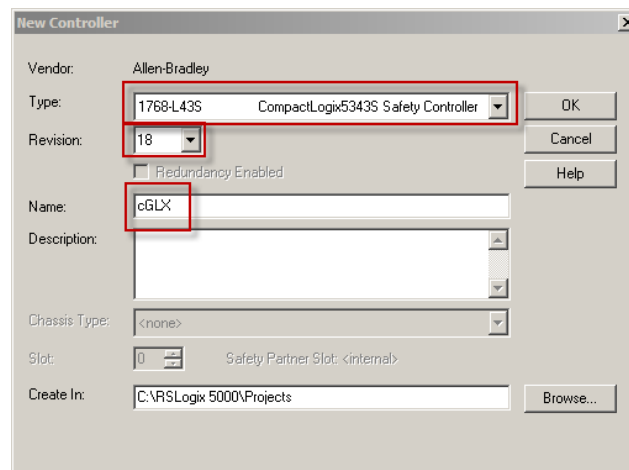
3. In the Controller Organizer, right-click 1768 Bus and choose New Module.
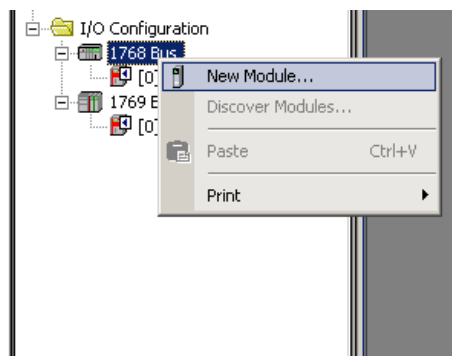
4. Select the 1768-ENBT module and click OK.
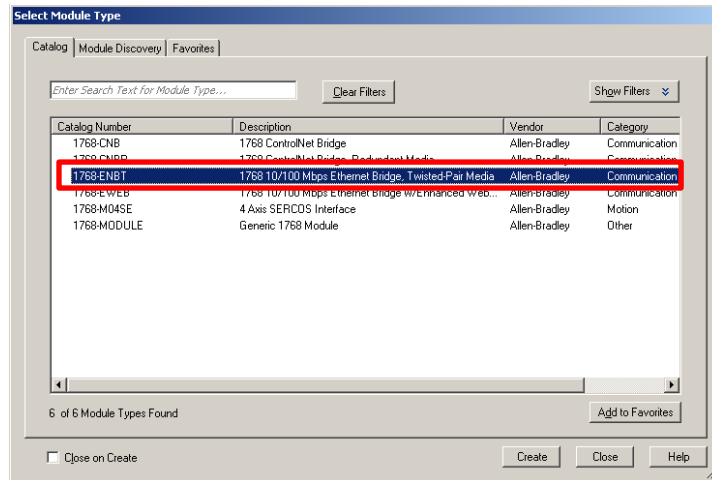
5. Name the module, type its IP address, and click OK.

    For this application example, we used 192.168.1.8; however, your IP address can be different.
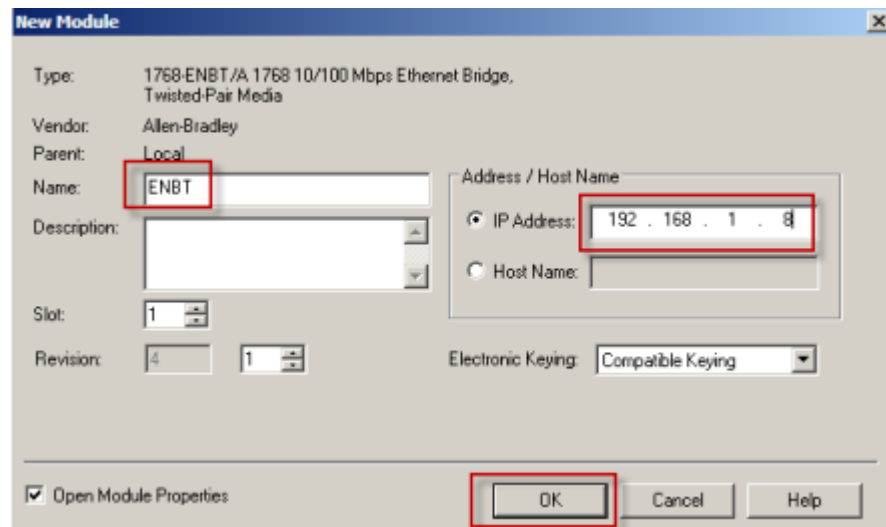
6. In the Controller Organizer, right-click the Ethernet network and choose New Module.
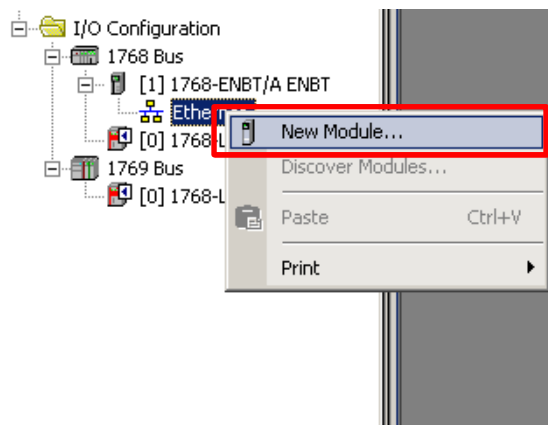
7. Select the 1734-AENT adapter and click OK.
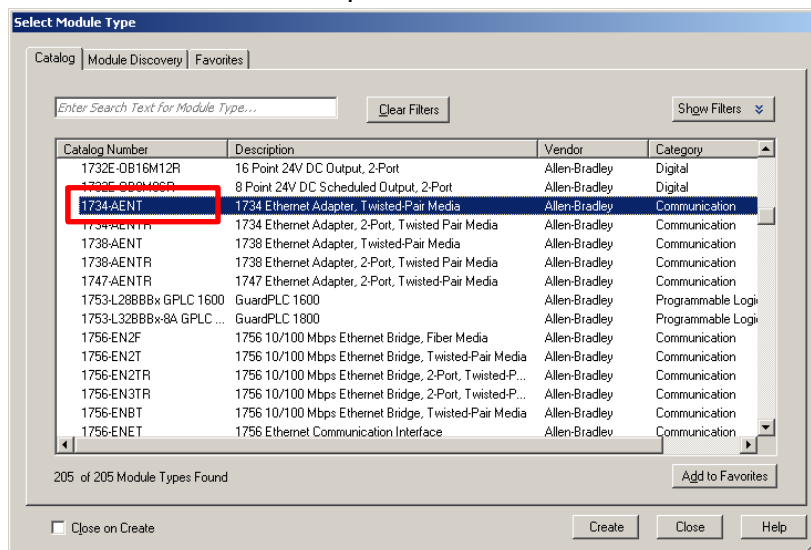
8. Name the module and type its Ethernet address.

    For this application example, we used 192.168.1.11; however, your IP address can be different.
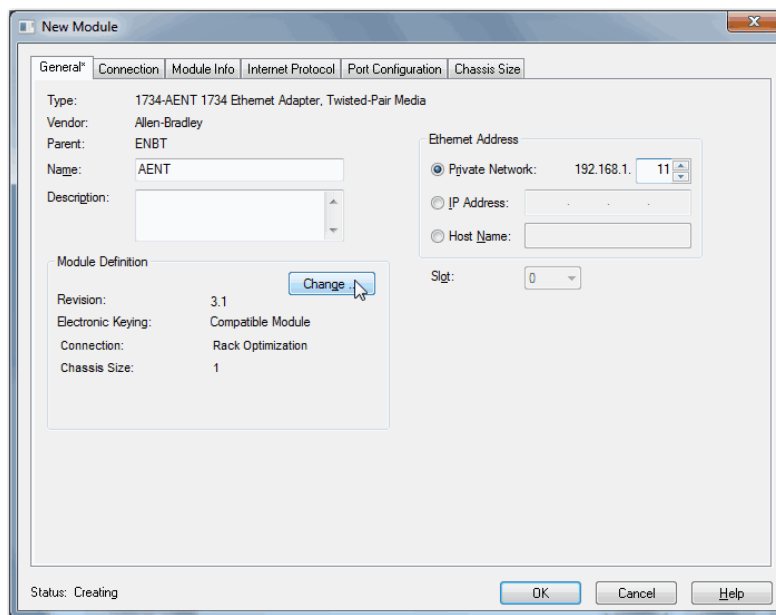
9. Click Change.

    The Module Definition dialog box appears.

10. From the Chassis Size pull-down menu, choose 3.

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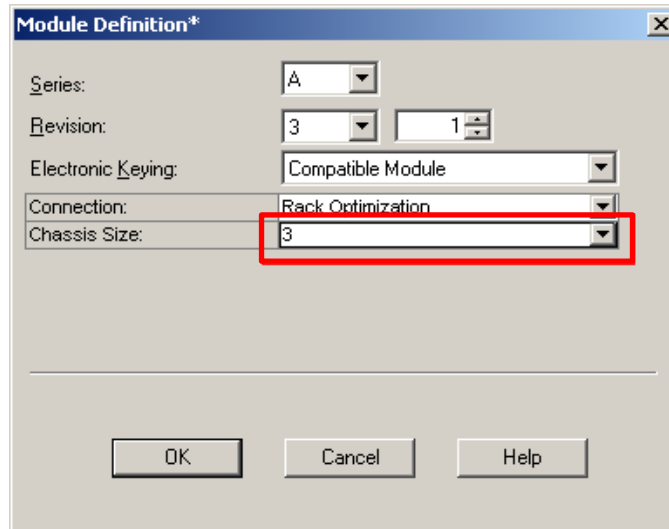
11. Click OK.

The confirmation screen is displayed.
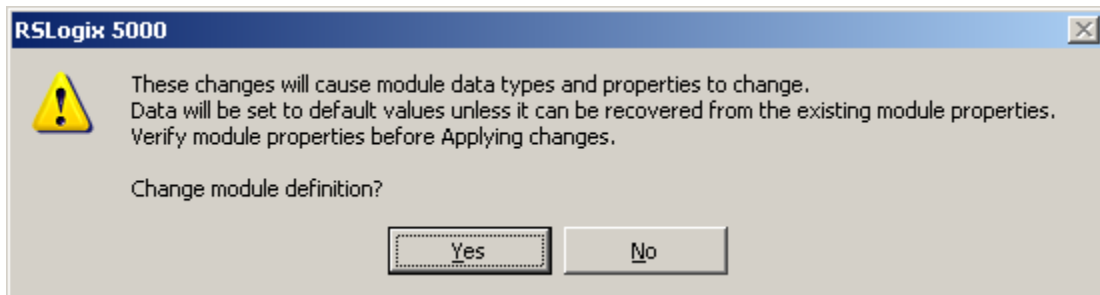
12. Click Yes to accept the changes.

13. In the Controller Organizer, right-click the PointIO 3 Slot Chassis and choose New Module.
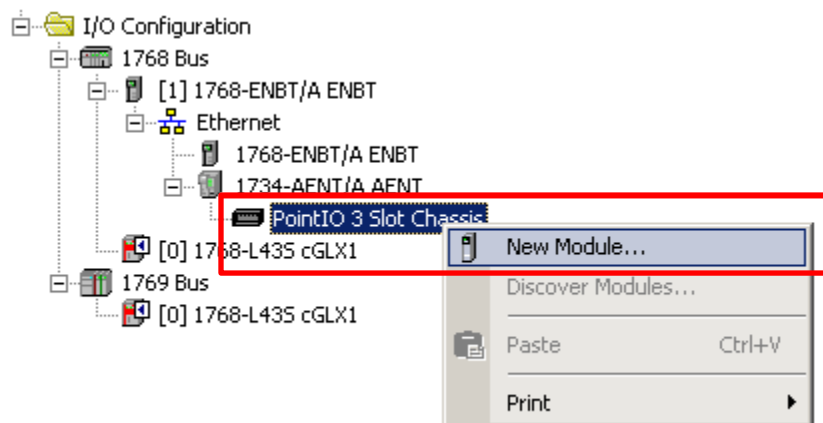
14. Expand Safety, select the 1734-IB8S module, and click OK.
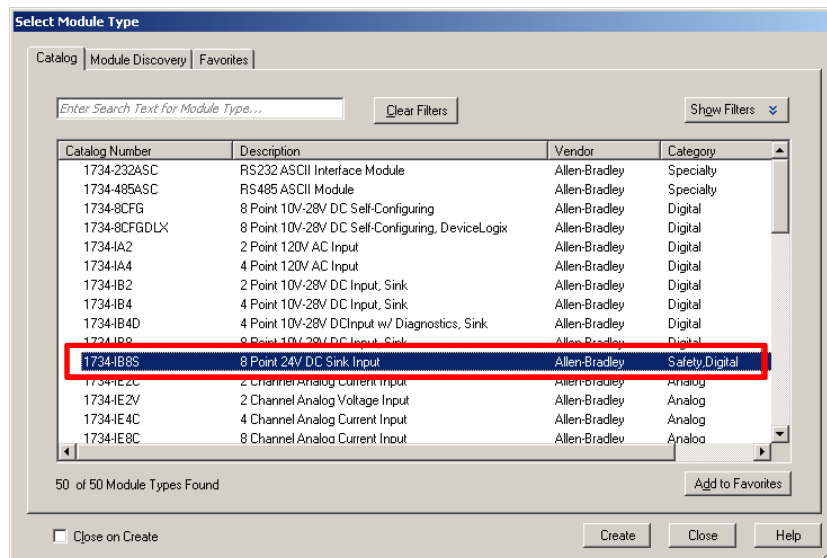
15. In the New Module dialog box, name the device IB8S and click Change.
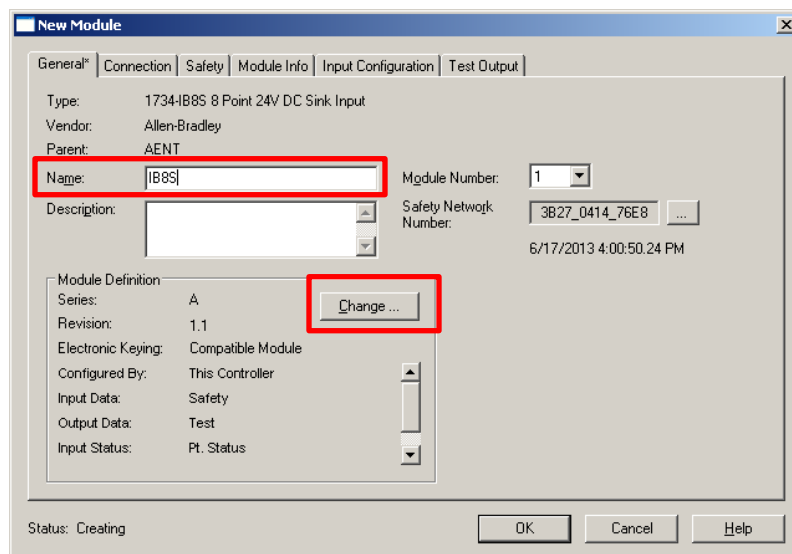
The Module Definition dialog box appears.

16. From the Output Data pull-down menu, choose None.

17. Verify that the Input Status is set to Combined Status-Power and click OK.

Setting the output data to None means the Test Outputs cannot be used as standard outputs. This saves one controller connection because we are using only the input connection.
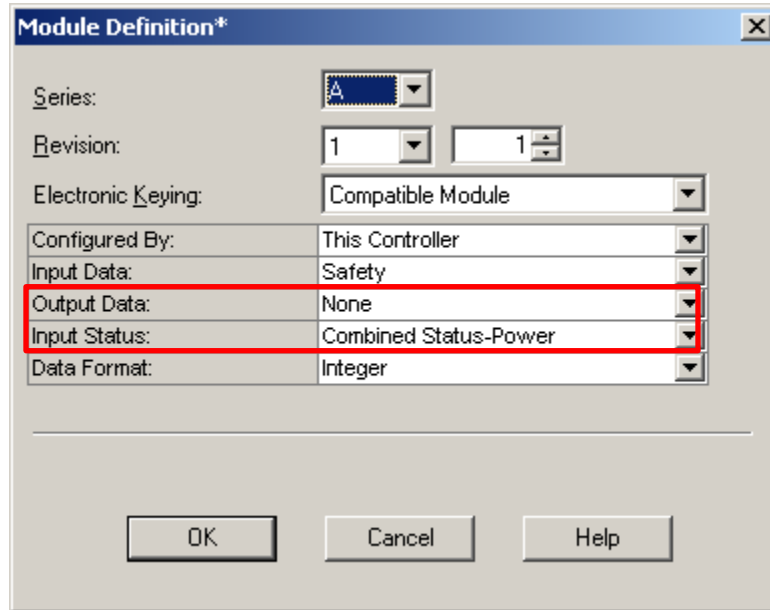
18. Repeat steps 13…17 to add the 1734-OB8S safety output module with these exceptions:

- Name the module OB8S

- Set the module to slot 2

- Set the Input Status to Combined Status-Feedback-Power

Configure the I/O Modules

1. In the Controller Organizer, right-click the 1734-IB8S module and choose Properties.

2. Click Test Output and configure the module as shown.
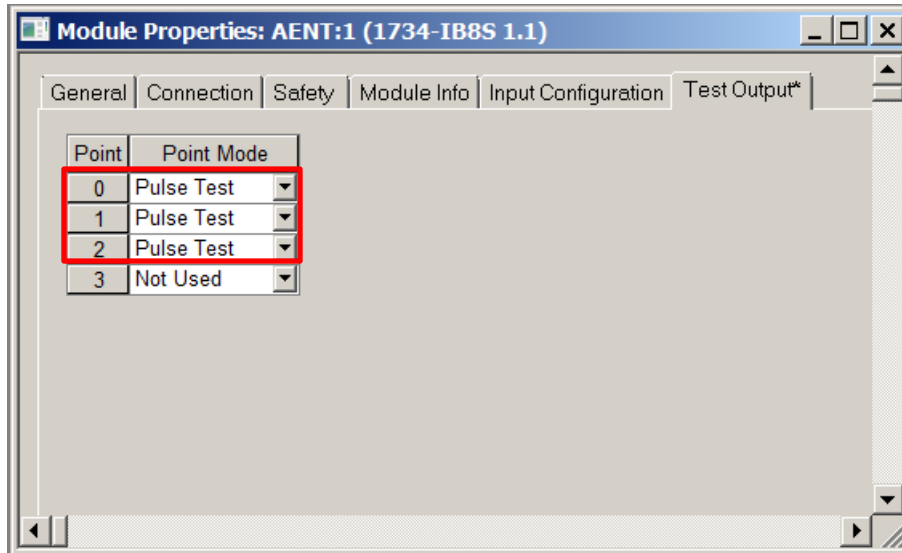
3. Click Input Configuration and configure the module as shown:

    *   Input Points 0/1 are the single beam area access control (AAC).

    *   Input Points 4/5 are the Reset buttons.

    *   Input Point 7 is the contactor monitoring circuit.

        Input Point 7 is being sourced from Test Output 2.
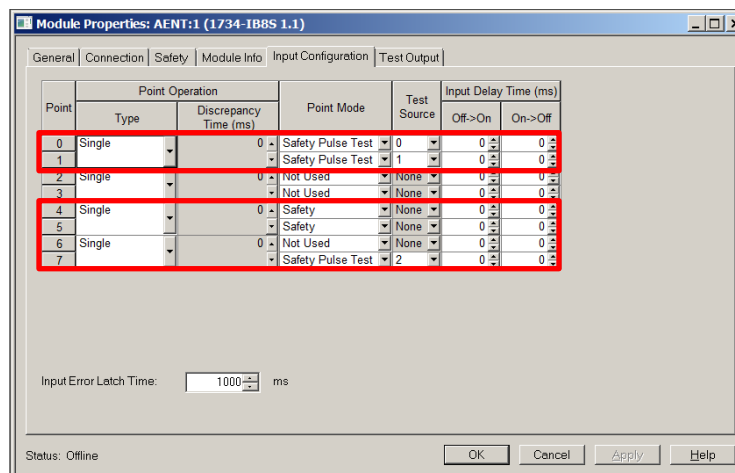
4. Click OK.

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

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

Typically, contactor coils will not react to the pulse testing of the output wires. If using a contactor that does react to the pulse test, then disable the pulse testing. This should not affect the overall safety rating if redundancy and monitoring are being utilized.
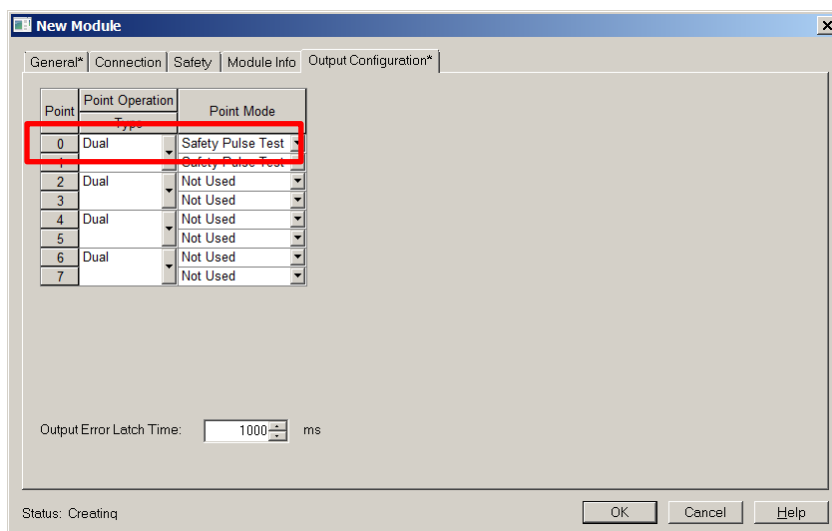
7. Click OK.

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. In this example, it is being used to monitor an area access control sensor.

The DCS instruction monitors dual-input channels for consistency (Equivalent-Active High) and detects and traps faults when the inconsistency is detected for longer than the configured Discrepancy Time (ms).

The automatic restart type allows the DCS output (O1) to reset automatically after a demand. The manual action typically required for safety is provided in rung 1 to reset the safety output enable.

Input status typically represents the channel status of the two input channels. In this example, the Combined Input Status bit goes low (0) if any of the eight input channels has a fault.

In this example, the DCS reset acts as a fault reset. Even when configured for automatic restart, a reset is required to recover from a fault.

The output (O1) of the DCS is used as a safety interlock in the seal-in rung to drive the output enable tag. If the DCS output drops out, so does the output enable, and it remains off until a manual reset action is carried out.

The Configurable Redundant Output (CROUT) instruction controls and monitors redundant outputs. Essentially, this instruction verifies that feedback follows the safety outputs appropriately. For the negative feedback used in this example; if the outputs are high (1), the feedback is low (0) and vice versa. In this example, the feedback has 500 ms to change to the proper state. Because only a single feedback circuit is being used, the feedback tag is used for both Feedback 1 and 2.

The two output tags from the CROUT instructions are used to drive the contactor outputs on the 1734-OB8S module.

```
0                                                                          ┌─DCS──────────────────────────────┐
                                                                           │ Dual Channel Input Stop           │
                                                                           │ DCS                      AAC_1    │──(O1)─
                                                                           │ Safety Function     SAFETY GATE   │
                                                                           │ Input Type    EQUIVALENT - ACTIVE HIGH │──(FP)─
                                                                           │ Discrepancy Time (Msec)      250  │
                                                                           │ Restart Type          AUTOMATIC  │
                                                                           │ Cold Start Type       AUTOMATIC  │
                                                                           │ Channel A           AENT:1:I.Pt00Data │
                                                                           │                              1 ←  │
                                                                           │ Channel B           AENT:1:I.Pt01Data │
                                                                           │                              1 ←  │
                                                                           │ Input Status  AENT:1:I.CombinedInputStatus │
                                                                           │                              1 ←  │
                                                                           │ Reset               AENT:1:I.Pt05Data │
                                                                           │                              0 ←  │
                                                                           └───────────────────────────────────┘

1   AENT:1:I.Pt04Data  ONS_Safety1   AAC_1.O1  ACC_CROUT1.FP                                      ACC_OutputEnable1
        ─] [─          ─[ONS]─       ─] [─     ─]/[─                                                    ─( )─
    ACC_OutputEnable1
        ─] [─

2                                                                          ┌─CROUT────────────────────────────┐
                                                                           │ Configurable Redundant Output     │
                                                                           │ CROUT                ACC_CROUT1   │──(O1)─
                                                                           │ Feedback Type          NEGATIVE   │──(O2)─
                                                                           │ Feedback Reaction Time (Msec)  500 │
                                                                           │ Actuate         ACC_OutputEnable1 │──(FP)─
                                                                           │                              1 ←  │
                                                                           │ Feedback 1          AENT:1:I.Pt07Data │
                                                                           │                              0 ←  │
                                                                           │ Feedback 2          AENT:1:I.Pt07Data │
                                                                           │                              0 ←  │
                                                                           │ Input Status  AENT:1:I.CombinedInputStatus │
                                                                           │                              1 ←  │
                                                                           │ Output Status AENT:2:I.CombinedOutputStatus │
                                                                           │                              1 ←  │
                                                                           │ Reset               AENT:1:I.Pt05Data │
                                                                           │                              0 ←  │
                                                                           └───────────────────────────────────┘

3   ACC_CROUT1.O1  ACC_CROUT1.O2                         AENT:2:O.Pt00Data  AENT:2:O.Pt01Data
        ─] [─         ─] [─                                    ─( )─              ─( )─

(End)
```

Falling Edge Reset

EN 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 ACC_OutputEnable1 rung. Then use the OSF instruction Output Bit tag as the reset bit for the following rung. The ACC_OutputEnable is still used to enable the CROUT instruction. The modified code appears below in rungs 1 and 2.

```
0
                                                        ┌────DCS─────────────────────────┐
                                                        │ Dual Channel Input Stop        │
                                                        │ DCS                    AAC_1   │──(O1)──
                                                        │ Safety Function    SAFETY GATE │
                                                        │ Input Type  EQUIVALENT - ACTIVE HIGH │──(FP)──
                                                        │ Discrepancy Time (Msec)    250 │
                                                        │ Restart Type        AUTOMATIC  │
                                                        │ Cold Start Type     AUTOMATIC  │
                                                        │ Channel A        AENT:1:I.Pt00Data │
                                                        │                             1 ← │
                                                        │ Channel B        AENT:1:I.Pt01Data │
                                                        │                             1 ← │
                                                        │ Input Status AENT:1:I.CombinedInputStatus │
                                                        │                             1 ← │
                                                        │ Reset            AENT:1:I.Pt05Data │
                                                        │                             0 ← │
                                                        └────────────────────────────────┘

      AENT:1:I.Pt04Data                                 ┌────OSF─────────────────────────┐
1     ─┤ ├─                                             │ One Shot Falling               │
                                                        │ Storage Bit      ACC_OSF       │──(SB)──
                                                        │ Output Bit  OSF_Safety1        │──(OB)──
                                                        └────────────────────────────────┘

      OSF_Safety1    AAC_1.O1   ACC_CROUT1.FP                                   ACC_OutputEnable1
2     ─┤ ├───────────┤ ├────────┤/├────────────────────────────────────────────────( )──
      ACC_OutputEnable1
      ─┤ ├─

3                                                       ┌────CROUT───────────────────────┐
                                                        │ Configurable Redundant Output  │
                                                        │ CROUT              ACC_CROUT1  │──(O1)──
                                                        │ Feedback Type        NEGATIVE  │
                                                        │ Feedback Reaction Time (Msec)  500 │──(O2)──
                                                        │ Actuate        ACC_OutputEnable1 │
                                                        │                             1 ← │──(FP)──
                                                        │ Feedback 1       AENT:1:I.Pt07Data │
                                                        │                             0 ← │
                                                        │ Feedback 2       AENT:1:I.Pt07Data │
                                                        │                             0 ← │
                                                        │ Input Status  AENT:1:I.CombinedInputStatus │
                                                        │                             1 ← │
                                                        │ Output Status AENT:2:I.CombinedOutputStatus │
                                                        │                             1 ← │
                                                        │ Reset            AENT:1:I.Pt05Data │
                                                        │                             0 ← │
                                                        └────────────────────────────────┘

      ACC_CROUT1.O1  ACC_CROUT1.O2                       AENT:2:O.Pt00Data   AENT:2:O.Pt01Data
4     ─┤ ├───────────┤ ├──────────────────────────────────────( )───────────────( )──

(End)
```
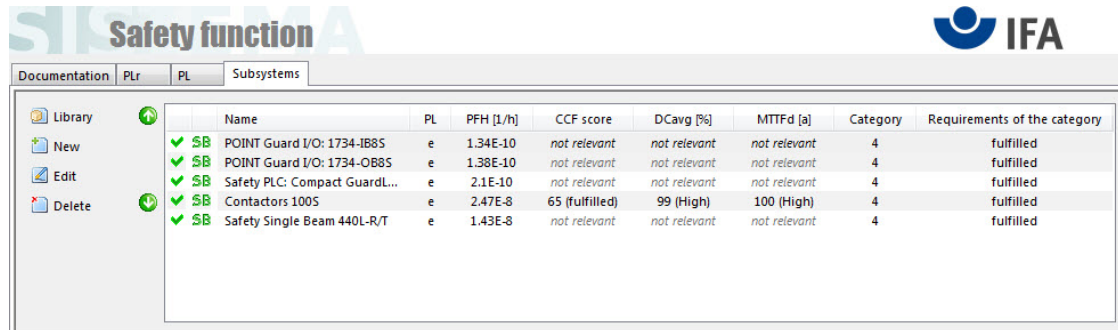
Calculation of the Performance Level

The Performance Level required from the risk assessment is Category 3, Performance Level d (CAT. 3, PLd). When properly implemented, the safety function described here can achieve a CAT. 4, PLe according to EN ISO 13849-1: 2008, as calculated by using the SISTEMA software PL calculation tool. Calculations are based on the safety function being operated once an hour, 24 hours a day, 365 days a year for a total of 8760 operations a year. The 100S contactors are used in the safety function; therefore, their calculations are based on 17,520 operations per year.

The overall Safety Function Performance Level is shown below.

The Safety Function can be represented in block diagrams.
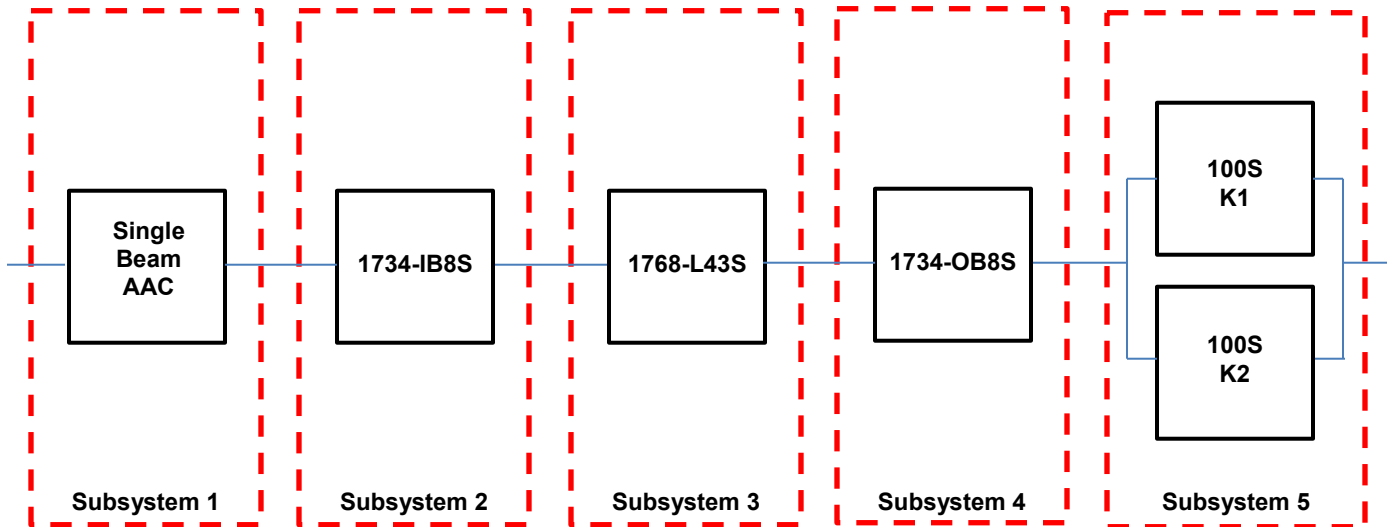
Single-beam Area Access Control Sensor Safety Function Subsystem 1

SB Safety Single Beam 440L-R/T	
PL	e
PFH [1/h]	1.43E-8
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Single-beam Area Access Control Sensor Safety Function Subsystem 2

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

Single-beam Area Access Control Sensor Safety Function Subsystem 3

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

Single-beam Area Access Control Sensor Safety Function Subsystem 4

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

Single-beam Area Access Control Sensor Safety Function Subsystem 5

SB Contactors 100S	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Because these are electro-mechanical devices, the safety contactors 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 contactors along with the estimated frequency of use, entered during the creation of the SISTEMA project.

The DCavg (99%) for the contactors is selected from the Output Device table of EN ISO 13849-1 Annex E, Direct Monitoring.

The CCF value is generated by using the scoring process outlined in Annex F of EN ISO 13849-1. The complete CCF scoring process must be performed when actually implementing an application. A minimum score of 65 must be achieved.

Verification and Validation Plan

Verification and validation play important roles in the avoidance of faults throughout the safety system design and development process. 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).

GuardLogix Single-beam Area Access Control (AAC) Sensor Safety Function Verification and Validation Checklist

General Machinery Information	
Machine Name/Model 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 Manuals listed in the Additional Resources.		
	Verify that the safety application program has been designed in accordance with the GuardLogix Application Instruction Safety Reference Manuals listed in the Additional Resources.		
	Visually inspect the safety system network and I/O and verify that it is wired as documented in the schematics.		
	Visually inspect the area access control and verify that it is wired as documented.		
	Visually inspect the RSLogix 5000 program to verify that safety systems network and I/O module configurations are configured as documented.		
	Visually inspect the RSLogix 5000 application program to verify suitable safety-certified instructions are utilized. 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 window.		
	All the output devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags window.		

GuardLogix Single-beam AAC Sensor Safety Function Verification and Validation Checklist (continued)

Normal Operation Verification - The GuardLogix safety system properly responds to all normal Start, Stop, AAC Sensor Input, and Reset commands.			
Test Step	**Verification**	**Pass/Fail**	**Changes/Modifications**
	Initiate a Start command. Both contactors energize for a normal machine run condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	Initiate a Stop command. Both contactors de-energize for a normal machine Stop condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	While the system is running, interrupt the single-beam area access control sensor. Both contactors de-energize and open for a normal safe condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication. Repeat for all sensors.		
	While the system is stopped, interrupt the single-beam area access control sensor and initiate a Start command. Both contactors remain de-energized and open for a normal safe condition. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	Initiate a Reset command. Both contactors remain de-energized. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
Abnormal Operation Validation - The GuardLogix safety system properly responds to all foreseeable faults with corresponding diagnostics.			
Single-beam Area Access Control Sensor Tests			
Test Step	**Validation**	**Pass/Fail**	**Changes/Modifications**
	While the system is running, remove the channel 1 wire from the safety I/O. Both contactors de-energize. 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. Both contactors de-energize. 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. Both contactors de-energize. 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. Both contactors de-energize. Verify proper machine-status indication and RSLogix 5000 safety application program indication. Repeat for channel 2. Verify that the system is unable to reset and restart with a fault. Restore channel 1 and channel 2 wiring.		

GuardLogix Single-beam AAC Sensor Safety Function Verification and Validation Checklist (continued)

Test Step	Verification and Validation	Pass/Fail	Changes/Modifications
	GuardLogix Control and Network Tests		
	While the system is running, remove the Ethernet network connection between the safety I/O and the controller. All contactors de-energize. 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 state of 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. All contactors de-energize. Return controller keyswitch back to Run mode. All contactors remain de-energized. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	Safety Contactor Output Tests		
Test Step	**Verification and Validation**	**Pass/Fail**	**Changes/Modifications**
	Initiate a Start Command. Both contactors energize 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 contactor feedback from the safety I/O module. All contactors remain energized. Initiate a Stop command followed by a Reset command. The system does not restart or reset. Verify proper machine-status indication and RSLogix 5000 safety application program indication.		
	While the system is running, short the contactor feedback to the safety I/O. 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.		

Additional Resources

Refer to these publications for more information about related products from Rockwell Automation.

Resource	Description
Compact GuardLogix Controllers User Manual, publication 1768-UM002	Provides information on configuring, operating, and maintaining 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 Control Systems Safety Reference Manual, publication 1756-RM093	Provides detailed requirements for achieving and maintaining safety ratings with the GuardLogix and Compact GuardLogix controller systems.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides detailed information on the GuardLogix Safety Application Instruction Set.
GuardLogix 5570 Controller Systems Safety Reference Manual, publication 1756-RM099	Contains detailed requirements for achieving and maintaining safety ratings with the GuardLogix 5570 controller system.
Safety Accelerator Toolkit for GuardLogix System 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.
Area Access Control Safety Single Beam User Manual, publication 440L-UM002	Provides information on configuring, operating, and maintaining Area Access Control Safety Single Beam Light Curtains.
Safety Product Catalog, publication S117-CA001	Provides data and guidance concerning safety principals, standards component data, 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