Application Technique

Original Instructions

Door Locking and Monitoring with a 442G Access Box and an Integrated Safety Controller Safety Function

Products: GuardLogix 5580 or Compact GuardLogix 5380 Controller, 442G Multifunctional Access Box, 440T Rotary Switch, Compact 5000 I/O Safety Modules, 100S-C Contactors

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

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

General Safety Information

Contact Rockwell Automation to learn more about our safety risk assessment services.

IMPORTANT This application example is for advanced users and assumes that you are trained and experienced in safety system requirements.

ATTENTION: Perform a risk assessment to make sure that all task and hazard combinations have been identified and addressed. The risk assessment can require additional circuitry to help reduce the risk to a tolerable level. Safety circuits must consider safety distance calculations, which are not part of the scope of this document.

Safety Distance Calculations

ATTENTION: While safety distance or access time calculations are beyond the scope of this document, compliant safety circuits must often consider a safety distance or access time calculation.

Non-separating safeguards provide no physical barrier to help prevent access to a hazard. Publications that offer guidance for calculating compliant safety distances for safety systems that use non-separating safeguards, such as light curtains, scanners, two-hand controls, or safety mats, include the following:

- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

Separating safeguards monitor a movable, physical barrier that guards access to a hazard. Publications that offer guidance for calculating compliant access times for safety systems that use separating safeguards, such as gates with limit switches or interlocks (including SensaGuard™ switches), include the following:

- EN ISO 14119:2013 (Safety of Machinery – Interlocking devices associated with guards - Principles for design and selection)
- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

In addition, consult relevant national or local safety standards to verify compliance.

Introduction

This safety function application technique explains how to wire, configure, and program a 442G Multifunction Access Box (MAB) with CIP Safety™ to monitor a 440T Rotary Trapped Key interlock switch to control a power-to-release door using a Compact GuardLogix® controller. The 440T Rotary Trapped Key interlock switch is used in the personnel access sequence and to grant exclusive control of the machine to the holder of the key. The 442G MAB locks and monitors the access to the hazardous area. If the door is opened or unlocked, or a fault is detected in the safety function, the Compact 5000™ I/O safety modules de-energize and monitor a redundant pair of 100S-C contactors.

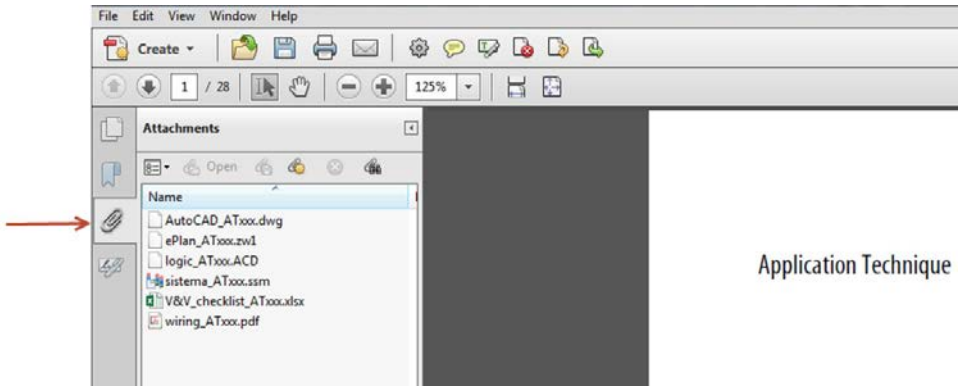
This example uses a Compact GuardLogix (5069-L3100ERMS2) controller, but you can substitute a GuardLogix controller that supports the safety rating that is demonstrated in this safety function application technique. The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA)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

Use Sample Project Files

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

To access these files, follow these steps.

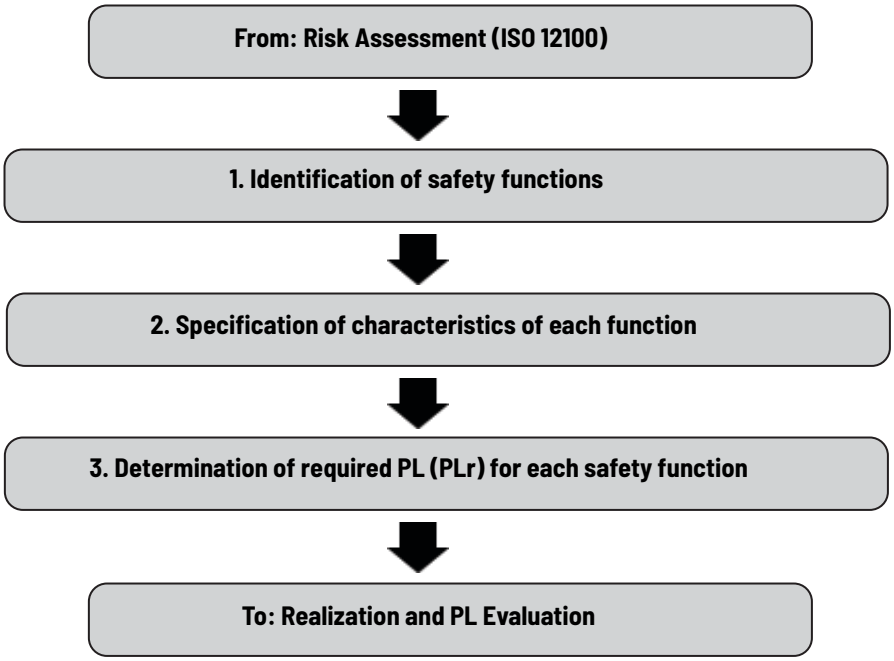
1. If you are viewing the PDF file in a browser and do not see the Attachments link, download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link.
3. Right-click and save the desired file.



4. Open the file in the appropriate application.

Safety Function Realization: Risk Assessment

The Performance Level required (PLr) is the result of a risk assessment and refers to the amount of the risk reduction to be conducted by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. In this application, the Performance Level required by the risk assessment is category 3, Performance Level d (cat. 3, PLd), for each safety function. A safety system that achieves cat. 3, PLd, or higher, can be considered control reliable. Each safety product has its own rating and can be combined to create a safety function that meets or exceeds the PLr.



Safety Functions

This application technique includes four safety functions:

- E-stop stop category 0
- Enabling switch monitor
- Guard door lock monitor
- Guard door lock control

Safety Function Requirements

Access to hazardous motion is prevented by using an interlocked guard door with guard locking. This safety function makes sure that the hazard has stopped, that safety output power has been removed, and that the trapped key has been released, before the gate is unlocked upon request. It also monitors the lock and door, and it drops output power if they unexpectedly change state. If any fault occurs, such as loss of communications, output power to the safety actuators is dropped. While the door is open, its status is monitored to prevent unexpected startup while it is open. When the door is closed and locked, hazardous motion and power to the motor do not resume until the exclusive control device is activated and a secondary action (Reset button depressed) occurs.

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

Functional Safety Description

In this example, an unlock is requested by pressing an Unlock Request button on the MAB. The unlock request is sent over a CIP Safety connection to the Compact GuardLogix safety controller. The safety controller drops out the redundant contactors, and the hazard coasts to a stop. The safety contactors (K1 and K2) are connected to a pair of safety outputs on a 5069-OBV8S safety output module. The I/O modules are connected, via the backplane, to the Compact GuardLogix safety controller. Once the operator has pressed the Unlock Request, the operator is required to turn the trapped key clockwise and release it before access to the hazardous area is permitted. The operator must carry the trapped key into the hazardous area, which gives the key holder exclusive control over the restart of the machine. After the hazard stops, and if the trapped key has been released, the safety controller commands the MAB to unlock the door, which allows entry to the hazard. In this example, there is a 5 second time delay to simulate this stop. In your application you must determine how to monitor for the hazard stopping. Once the operator has completed the routine and repetitive maintenance, the operator closes the door and extends the bolt via the handle. If the door is closed, the bolt is extended, and the operator has put the trapped key back in place, a Lock button on the MAB can be used to send a signal to the safety controller to lock the door by de-energizing the lock solenoid. In this example, the lock is power-to-release.

The GuardLogix safety code monitors the status of the door by using the pre-certified safety instruction, Dual Channel Input Stop with Test and Lock (DCSTL). The MAB provides a status bit that indicates that the door is closed, the bolt is extended, and the bolt is locked. These status interlocks are monitored by the GuardLogix DCSTL instruction.

When all safety input interlocks (the DCSTL is one of these interlocks) are satisfied, no faults are detected, and a safety restart button on the MAB is pressed, a second GuardLogix certified function block called Configurable Redundant Output (CROUT) controls and monitors feedback for a pair of 100S redundant contactors. The CROUT instruction energizes and de-energizes the contactors and monitors electromechanical feedback to make sure that both contactors operate properly.

If a demand is placed on any other safety interlock, in this example it is the MAB E-stop, the redundant contactors are dropped out. The Unlock Request button can then be used to request access to the hazard. The DCSTL safety instruction makes sure that the hazard is stopped before the door is unlocked.

Bill of Material

This application technique uses these products.

Cat. No.	Description	Quantity
442G-MABAMPH	442G-MAB mounting plate, handle assembly	1
442G-MABE1	Escape release, 442G-MAB, standard shaft	1
442G-MABRB-UR-EOJP4679	Lock module, 442G access box, power-to-release, unique code, EtherNet/IP® (2 x M12, D-coded), right-hand guard, E-stop, four push buttons, and connector for enabling switch	1
442G-MABH-R	Handle assembly, 442G access box, right-hinged door, with bolt-locking mechanism	1
442G-MABAMPE	442G-MAB mounting plate, escape release	1
440T-MRKSE110A	Single-key rotary switch - enclosure-mounted, standard key code labeling, 2 N.O. and 2 N.C. contacts, 20 Amp current	1
440T-AKEYE130A	Key for 440T trapped-key systems, code A	1
100S-C09EJ23C	100S-C safety contactor, 9 A, line side, 24V DC (with electric coil)	2
5069-IB8S	5069 Compact I/O 8-channel, 24V DC safety input module	1
5069-OBV8S	5069 Compact I/O 8-channel 24V DC safety configurable output module	1
5069-RTB18-SCREW	5069 Compact I/O 18 pins screw type terminal block kit in a pack of 1 piece	2
889D-F4AC-2	Power cable - DC Micro (M12), female, straight, 4-pin, PVC cable, yellow, unshielded, IEC color-coded, no connector, 2 meter (6.56 feet), 22 AWG	1
889D-M4AC-2	Trapped-key cable - DC Micro (M12), male, straight, 4-pin, PVC cable, yellow, unshielded, IEC color-coded, no connector, 2 meter (6.56 feet), 22 AWG	1
1585D-M4UBJM-2	MAB to controller Ethernet cable - 1585 Ethernet cables, cat. 5e, 100BASE-TX, 100 Mbit/s, 4 conductors, M12, straight male, standard, RJ45, straight male, teal PUR, shielded, high flex, PUR, halogen-free, 10 million cycles	1
1585J-M4TBJM-1	Controller to laptop cable – 1585 Ethernet cables, Cat 5e, 100BASE-TX, 100 Mbit/s, 4 conductors, RJ45, straight male, standard, RJ45, straight male, teal, robotic TPE, UL CMB, CMX, c-UL, CMG, standard TIA 568-B	1

Choose one of the following safety-controller hardware groups.

Controller	Cat. No.	Description	Quantity
GuardLogix 5580[1]	1756-L81ES 1756-L82ES 1756-L83ES 1756-L84ES	GuardLogix Processor, 3 MB standard memory, 1.5 MB safety memory GuardLogix Processor, 5 MB standard memory, 2.5 MB safety memory GuardLogix Processor, 10 MB standard memory, 5 MB safety memory GuardLogix Processor, 20 MB standard memory, 6 MB safety memory	1
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A7	Seven-slot ControlLogix chassis	1
Compact GuardLogix 5380–SIL 2	5069-L306ERS2 5069-L306ERMS2 5069-L310ERMS 5069-L310ERMS2 5069-L320ERS2 5069-L320ERMS2 5069-L330ERS2 5069-L330ERMS2 5069-L340ERS2 5069-L340ERMS2 5069-L350ERS2 5069-L350ERMS2 5069-L380ERS2 5069-L380ERMS2 5069-L3100ERS2 5069-L3100ERMS2	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	1
	1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 100...120 / 220...240V AC / 290V DC input voltage	1
	5069-ECR	Right end cap and terminator	1

Controller	Cat. No.	Description	Quantity
Compact GuardLogix 5380 - SIL 3	5069-L306ERMS3 5069-L310ERMS3 5069-L320ERMS3 5069-L330ERMS3 5069-L340ERMS3 5069-L350ERMS3 5069-L380ERMS3 5069-L3100ERMS3	Compact GuardLogix processor, 0.6 MB standard memory, 0.3 MB safety memory Compact GuardLogix processor, 1.0 MB standard memory, 0.5 MB safety memory Compact GuardLogix processor, 2.0 MB standard memory, 1.0 MB safety memory Compact GuardLogix processor, 3.0 MB standard memory, 1.5 MB safety memory Compact GuardLogix processor, 4.0 MB standard memory, 2.0 MB safety memory Compact GuardLogix processor, 5.0 MB standard memory, 2.5 MB safety memory Compact GuardLogix processor, 8.0 MB standard memory, 4.0 MB safety memory Compact GuardLogix processor, 10.0 MB standard memory, 5.0 MB safety memory	1
	1606-XLP72E	Compact power supply, 24...28V DC, 72 W, 100...120 / 220...240V AC / 290V DC input voltage	1
	5069-ECR	Right end cap and terminator	1

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

Setup and Wiring

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

System Overview

The MAB and Compact GuardLogix safety controller are connected over a CIP Safety connection.

The following status information is communicated from the MAB to the controller:

- Door/handle position, RFID technology (safety-rated status)
- Bolt position (safety-rated status)
- Lock status (safety-rated status)
- E-stop position (safety-rated status)
- Trapped-key status (safety-rated status)
- Four push buttons (used for Unlock request/Lock request/resets in this safety function)
- RUN Mode
- MAB Faults
- Trapped-key faults

The following control information is communicated from the controller to the MAB:

- Fault resets
- Lock solenoid control (safety-rated control data)
- Four lights
- E-stop light

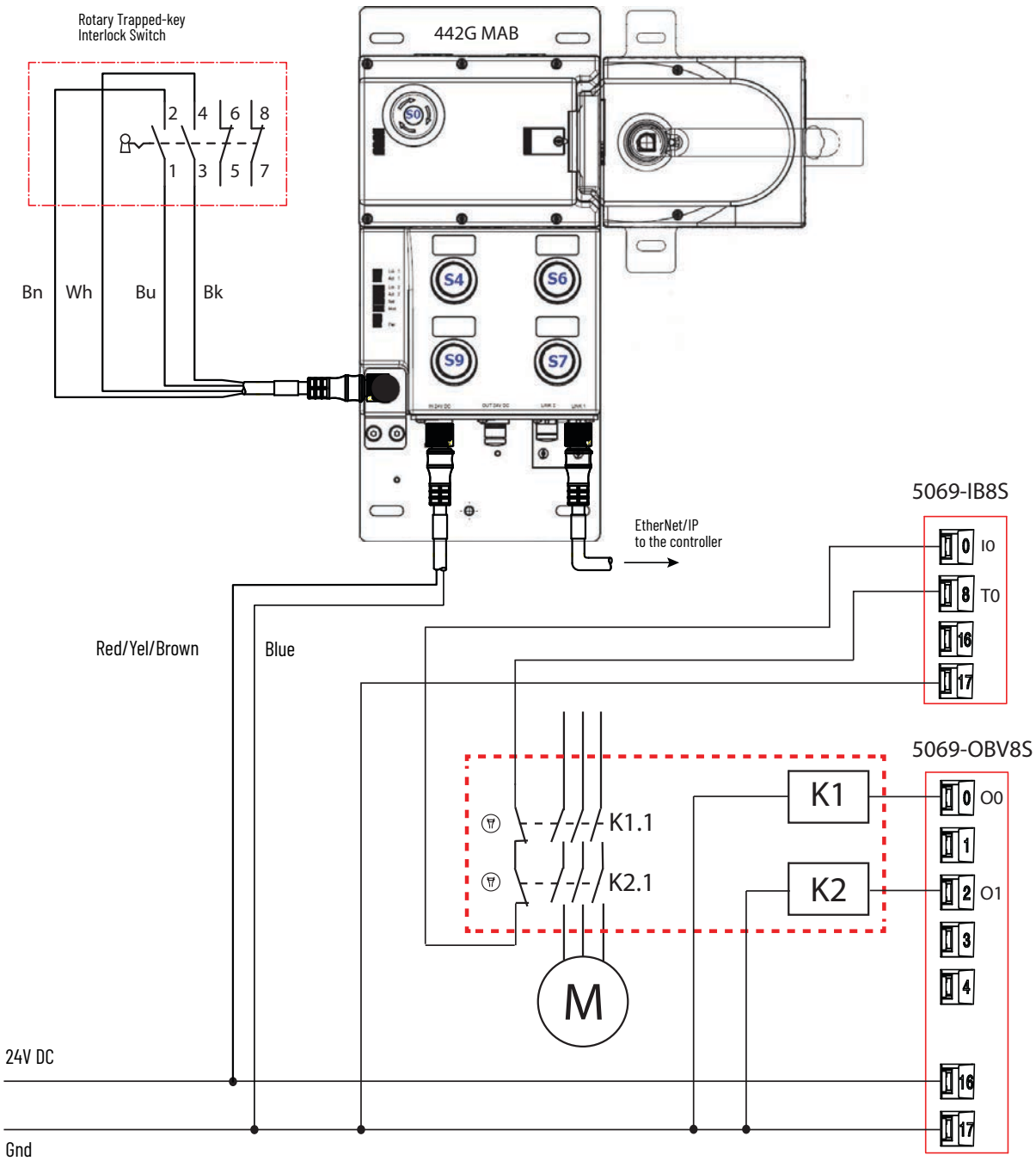
The final control device, in this case, is a pair of 100S safety contactors, K1 and K2. The contactors are controlled by a 5069-OBV8S safety output module. The contactors are wired in a redundant-series configuration. A feedback circuit is wired through the K1 and K2 normally open contacts and back to an input on the 5069-IB8S module to monitor the contactors for proper operation. The contactors cannot restart if the feedback circuit is not in the correct state.

The contactor feedback circuit is wired to the 5069-IB8S safety input module in this example. Feedback wiring to a safety module is not required for functional safety. The feedback circuit could be wired to a standard input module.

The system has individual reset buttons for resetting faults and resetting safety outputs.

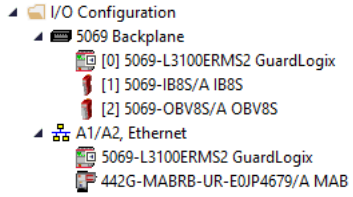
Electrical Schematic

For an electrical schematic in AutoCAD or EPLAN format, see the attached files.



Network Architecture

For information about the I/O configuration from the Controller Organizer in the Logix Designer application, see the attached ACD files.



Compact GuardLogix 5380 Controller with Embedded Ethernet Connection

Configuration

The Compact GuardLogix controller is configured by using the Studio 5000 Logix Designer® application, version 32 or later. You must create a project and add the Compact 5000 I/O modules and the 442G multifunctional access box. A detailed description of each step is beyond the scope of this document. Knowledge of the Logix Designer application is assumed.

For a Studio 5000 Logix Designer project file that you can import into your own project, see the attached ACD file. The attached ACD file includes a GuardLogix 5580 controller, but if you choose a Compact GuardLogix 5380 controller, you can change the controller in the Logix Designer program.

Minimum Logix Designer Application Version	Product
31	GuardLogix 5580 or Compact GuardLogix 5380 controller
32	5069-IB8S Compact I/O 8 channel safety sink input module or 5069-OBV8S Compact I/O 8 channel configurable safety output module
20	Guardmaster® 442G Multifunctional Access Box

Input 0 in the 5069-IB8S module is for the contactor-monitoring circuit. Input 0 is sourced from Test Output T0.

The output points 1 and 2 in the 5069-OBV8S module are configured in dual mode and are connected to the coils of the contactor pair.

Create a Project with a GuardLogix Controller

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

1. In the Logix Designer application, create a project with a GuardLogix controller that includes the following:
   - A connection to an Ethernet network
   - GuardLogix 5580 and Compact GuardLogix 5380 controllers have Ethernet ports

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

2. Set the IP address for the controller or any Ethernet communication modules, if used.
3. Add a Compact 5000 Ethernet adapter to your project, if you are using a GuardLogix 5580 controller.
4. Add a 5069-IB8S Compact 5000 I/O Safety Input module to your project.
5. Add a 5069-OBV8S Compact 5000 I/O Safety output module to your project.
6. Configure the modules properly for your application.
   See the Additional Resources for information on your I/O modules.

7. Add a 442G MAB to your project.
8. Configure the 442G MAB properly for your application.
   See the Additional Resources for information on your product.

Programming

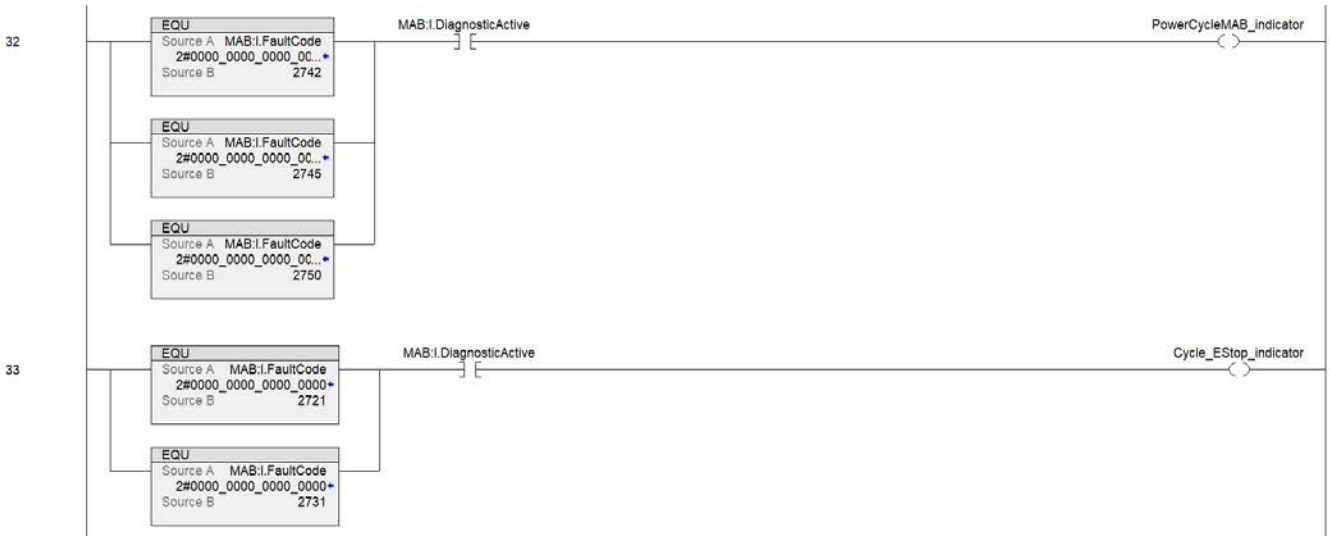
For controller logic that you can download to your controller, see the attached ACD file.

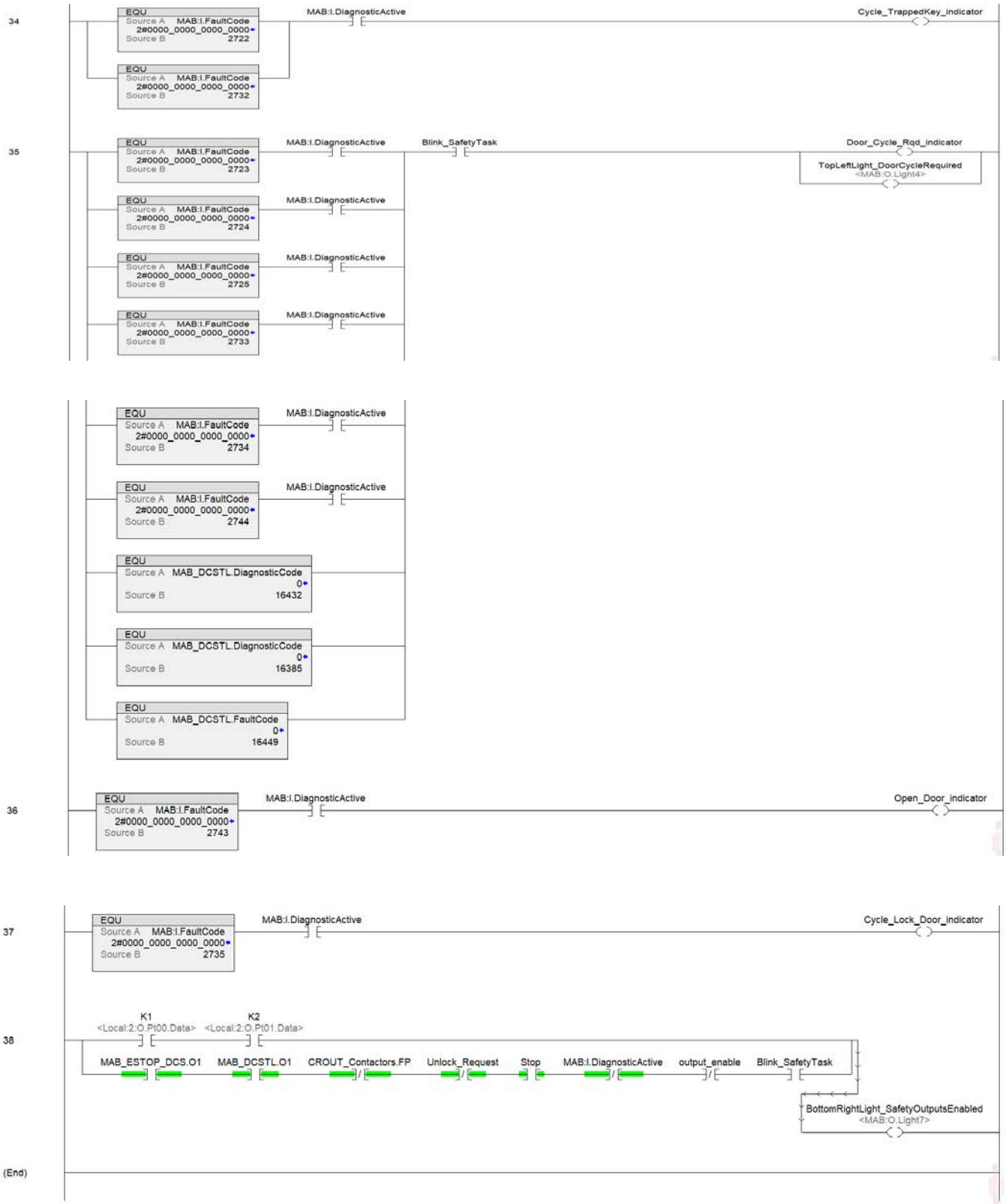

8
Unlock_Stop
TRAPPED_KEY_RELEASED
MAB:I.GuardLocked
Unlock_Request
MAB:I.GuardLocked
Unlock_Request
Lock_Request
9
MAB_DCSTL.ULC
MAB:O.Unlock
10
TopRightPB_LockRequest
<MAB:I.Switch6>
TRAPPED_KEY_DCS.O1
MAB:I.GuardClosed
MAB:I.GuardInterlocked
Lock_Request
11
BottomRightPB_SafetyReset
<MAB:I.Switch7>
OSF
Storage Bit Wrk_OSF_SB
Output Bit Wrk_OSF_OB
SB
OB
12
Wrk_OSF_OB
MAB_ESTOP_DCS.O1
MAB_DCSTL.O1
TRAPPED_KEY_DCS.O1
CROUT_Contactors.FP
Unlock_Stop
Unlock_Request
Stop
MAB:I.DiagnosticActive
output_enable
output_enable
13
Local:2:I.Pt00.Status
Local:2:I.Pt01.Status
CONTACTORS_OK
14
Local:1:I.Pt00.Status
FEEDBACK_OK


15
CROUT
CROUT CROUT_Contactors
Feedback Type NEGATIVE
Feedback Reaction Time (Msec) 1000
Actuate output_enable
1
Feedback 1 Local:1:I.Pt00.Data
0
Feedback 2 Local:1:I.Pt00.Data
0
Input Status FEEDBACK_OK
0
Output Status CONTACTORS_OK
1
Reset BottomLeftPB_Reset
<MAB:I.Switch9>
0
O1
O2
FP
16
CROUT_Contactors.O1
CROUT_Contactors.O2
K1
<Local:2:O.Pt00.Data>
K2
<Local:2:O.Pt01.Data>
17
ToggleLO_for_Test_Request
Hazard_Stopped
Test_Request
18
CROUT_Contactors.O1
CROUT_Contactors.O2
CROUT_Contactors.Feedback1
TON
Timer Hazard_Stopped_Timer
Preset 5000
Accum 0
EN
DN


19
Hazard_Stopped_Timer.DN
Hazard_Stopped
20
MAB_DCSTL.FP
Blink_SafetyTask
BottomLeftLight_ResetRequired
<MAB:O.Light9>
MAB_ESTOP_DCS.FP
CROUT_Contactors.FP
MAB:I.DiagnosticActive
TRAPPED_KEY_DCS.FP
21
MAB:I.GuardLocked
TopRightLight_DoorLocked
<MAB:O.Light6>
Unlock_Request
MAB:I.DiagnosticActive
MAB:I.GuardClosed
MAB:I.GuardInterlocked
Blink_SafetyTask
22
BottomLeftPB_Reset
<MAB:I.Switch9>
MAB:I.LockSequenceFault
MAB:O.LockSequenceFaultUnlatch
23
MAB:O.LockSequenceFaultUnlatch
TON
Timer LockFaultTimer
Preset 2000
Accum 0
EN
DN
24
LockFaultTimer.DN
MAB:O.LockSequenceFaultUnlatch


25
BottomLeftPB_Reset
<MAB:I.Switch9>
MAB:I.LockSequenceFault
MAB:I.DiagnosticActive
MAB:O.GeneralFaultUnlatch
26
MAB:O.GeneralFaultUnlatch
TON
Timer GeneralFaultTimer
Preset 2000
Accum 0
EN
DN
27
GeneralFaultTimer.DN
MAB:O.GeneralFaultUnlatch
28
MAB:I.CycleThresholdExceeded
Cycle_Threshold_Exceeded_indicator
29
TRAPPED_KEY_DCS.O1
ONS.1
ONS
CTU
Counter TRAPPED_KEY_CTU
Preset 100000
Accum 0
CU
DN
30
TRAPPED_KEY_CTU.DN
TrappedKey_Cycle_Threshold_Exceeded
31
TRAPPED_KEY_Replaced
TRAPPED_KEY_CTU
RES


32
EQU
Source A MAB:I.FaultCode
2#0000_0000_0000_00...
Source B 2742
EQU
Source A MAB:I.FaultCode
2#0000_0000_0000_00...
Source B 2745
EQU
Source A MAB:I.FaultCode
2#0000_0000_0000_00...
Source B 2750
MAB:I.DiagnosticActive
PowerCycleMAB_indicator
33
EQU
Source A MAB:I.FaultCode
2#0000_0000_0000_0000
Source B 2721
EQU
Source A MAB:I.FaultCode
2#0000_0000_0000_0000
Source B 2731
MAB:I.DiagnosticActive
Cycle_EStop_indicator



Rung 0

This rung sets the input status in the emergency stop DCS instruction. This MAB_EStop_Status is required in order to meet the requirements for diagnostics and monitoring of the healthy state of the safety devices. If the MAB connection is valid, and there are no MAB emergency stop faults, then set the DCS MAB emergency stop input status to high (1). This can be done in the same way for other safety input devices.

Rung 1

The DCS instruction monitors the E-stop button on the MAB. The E-stop button is not part of the door-lock safety function. Both the emergency stop interlock and door interlock drop out the safety output enable in rung 12. The MAB is a safety device residing on the CIP Safety network, so there is no safety issue with use of only one tag for the MAB emergency stop state. That one tag is placed into both channel A and channel B. There is never a DCS discrepancy fault, because the same tag is used for both channels, but the DCS instruction provides the reset/restart functionality without having to write additional code. This system is also recommended for other single-channel safety signals or dual-channel safety input devices, even if they are not E-stop buttons.

Rungs 2 and 3

These rungs have the same structure as the previous two rungs. In this case, they provide status of and monitor the trapped key.

The bits generated in this block by the DCS are later used as part of the lock and unlock procedure in rungs 4 and 10. The O1 bit is also used to drop the safety output enable in rung 12.

Rung 4

This rung generates a bit that signals when the trapped key has been removed and there are not faults present. It uses the bits from the Trapped Key DCS in rung 3 to verify that.

This bit is used later in rung 8 as part of the unlock procedure.

Rung 5

This rung sets the input status in the MAB DCSTL instruction. If the MAB connection is valid, then set the DCSTL MAB door lock input status to high (1). The MAB Lock status cannot be used to influence the DCSTL input status. Many MAB faults require the door to be opened and closed to recover, and if the DCSTL input status goes to low (0), the DCSTL unlock command cannot be changed unless the input status recovers. That creates a problem—the MAB status cannot be reset until the DCSTL input status is repaired, which requires the MAB status to be repaired.

Rung 6

The DCSTL instruction monitors the door and lock on the MAB.

Every time the door unlocks, the DCSTL instruction requires that the door be opened and then closed. A fault occurs if the gate is unlocked and then locked without the door opening and closing. The branches above the DCSTL instruction provide a software-driven demand on the door. If the door unlocks, then the channels are set to low (0) for one scan only. Other than that single scan, the channels are driven by the MAB status, which indicates whether the door is closed and the bolt is extended. The software-driven demand does not operate when the DCSTL instruction sees a request to test the door, which occurs when the Test Request input is toggled to low (0).

The basic operation of the DCSTL instruction is as follows. To set the DCSTL output O1 (door interlock) to high (1):

- channel A and channel B must be set to high (1),
- the test request must be set to high (1),
- the unlock request must be set to low (0),
- the lock feedback (FB) must be set to high (1),
- the hazard stopped parameter must be set to high (1), which indicates that the hazard is stopped,
- the input status must be set to high (1).

A reset can then turn on output O1. The Hazard_Stopped parameter would typically then go to low (0) because the door interlock lets the hazard move.

To unlock the gate, the assumption is that the hazard is moving and that the Hazard_Stopped parameter is low (0). An unlock request is made by setting the unlock request of the DCSTL instruction to high (1)—rung 8 drives the unlock request in this example. When the hazard stops and turns to high (1), the unlock command (ULC) is set to high (1) by the DCSTL instruction. The high (1) unlock command unlocks the door by energizing the coil (this MAB is power-to-release), which sets the lock feedback to low (0)—rung 9 drives the unlock request in this example.The unlock remains high (1) and the operator can enter the hazardous area. Upon leaving the hazardous area, the operator closes the door and turns the handle to extend the bolt. To lock the door, remove the demand of the unlock request—rung 10 drives the unlock request in this example. The DCSTL instruction responds by setting the ULC to low (0). The low (0) unlock command de-energizes the coil and locks the door, which sets the lock feedback to high (1).

IMPORTANT The requirements of your application determine the proper way to generate the Hazard Stopped input value.

The DCSTL output 01 is used as a door interlock to drop out the safety actuators in rung 12.

Rung 7

This rung controls the beginning of the unlock procedure. When the Unlock Request (top-left button on the MAB) is pressed, this puts a safe stop demand in Rung 12. The Unlock Stop demand is sealed in until there is a Lock Request.

Rung 8

This rung controls the unlock request input to the DCSTL instruction. If the gate is locked, there is an unlock stop command and the operator releases the trapped key. Then the rung seals in the command until there is a Lock_Request. This lock request is controlled in rung 10.

Rung 9

This rung controls the lock solenoid of the power-to-release MAB. The DCSTL unlock command controls the Unlock output, which unlocks the MAB solenoid.

Run 10

This rung controls the Lock_Request in rungs 7 and 8. When the Lock Request (top-right button on the MAB) is pressed with the trapped key enabled and the door closed and interlocked, the Lock_Request bit turns high (1). This disables the Unlock Stop and Unlock Request in rungs 7 and 8, and it then locks the door.

Rung 11

This rung generates a reset command on the falling edge of the safety reset (bottom-right button on the MAB). For more information about the falling edge reset, see Falling Edge Reset on page 20.

Rung 12

This rung is a seal-in for the safety-output enable interlock. The enable is used as the actuate input in the CROUT instruction in rung 15. It seals in around the reset button. The seal-in is broken if either the emergency stop, door interlock, or the trapped key are dropped out due to either a demand or a fault. Faults in the output circuit that are monitored by the CROUT instruction also break the seal-in. If there is an unlock request or a stop command, the seal-in is broken. If the seal-in is broken, the CROUT instruction output is dropped out and the hazard coasts to a stop. Typically, a stop command is generated by a normally-closed, red push button. But in this sample code, the stop interlock is manually toggled. The only time that it is required to be used is to stop the hazard so that the operator can test the door.

Rungs 13 and 14

These rungs enable the CONTACTORS_OK and the FEEDBACK_OK bits to check the status of the safety contactors and the feedback input from the contactors. These status bits are required in the CROUT to verify the healthy state of the output and feedback points.

For the contactor status, the CONTACTORS_OK bit verifies that there is no fault present in the Output module or in the output points 0 and 1, where the contactors are wired. For the feedback status, the FEEDBACK_OK bit verifies that there is no fault present in the Input module or in the input point 0 where the feedback is wired.

Rung 15

The CROUT instruction controls the redundant safety contactors and monitors the feedback circuit to make sure that both contactors are operating properly. The actuator is driven by the output enable seal-in in rung 12. If the channel status is not valid, then the CROUT outputs drop out.

The outputs of the CROUT instruction drive the redundant safety contactors, K1 and K2. In this example, the bottom-right light on the MAB is energized in rung 16 when the contactors are energized.

Rung 16

The two output tags from the CROUT instruction are used to drive the contactor outputs on the 5069-OBV8S module.

Rung 17

The DCSTL instruction supports a test function. If Test_Request transitions from high (1) to low (0), then the operator must open and close the gate to satisfy the test requirement. The DCSTL instruction drops out output (01) during the test, so the hazard must be stopped before the test request is made.

Follow these steps to test the function:

- Press and release the E-stop button. This action stops the hazard.
- Wait for the hazards to stop.
- Toggle ToggleLO_for_Test_Request from high (1) to low (0) and back to high (1). This action places the Test_Request demand.
- Press the Unlock Request (top left button on the MAB) and release the Trapped Key. This action unlocks the MAB.
- Open and close the gate.
- Place the Trapped key back in place and press the Lock Request (top right button on the MAB). This action locks the MAB.
- Reset the safety function to complete the test procedure and enable the safety outputs.

Rungs 18 and 19

These rungs explain how to implement the Hazard Stopped condition.

To unlock the MAB, you must generate a safety tag for the DCSTL instruction that indicates the hazard is stopped, and that it is safe for the DCSTL instruction to unlock the door.

In this example, for test purposes, a timer is used to signal the hazard stop after the worst time scenario for the stopping time (in this case 5000 ms) after the outputs are disabled.

This Hazard Stopped condition is specific to each application and can be determined during the risk assessment process.

Rungs 20 through 38

These rungs show some of the extra features and available tags on the MAB and how to implement them.

Rung 20

This rung blinks a light (bottom left) on the MAB, if the door monitor (DCSTL instruction), the MAB emergency stop monitor (DCS instruction), the trapped keys (DCS instruction), the contactors (CROUT instruction), or the MAB hardware has a fault for which a fault reset is required to recover. The blink is driven by code in a standard task, and the Blink_SafetyTask tag is generated in the mapping tool.

Rung 21

This rung energizes the top-right light on the MAB, if the door is locked. The light blinks if the door is closed and unlocked, waiting to be locked.

Rungs 22 through 24

If the MAB has an internal Lock Sequence Fault, then the reset button (bottom left on the MAB) can be used to unlatch the fault. The MAB requires that the reset pulse width be 10 ms…10,000 ms in length, which is the purpose of the 2000 ms timer.

Rungs 25 through 27

If the MAB has an internal General Fault, then the reset button (bottom left on the MAB) can be used to unlatch the fault. The MAB requires that the reset pulse width be 10 ms…10,000 ms in length, which is the purpose of the 2000 ms timer.

Rung 28

This rung indicates when the MAB lock solenoid has reached 1,000,000 cycles. One million is the maximum number of switching cycles that are allowed in the lifetime of the MAB.

Rung 29 through 31

These rungs indicate when the trapped-key contactors have reached 100,000 cycles. This number of cycles is the maximum number of switching cycles that are allowed in the lifetime of the trapped keys.

Each time the contactor is open and closed, that action adds a cycle to the total. When the value reaches the lifetime maximum, it enables a bit that indicates the need of the change.

In rung 31, there is a bit that can be used to signal when the trapped key was replaced, which restarts the count.

Rung 32

This indicator can be used to inform maintenance that the MAB has a fault that requires a power cycle to recover.

Rung 33

This indicator can be used to inform maintenance that the MAB has a fault that requires the emergency stop (E-stop) on the MAB to be cycled, followed by a reset, to recover.

Rung 34

This indicator can be used to inform maintenance that the MAB has a fault that requires the trapped key to be cycled, followed by a reset, to recover.

Rung 35

This indicator can be used to inform maintenance that the MAB has a fault that requires the door on the MAB to be opened, followed by a reset, to recover.

Rung 36

This indicator can be used to inform maintenance that the MAB has a fault that requires the door on the MAB to be cycled, followed by a reset, to recover. In this example, the top-left light on the MAB is flashed to indicate that an unlock is required before the door can be cycled. This light also flashes if the DCSTL instruction is in a state that requires a door cycle.

Rung 37

This indicator can be used to inform maintenance that the MAB has a fault that requires the lock on the MAB to be cycled, followed by a reset, to recover.

Rung 38

The bottom-right light on the MAB is energized when the contactors are energized, and the light blinks if the safety interlocks are satisfied and all that remains to energize the contactors is a safety reset (bottom-right button on the MAB).

Falling Edge Reset

ISO 13849-1 stipulates that instruction reset functions must occur on falling edge signals. To comply with this requirement, a One Shot Falling (OSF) instruction is used on the reset rung. Then, the OSF instruction Output Bit tag is used as the reset bit for the STO output rung.

Calculation of the Performance Level

When properly implemented, these safety functions can achieve a safety rating of category 3, Performance Level d (cat. 3, PLd), according to ISO 13849-1: 2015, as calculated by using the SISTEMA software PL calculation tool.

IMPORTANT To calculate the PL of your entire safety function, you must include the specific subsystems you chose. Depending on the devices you choose, the overall safety rating of your system will be different.

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

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

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

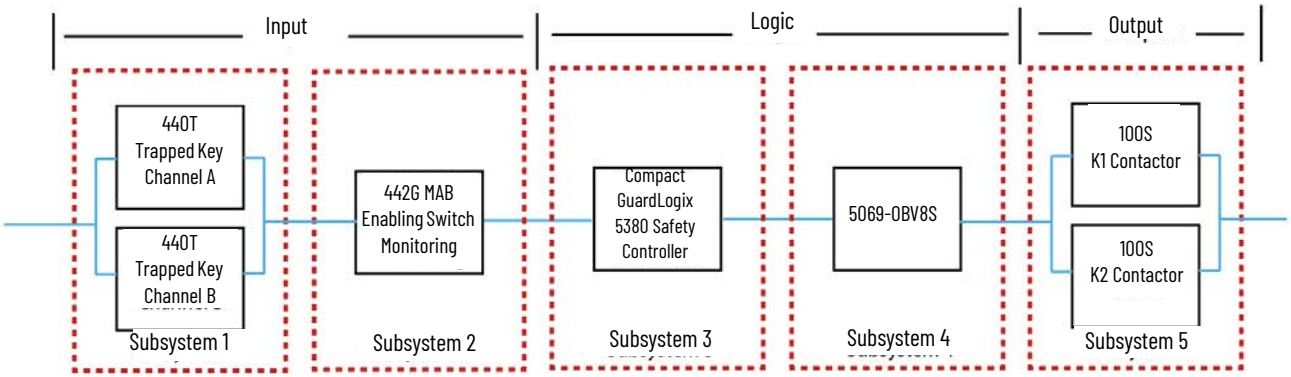
Status	Name	PL	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category
✔ SB	Safety PLC: GuardLogix 1756-L8xES	d	6.4E-9	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3

Assuming the use and proper installation, and configuration of the products suggested in this document, the following category and Performance Level achieved for each safety function is shown in the following graphic. The levels that are achieved on the four safety functions are identical.

Enabling Switch Monitor Safety Function

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category
✔ SB	Prosafe 440T - Trapped key interlock system	d	d	1E-7	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Access Box: 442G-MAB CIP Safety Enabling Switch Monitor	d	d	3.1E-9	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Compact GuardLogix Safety I/O	d	d	3.1E-10	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Contactors 100S-C	d	d	1E-9	65 (fulfilled)	99 (High)	2,173.2 (High)	4

The Enabling Switch Monitor Safety Function can be modeled as follows.



Calculations are based on the total number of operations for all safety functions. On the one hand, the enabling switch monitor, the guard door lock monitor, and the guard door lock control work together. They run 360 days per year for 16 hours per day, with an actuation of the safety gate once every hour. This frequency equals 5760 operations per year. On the other hand, the E-stop Category 0 Stop runs 360 days per year for 16 hours per day, with an actuation of the safety gate once every day. This frequency equals 360 operations per year. Therefore, the total number of operations (nop) equals 6120 operations per year.

The measures against Common Cause Failure (CCF) are quantified by using the scoring process that is outlined in Annex F of ISO 13849-1. For the purposes 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.

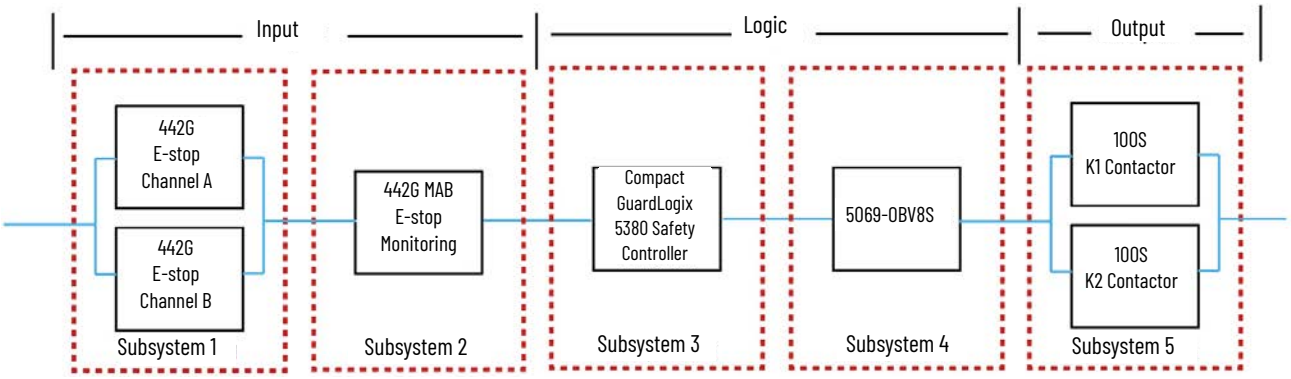
IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 1.1E-7. The PL for the complete safety function is PLd.

The other safety functions in this document can be modeled as follows.

E-stop Category 0 Stop Safety Function

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category
✔ SB	Access Box: 442G-MAB CIP Safety E-Stop Switch	d	d	9.1E-10	65 (fulfilled)	99 (High)	2,500 (High)	4
✔ SB	Access Box: 442G-MAB CIP Safety E-Stop Monitor	d	d	3.1E-9	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Compact GuardLogix Safety I/O	d	d	3.1E-10	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Contactors 100S-C	d	d	1E-9	65 (fulfilled)	99 (High)	2,173.2 (High)	4

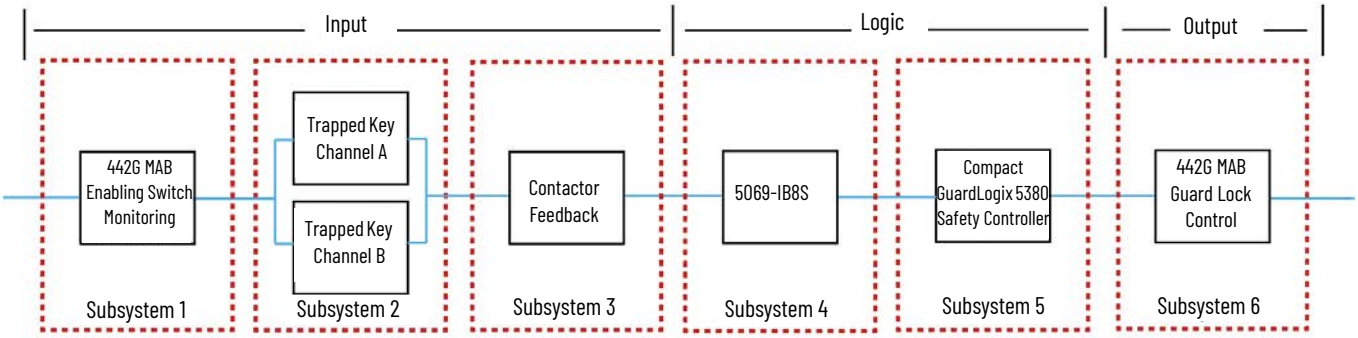
This safety function can be modeled as follows:



Guard Door Lock Control Safety Function

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category
✔ SB	Prosafe 440T - Trapped key interlock system	d	d	1E-7	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Access Box: 442G-MAB CIP Safety Enabling Switch Monitor	d	d	3.1E-9	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Contactor Feedback	d	d	2.3E-7	65 (fulfilled)	99 (High)	100 (High)	2
✔ SB	Compact GuardLogix Safety I/O	d	d	2.5E-10	*not relevant*	*not relevant*	*not relevant*	4
✔ SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3
✔ SB	Access Box: 442G-MAB CIP Safety Guard Lock Control	d	d	4.9E-9	*not relevant*	*not relevant*	*not relevant*	4

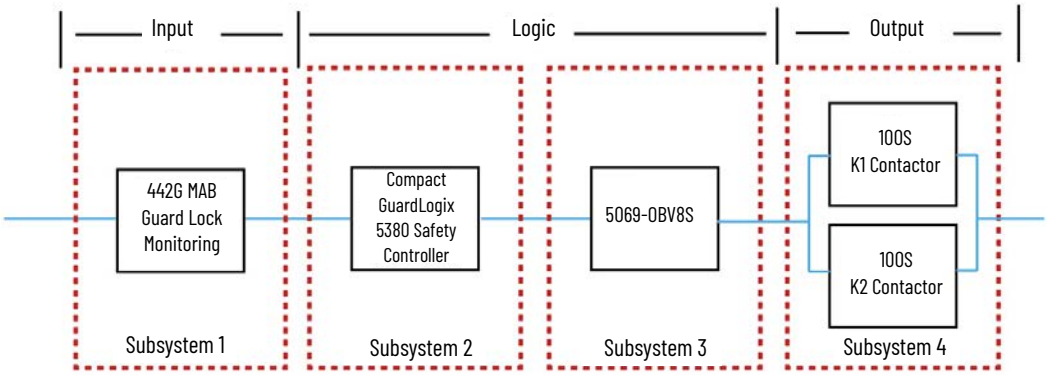
This safety function can be modeled as follows:



Guard Door Lock Monitor Safety Function

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category
SB	Access Box: 442G-MAB CIP Safety Guard Lock Monitor	d	d	3.4E-9	*not relevant*	*not relevant*	*not relevant*	4
SB	Compact GuardLogix 5380, SIL 2, Category 3	d	d	7.2E-9	*not relevant*	*not relevant*	*not relevant*	3
SB	Compact GuardLogix Safety I/O	d	d	3.1E-10	*not relevant*	*not relevant*	*not relevant*	4
SB	Contactors 100S-C	d	d	1E-9	65 (fulfilled)	99 (High)	2,173.2 (H...	4

This safety function can be modeled as follows:



Functional Safety Data Required for Determining the Performance Level of Electromechanical Devices

Because these contactors are electromechanical devices, the functional safety data that are required for the Performance Level calculation includes the following:

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

The functional safety evaluations of the electromechanical devices include the following:

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

SISTEMA calculates the MTTFd by using B10d data that are 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 ISO 13849-1 Annex E, Direct Monitoring.

The CCF value is generated by using the scoring process that is outlined in Annex F of 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. ISO 13849-2 sets the requirements for verification and validation. The standard calls for a documented plan to confirm that all safety functional requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm that the system meets the required Performance Level (PLr) specified. The SISTEMA software is typically used to perform the calculations and assist with satisfying the requirements of ISO 13849-1.

Validation is a functional test of the safety control system to demonstrate that the system meets the specified requirements of the safety function. The safety control system is tested to confirm that all safety-related outputs respond appropriately to their corresponding safety-related inputs. The functional test includes normal operating conditions and potential fault injection of failure modes. A checklist is typically used to document the validation of the safety control system.

Before validating the GuardLogix Safety System, confirm that the safety system and safety application program have been designed in accordance with the controller safety reference manuals that are listed in the Additional Resources and the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095.

For a validation checklist, see the attached spreadsheet.

Additional Resources

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

Resource	Description
GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012	Describes the GuardLogix 5580 and Compact GuardLogix 5380 controller system. Provides instructions on how to develop, operate, or maintain a controller-based safety system that uses the Studio 5000 Logix Designer application.
ControlLogix and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information on how to install, configure, and program the GuardLogix 5580 controllers in the Logix Designer application.
CompactLogix and Compact GuardLogix Controllers User Manual, publication 5069-UM001	Provides information on how to install, configure, and program the Compact GuardLogix 5380 controllers in the Logix Designer application.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Describes the Rockwell Automation GuardLogix Safety Application Instruction Set. Provides instructions on how to design, program, or troubleshoot safety applications that use GuardLogix controllers.
Multifunctional Access Box with CIP Safety over EtherNet/IP User Manual, publication 442G-UM002	Provides instructions on how to design, install, wire, program, and troubleshoot systems that use the 442G multifunctional access box with CIP Safety over EtherNet/IP protocol.
Multifunctional Access Box Installation Instructions, publication 442G-IN001	Provides instructions on how to configure and mount the 42G multifunctional access box.
Prosafe Rotary Key Switch-Box Mounted Installation Instructions, publication 440T-IN026	Provides instructions on how to install and maintain a Prosafe® rotary switch box.
Rockwell Automation Functional Safety Data Sheet, publication SAFETY-SR001	Provides functional safety data for Rockwell Automation® products.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.
Safety Automation Builder© and SISTEMA Library website, rok.auto/sistema	Download Safety Automation Builder to help simplify machine safety design and validation, and reduce time and costs. Integration with our risk assessment software provides you with consistent, reliable, and documented management of the Functional Safety Lifecycle. The SISTEMA tool, also available for download from the Safety Automation Builder page, automates calculation of the attained Performance Level from the safety-related parts of a machine's control system to (EN) ISO 13849-1.

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

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Safety Function Capabilities

Visit rok.auto/safety for more information on our Safety System Development Tools, including Safety Functions.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenkÖy, İstanbul, Tel: +90 (216) 5698400 EEE YÖnetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SAFETY-AT186A-EN-P - June 2021