

Effective Design Methods for Integrating Safety Using Logix Controllers



For Classroom Use Only!

LISTEN.
THINK.
SOLVE.®

 Allen-Bradley • Rockwell Software

**Rockwell
Automation**

Important User Information

This documentation, whether, illustrative, printed, “online” or electronic (hereinafter “Documentation”) is intended for use only as a learning aid when using Rockwell Automation approved demonstration hardware, software and firmware. The Documentation should only be used as a learning tool by qualified professionals.

The variety of uses for the hardware, software and firmware (hereinafter “Products”) described in this Documentation, mandates that those responsible for the application and use of those Products must satisfy themselves that all necessary steps have been taken to ensure that each application and actual use meets all performance and safety requirements, including any applicable laws, regulations, codes and standards in addition to any applicable technical documents.

In no event will Rockwell Automation, Inc., or any of its affiliate or subsidiary companies (hereinafter “Rockwell Automation”) be responsible or liable for any indirect or consequential damages resulting from the use or application of the Products described in this Documentation. Rockwell Automation does not assume responsibility or liability for damages of any kind based on the alleged use of, or reliance on, this Documentation.

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

Except as specifically agreed in writing as part of a maintenance or support contract, equipment users are responsible for:

- properly using, calibrating, operating, monitoring and maintaining all Products consistent with all Rockwell Automation or third-party provided instructions, warnings, recommendations and documentation;
- ensuring that only properly trained personnel use, operate and maintain the Products at all times;
- staying informed of all Product updates and alerts and implementing all updates and fixes; and
- all other factors affecting the Products that are outside of the direct control of Rockwell Automation.

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

Throughout this manual we use the following 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.

IMPORTANT

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

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
 - recognize the consequence
-

SHOCK HAZARD

Labels may be located on or inside the drive to alert people that dangerous voltage may be present.

BURN HAZARD

Labels may be located on or inside the drive to alert people that surfaces may be dangerous temperatures.

Effective Design Methods for Integrating Safety Using Logix Controllers

Contents

Before you begin	4
About this lab	4
Tools & prerequisites	4
Getting Started	5
Value of Integrated Safety.....	6
Single Program Editor for Safety and Standard Application	6
Safety Status Available in the Standard Application through Safety Tags.....	9
Safety Configuration Management	11
Ease of Use – Safety-Related Code	15
Manual Reset.....	18
Safety Output Interlocks.....	18
Certified Safety Instructions	20
Safety Performance without Sacrificing Productivity through Diagnostics	30
CIP Safety Diagnostics	30
Safety Input Diagnostics	32
Safety Output Diagnostics	48

Before you begin

This lab assumes a basic understanding of RSLogix 5000 software.

About this lab

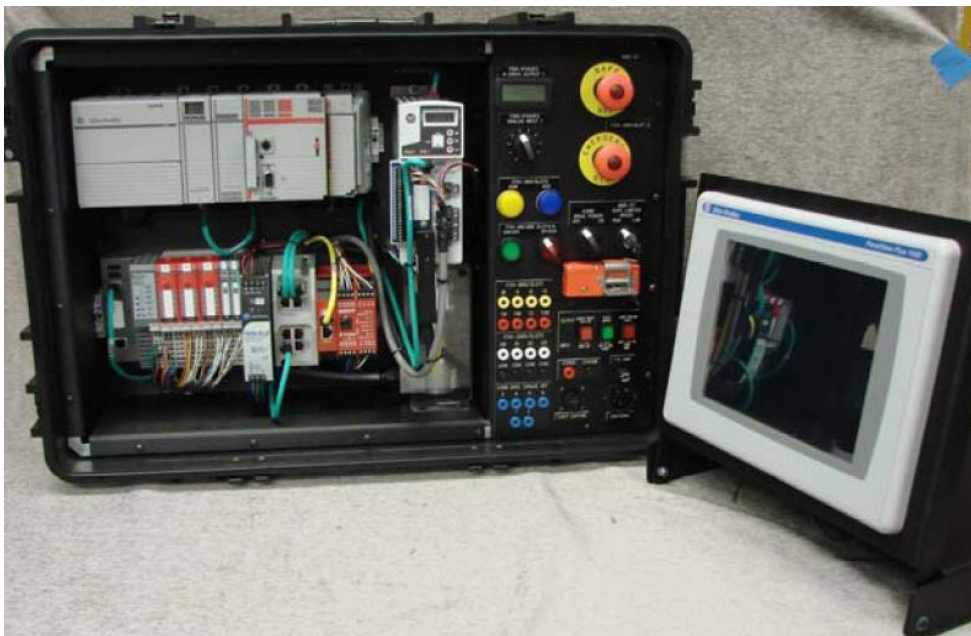
In this lab, you will see how Rockwell Automation has integrated safety products, features and functions into an environment that allows effective and efficient programming for your safety needs. Parallel safety processing, dedicated safety tasks in the PLC, certified safety function blocks and safety I/O handling work together allowing you to achieve your safety goals in a much simpler, straightforward manner.

This lab takes approximately 65 minutes to complete.

Tools & prerequisites

The following software programs, hardware, and files are required for use with this lab.

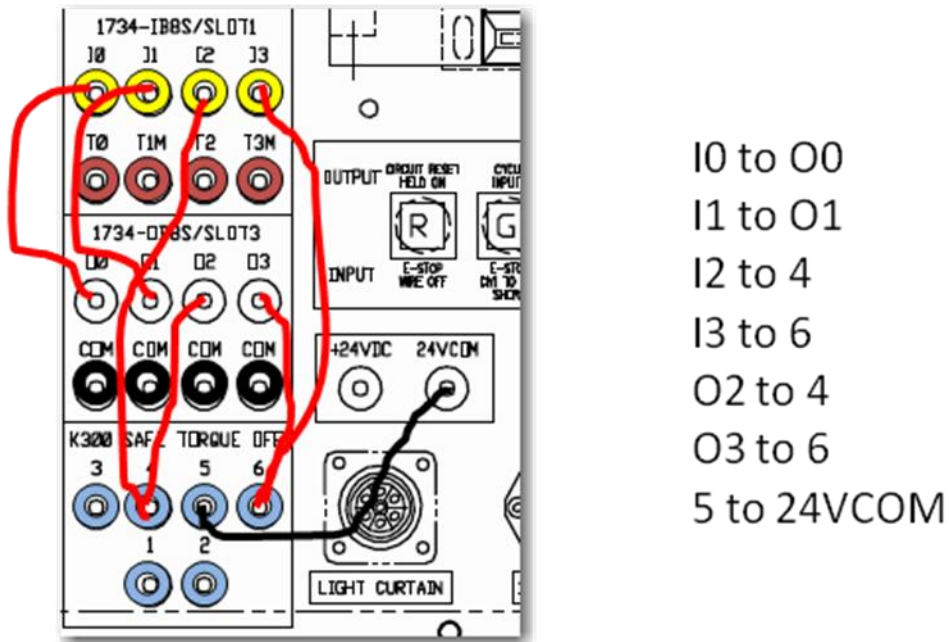
- Software Programs:
 - RSLinx Classic 2.58 or later
 - RSLogix 5000 Professional v19.01
- Hardware Devices:
 - Compact Machine Solutions Demo Case
- Files required:
 - Compac GuardLogix - CMSS_Core_Demo.acd
 - PanelView Plus 1000 - CMSS_Core_Demo.mer
 - MSR57 - CMSS_Core_Demo.csf



Getting Started

The 'CMSS_Core_Demo' ACD file should already be loaded. Please verify that the program is running and the case is ready for the lab by performing the following:

1. Verify the seven jumper cables are attached as shown:



2. Set the potentiometer to 5 on the dial.
The potentiometer controls the speed of the motor. The value of 5 is well below the safe speed threshold configured in the MSR57P.
3. Verify the MSR57P safe limited speed key switch is set to the **RUN** position.
4. Verify the K300 Drive Power key switch is in the **ON** position.
5. If the Safe Off pushbutton is flashing, release it.
6. If the Emergency Stop pushbutton is flashing, release it.
7. The red selector switch (**Fault Reset**) is flashing, cycle it from the counter-clockwise left position to the clockwise right position and back to the left.
8. The green button (**Safety Circuit Reset**) is flashing; press it to energize the K300 safety enables.
The 'K300 Status' light should energize. The light indicates the K300 Safety inputs are energized. You should hear the drive/motor energize, but the motor is not turning.
9. The yellow button (**Start Drive Motion**) is flashing; press it to start drive motion.

Value of Integrated Safety

Compact GuardLogix is a CompactLogix with integrated safety, certified to be used in safety control systems up to SIL3 (IEC61508), CAT4 (EN954-1) and PLe (ISO13849-1). It performs all of the same functions as a standard CompactLogix in addition to performing safety control. To achieve these safety ratings GuardLogix uses dual controller architecture (1oo2):

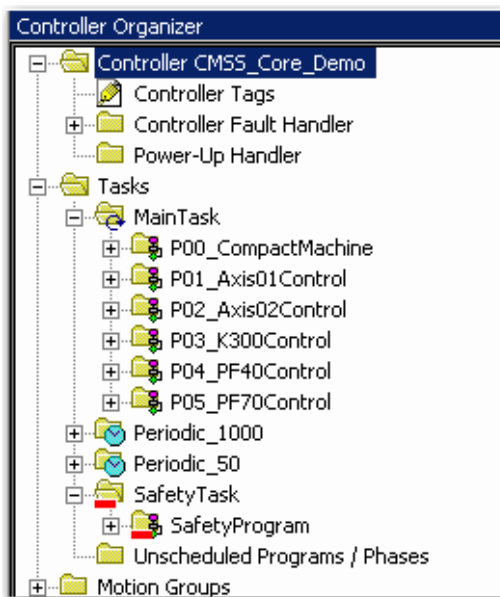
- The primary controller is in charge of standard and safety
- The partner controller runs only safety

The primary and partner controllers compare their safety task scan results. If they ever disagree, they will go to the safe state (de-energized).

Single Program Editor for Safety and Standard Application

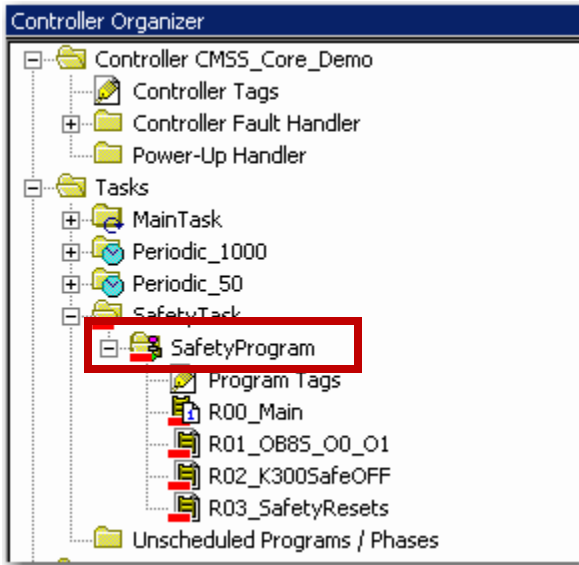
Compact GuardLogix is configured with a single software package, RSLogix 5000, simplifying your engineering efforts. You create a single project to manage both your standard and safety code. All of the safety code is contained within the Safety Task. It has the same structure as a standard task; but it is unique in that it is scanned in both the primary and partner processors. .

1. Open the **CMSS_Core_Demo.acd** file on the desktop.



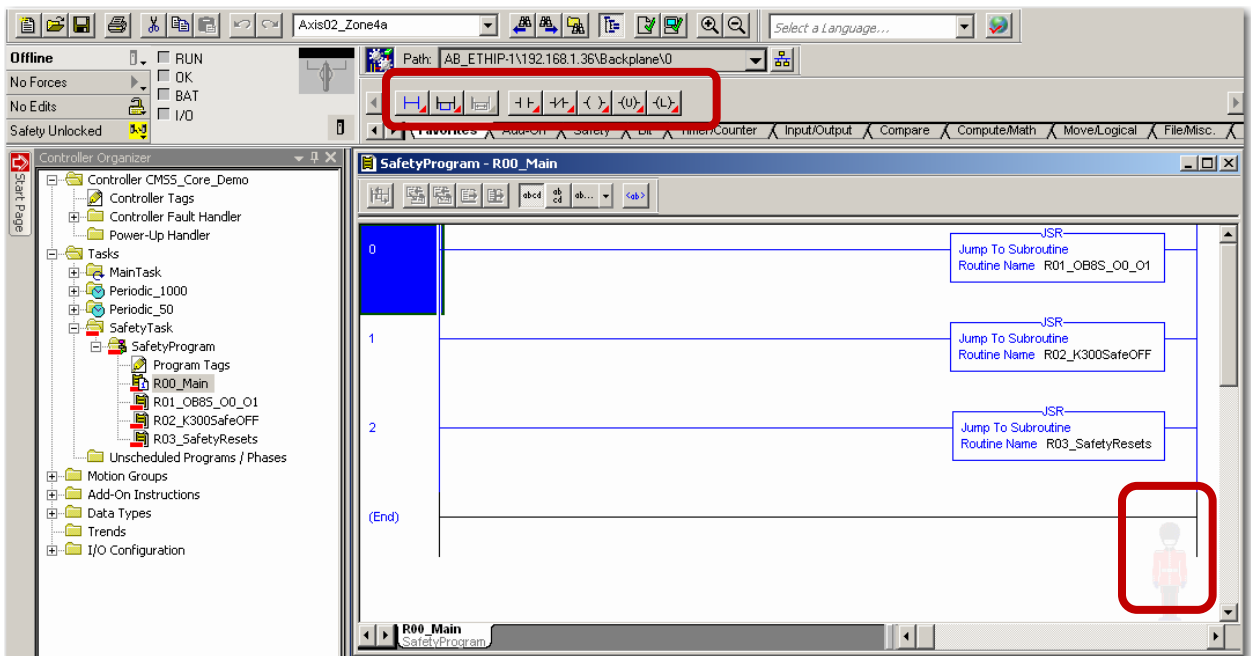
A single project contains both the standard and safety code.

2. Expand the **SafetyProgram** in the **SafetyTask**.



All of the safety code is contained within the Safety Task. It has the same structure as a standard task; but it is unique in that it is scanned in both the primary and partner processors. The red bar under the routines and folders in the safety task indicate these routines perform safety logic.

3. Double-click **R00_Main** routine in the **SafetyProgram**.



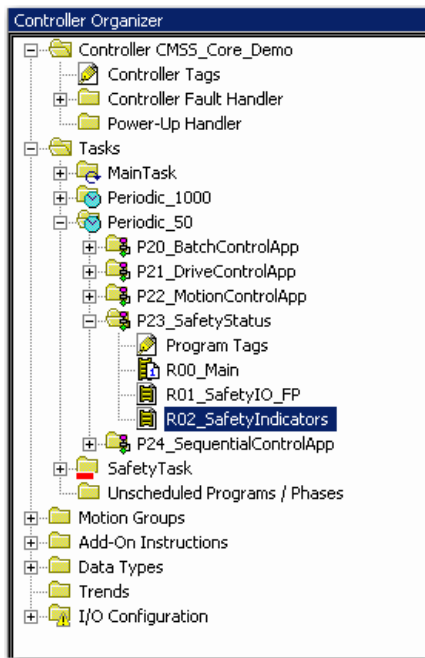
Notice the Guard safety icon in the bottom-right side of the MainRoutine window, indicating you are accessing safety code. Also notice the red labels on the instructions available in the safety task. These instructions are certified for use in the safety task.

4. Close the **R00_Main** routine.

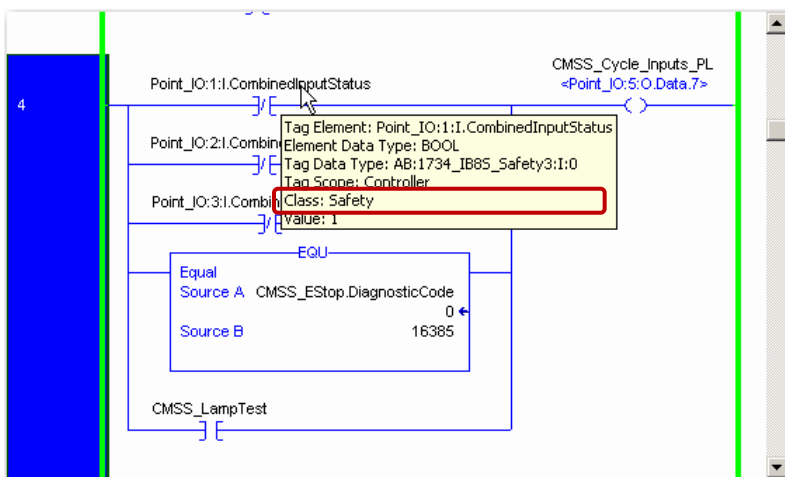
Safety Status Available in the Standard Application through Safety Tags

A special class of tag called a Safety tag is used within the Safety Task. The integrity of a safety tag is protected because they can only be written to by logic within the Safety Task. However, Safety tags can be read in the Standard or Safety Task. This eliminates the need to hardwire safety system status back to your standard control system.

1. Open the **R02_SafetyIndicators** standard routine in the **P23_SafetyStatus** program with the **Periodic_50** task:

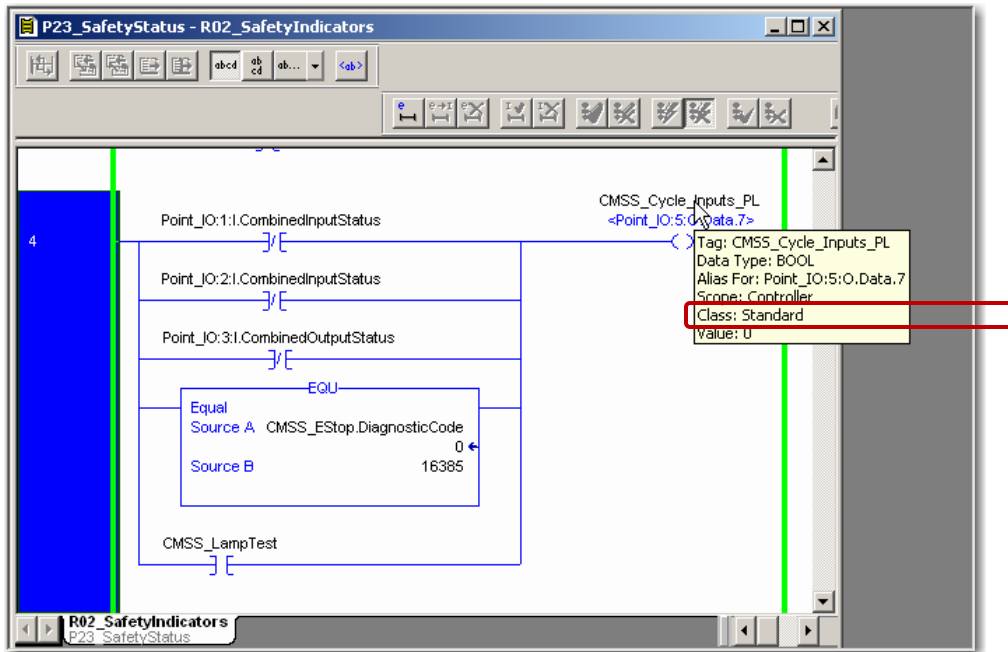


2. Scroll to rung 4 of the **R02_SafetyIndicators** routine and hover your cursor over the **Point_IO:1:I.CombinedInputStatus** tag.



The safety class tag [Point_IO:1:I.CombinedInputStatus] is being monitored within a standard routine to control a standard pilot light.

3. Hover your cursor over the output tag [CMSS_Cycle_Inputs_PL] on the same rung:



Prior to safety PLCs users would hardwire the auxiliary contacts on all of their safety devices back to the standard PLC for status information. This practice is obsolete with the GuardLogix because this status information is readily available for the standard side of the application with the Safety Tags.

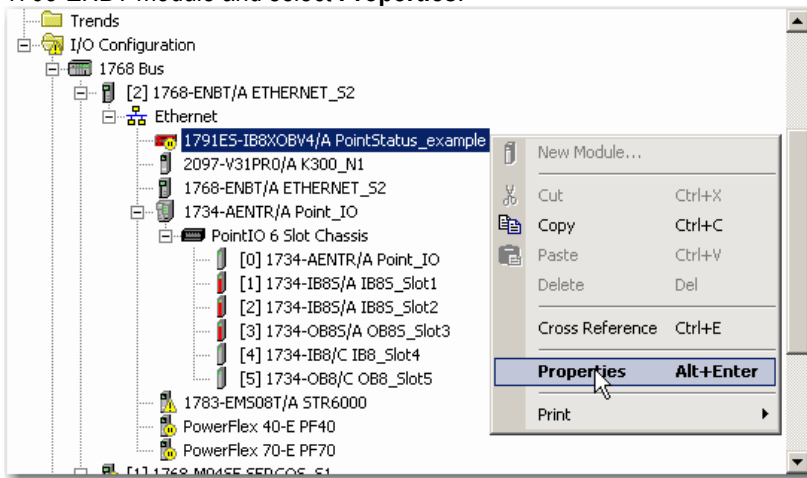
4. Close the **R02_SafetyIndicators** routine.

Safety Configuration Management

In a GuardLogix safety system, all safety I/O is distributed on either a DeviceNet or EtherNet/IP network. Safety I/O comes in either a block or point form factor. The Compact GuardLogix safety controller owns the configuration of every safety I/O module in the system. All the configuration of Safety I/O modules is handled within the I/O Configuration tree of RSLogix5000.

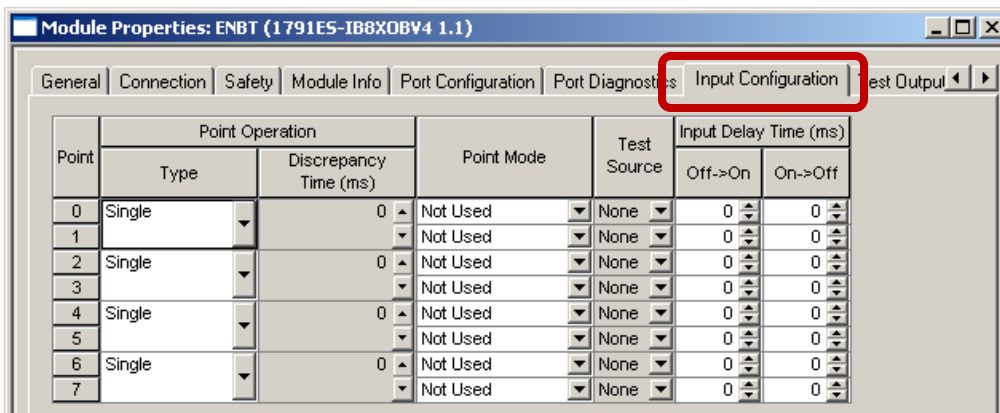
Since the I/O profiles store the configuration data, a safety I/O module can be replaced with a module off the shelf and the configuration will automatically be pushed down (unless you configure the application not to).

1. If it is not already open, open the **CMSS_Core_Demo.acd** file.
2. In the I/O Configuration tree, right-click the **1791ES-IB8XOBV4 PointStatus_Example** module profile under the 1768-ENBT module and select **Properties**.



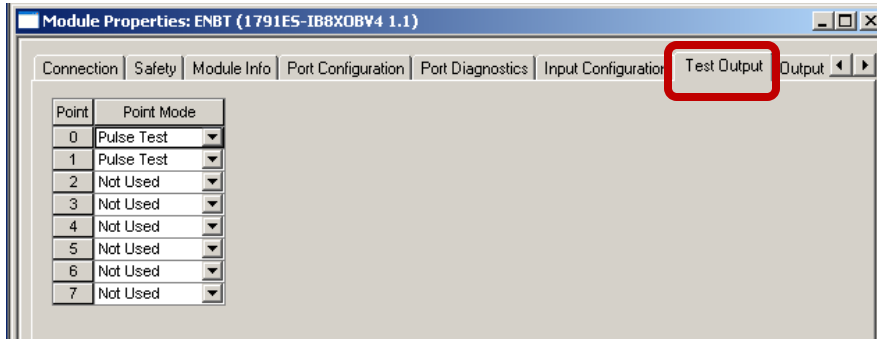
All the configuration of Safety I/O modules is handled within the I/O Configuration tree of RSLogix5000.

3. Select the Input Configuration tab:



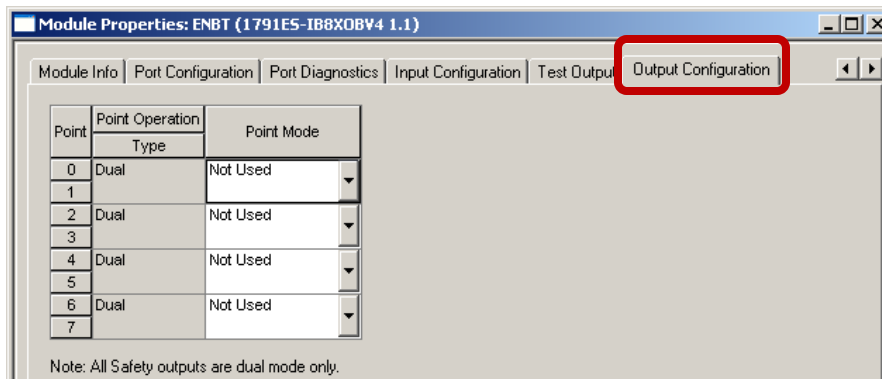
This profile includes the configuration of safety inputs, safety outputs, and test outputs. On this screen you configure the behavior of the input points on the module.

4. Select the Test Output tab:



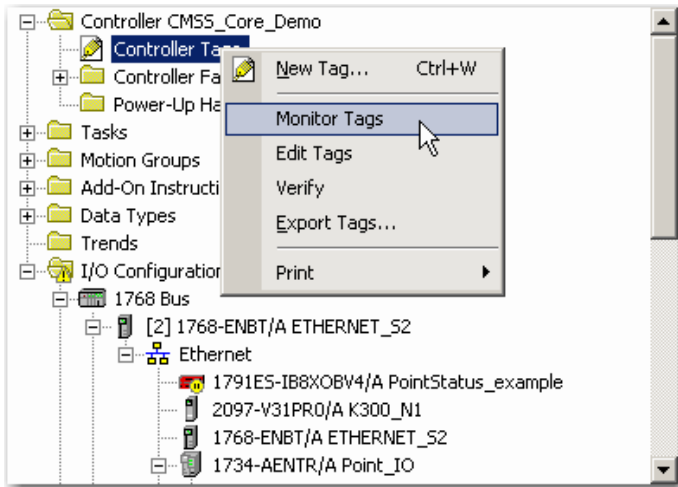
Test outputs are used to pulse test the safety inputs to detect wiring faults. This screen allows you to configure the behavior of the test outputs points.

5. Select the Output Configuration tab:

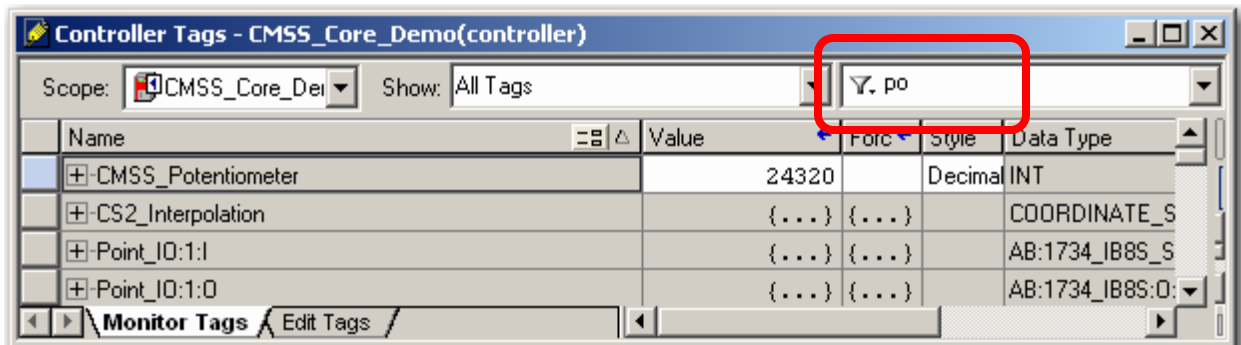


This is the screen where the output behaviors are defined.

6. Click **OK**.
7. Right click on **Controller Tags** in the Controller Organizer and select **Monitor Tags**.



8. Enter **po** in the tag filter:



- Expand the tag **PointStatus_example:I** to view all the tags created for this safety I/O module:

Name	Value	Forc	Style	Data Type	Class	Description
PointStatus_example:I	{...}	{...}		AB:1791ES_IB&XDB8_Safety3:I:0	Safety	
PointStatus_example:I.BurnCode	0		Decimal	BOOL	Safety	
PointStatus_example:I.ConnectionFaulted	1		Decimal	BOOL	Safety	
PointStatus_example:I.Pt00Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt01Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt02Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt03Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt04Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt05Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt06Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt07Data	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt00InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt01InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt02InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt03InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt04InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt05InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt06InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt07InputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt00OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt01OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt02OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt03OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt04OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt05OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt06OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Pt07OutputStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.Muting03Status	0		Decimal	BOOL	Safety	
PointStatus_example:I.Muting07Status	0		Decimal	BOOL	Safety	
PointStatus_example:I.OutputPowerStatus	0		Decimal	BOOL	Safety	
PointStatus_example:I.InputPowerStatus	0		Decimal	BOOL	Safety	

After the safety IO module is configured, the appropriate safety class tags are generated. The input tags for this combo I/O module include input data and varied status tags.

For DeviceNet Safety I/O modules, this means there is no I/O mapping or scanlist configuration needed as there is with standard DeviceNet nodes. All configurations of the safety modules are handled in RSLogix 5000, eliminating the need for RSNetWorx for DeviceNet software.

- Close the Controller tag window.

Ease of Use – Safety-Related Code

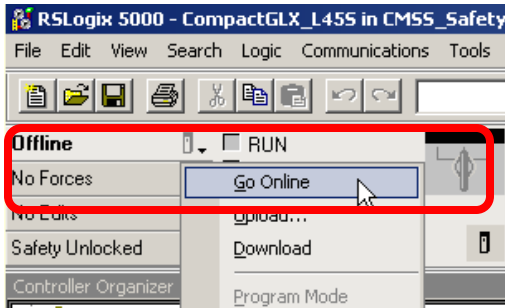
If you write bad safety code, the end result could be a dangerous machine. Writing simple, easy-to-understand safety code that has been tested and validated is imperative when using a safety PLC.

Fortunately, writing safety code in a GuardLogix controller is simple. You are likely already familiar with the Logix5000 editor. Logix5000 has certified Safety instructions that monitor and control safety devices so you don't have to write your own. Typically code that turns things OFF is much simpler than the code that runs the machine/process. Turning things OFF is easy. Turning things ON is hard.

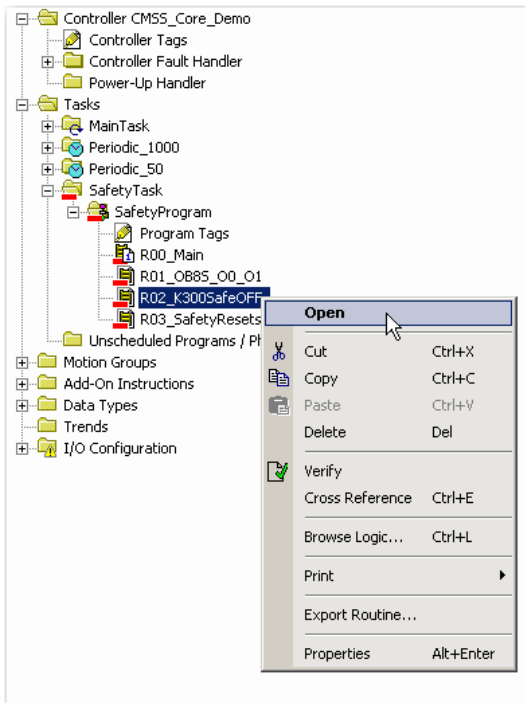
The most critical aspects of proper safety code include the following:

- Make sure that a manual action is required to restart.
- Make sure the outputs go to the safe state (logically LO) when any of the interlocks are inactive.
- Make sure it is clear and legible.

1. If it is not already open, open the **CMSS_Core_Demo.acd** file and
2. Go online with the controller:



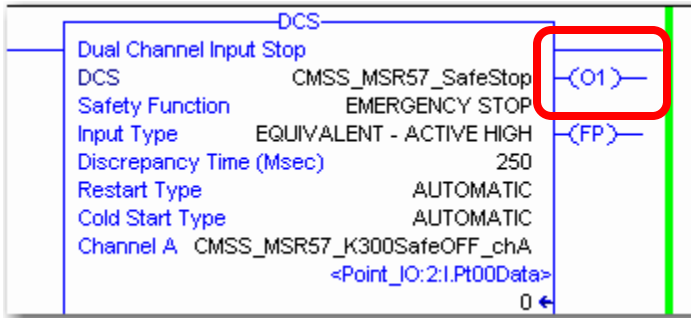
3. Call up the safety routine named **R02_K300SafeOFF**:



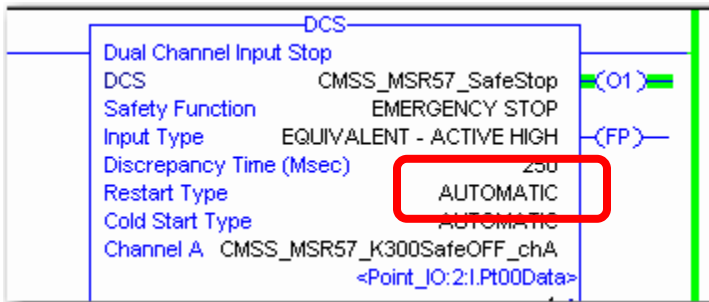
There is a set of instructions designed specifically to control safety functions. In the K300 safety routine, two of them are used, the DCS and the CROUT.

DCS stands for Dual Channel Stop. This instruction monitors the Emergency Stop button labeled Safe Stop and controls its O1 output accordingly.

4. Press the Safe OFF button (top E-Stop button) and note that the DCS output in rung 0 goes LO:



5. Pull the Safe OFF back out; the DCS output goes HI due to the AUTOMATIC restart parameter:



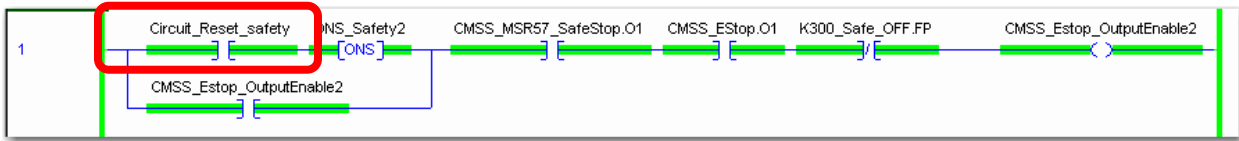
The DCS output tracks the device because it is configured for AUTOMATIC restart.

Question: What instruction would you use if your safety device was single channel?

The answer is an XIC (Examine ON). The DCS and the rest of the new safety instructions are used with Dual channel devices. They ensure that the dual channels are in sync. If your safety system is single channel, you just use the Boolean instructions.

Manual Reset

6. Press the green reset pushbutton [note that **Circuit_Reset_safety** input goes HI]:

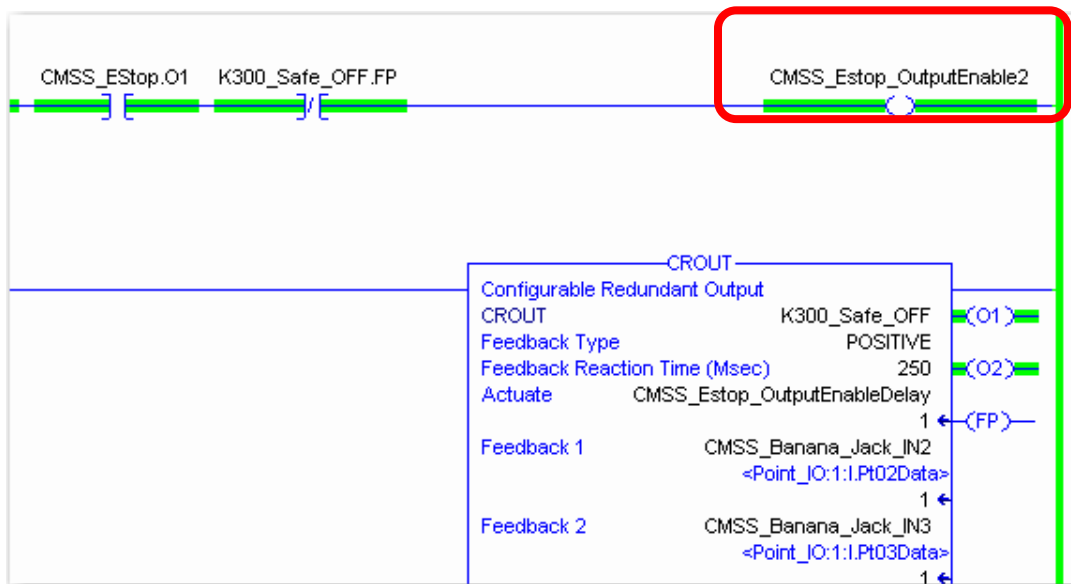


When the Safe OFF was pressed, the **CMSS_MSR57_SafeStop.O1** tag dropped out the safety output in rung 1. When you pulled out the Safe OFF, the motor did not restart even though the DCS output went HI automatically. Safety standards typically require that the machine does not restart automatically when the guard returns to the active state. To meet this requirement, a simple interlock rung is used. A simple seal-in and ONS instruction ensure that the output enable not return HI unless there is a LO to HI transition of the Circuit Reset.

7. Press the flashing yellow button to start drive motion.

Safety Output Interlocks

The **CMSS_Estop_OutputEnable2** tag drives the actuate parameter in the CROUT instruction:



The **output_enable2** tag is used to provide actuate for the CROUT instruction. The CROUT instruction does the same thing as a safety relay. If actuate drives the CROUT outputs HI, the positive feedback (In this example) requires the feedback to follow within 250ms.

Right now everything on the CROUT should be HI, the internal tags and the two outputs; O1 and O2.

8. Press the Safe OFF button and observe that actuate goes LO.

This drops out the outputs, which in turn causes the feedback to follow LO. The outputs of the CROUT instruction control the physical safety output(s) within your zone. The physical outputs of our zone in this demo case are the K300 Safe Torque OFFs. Note that the K300 status light, which monitors the Safe Torque OFF inputs, is de-energized.

The code that determines if the safety inputs are OK may be more complicated than shown here, but controlling the safety outputs is normally this simple.

The delay gives the K300 drive time to drop its safety enable signal before the CROUT drops the K300 Safe OFF inputs. This generates a STOP versus an ABORT when Safe OFF is pressed.

9. Pull the Safe Off push button back out.

10. Press the flashing green circuit reset button.

The safety circuit has been reset, the CROUT outputs are energized, and the K300 status light is energized because the K300 Safe Torque OFFs are now HI.

11. Press the flashing yellow button.

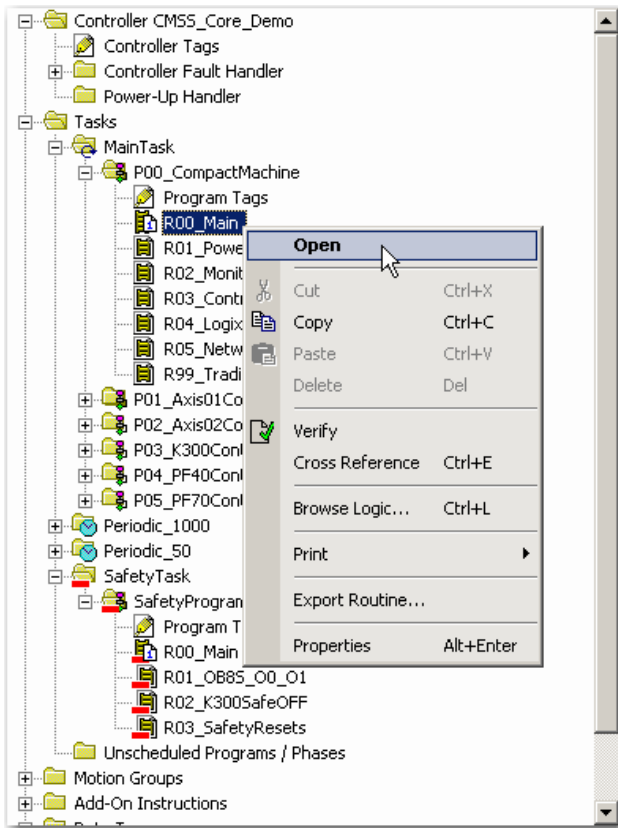
You can likely hear that the motor is energized, but motion start is required before the motor will spin. Safety and motion are separate functions. Circuit reset energizes the safety outputs, but that has no affect on whether or not motion is allowed to start.

12. Close the **R02_K300SafeOFF** routine.

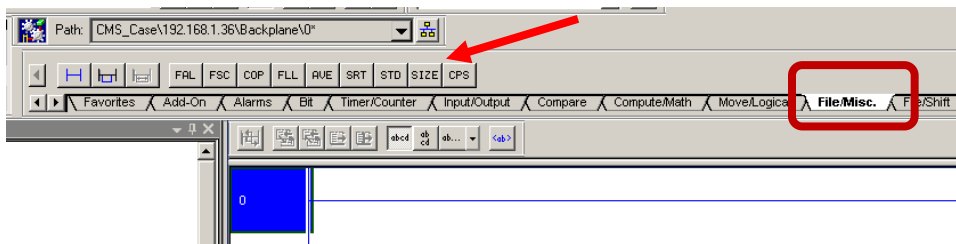
Certified Safety Instructions

Over 50 certified safety instructions are available for use within the safety task. This is a subset of the total instruction list available in RSLogix 5000. A core safety principle is to keep safety code as simple as possible. The certified instructions help keep the code simple. Complex math and program control instructions are unavailable in the safety task due to the complexity they could inject into the safety code.

1. Open the **R00_Main** standard routine within the **P00_CompactMachine** program.

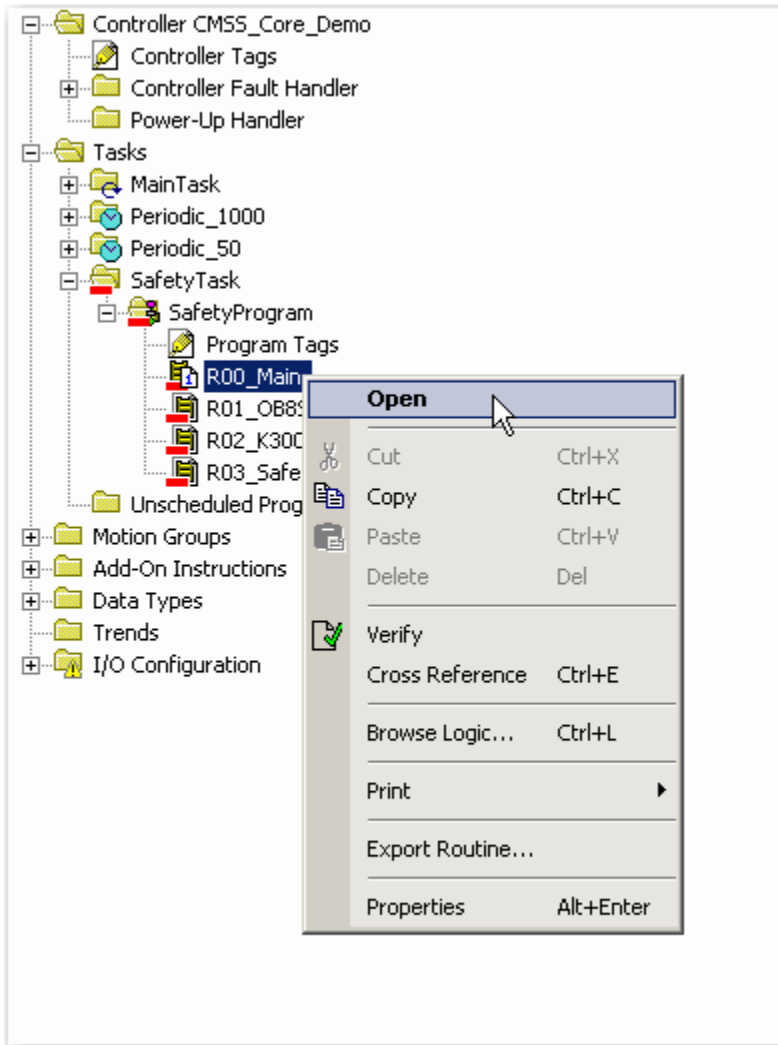


2. On the **Language Elements** toolbar, select the **File/Misc.** tab.

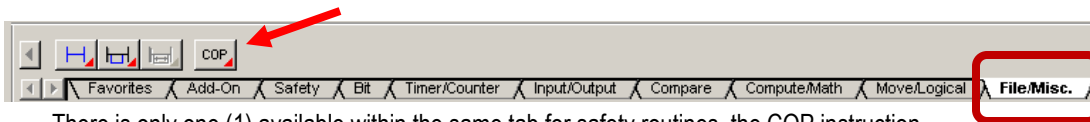


For example, there are nine (9) instructions available within the File/Misc tab for standard routines.

3. Close the **R00_Main** standard routine.
4. Open the **R00_Main safety** routine in the SafetyTask



5. On the **Language Elements** toolbar, select the **File/Misc.** tab.



6. Close the **R00_Main** routine.

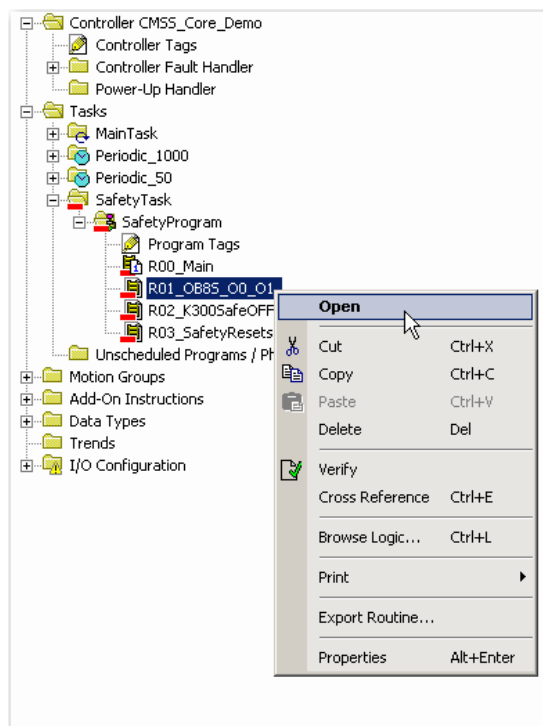
Safety Input Instructions

Under the safety tab, you will see a set of instructions developed to control specific safety functions. We will begin by focusing on the safety input instructions. The base instruction is DCS (Dual Channel Input Stop) is typically used for devices that STOP safety outputs, for example, an Emergency Stop button.

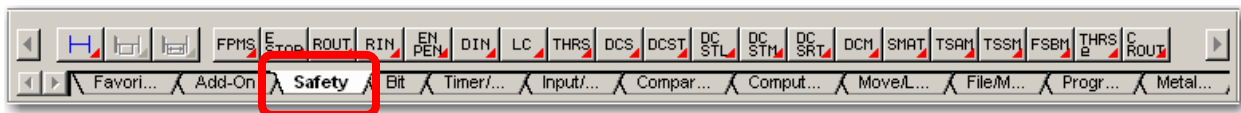
To summarize, the DCS instruction monitors dual channel devices and sets the output when both channels are in the active state (HI), and proper restart actions are completed. If the channels are not equivalent for longer than the discrepancy time, a fault is declared.

Many of the other safety input instructions simply build on this base functionality.

1. Open the **R01_OB8S_00_01** routine in the Safety Task:



2. Select the Safety tab on the language elements toolbar:

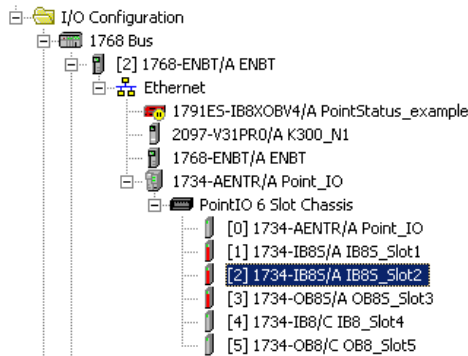


Under the safety tab, you will see a set of instructions developed to control specific safety functions. We will begin by focusing on the safety input instructions. The base instruction is DCS (Dual Channel Input Stop). It is typically used for devices that STOP safety outputs, for example, an Emergency Stop button.

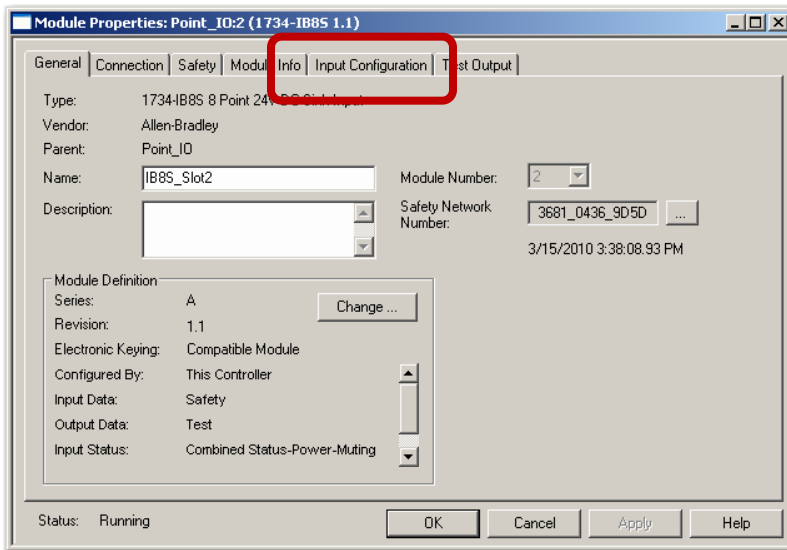
3. If not already online, In the Online toolbar, change the controller mode to Online by selecting **Go Online**.



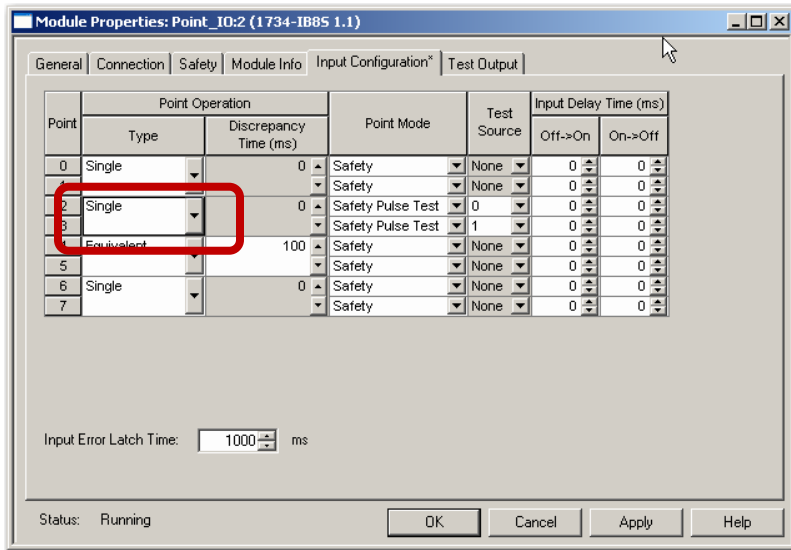
4. Select **Yes** to any prompts.
5. Open the **1734-IB8S_Slot2** Properties dialog box.



6. Select the **Input Configuration** tab:

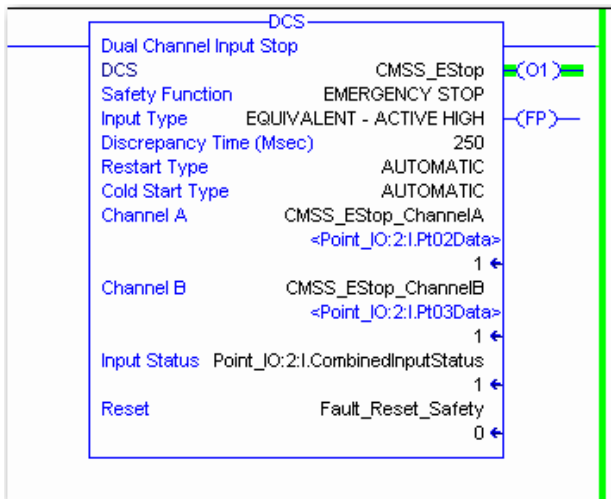


- From the Input Configuration tab change the Point Operation for input channels 2 and 3 to single-channel mode.

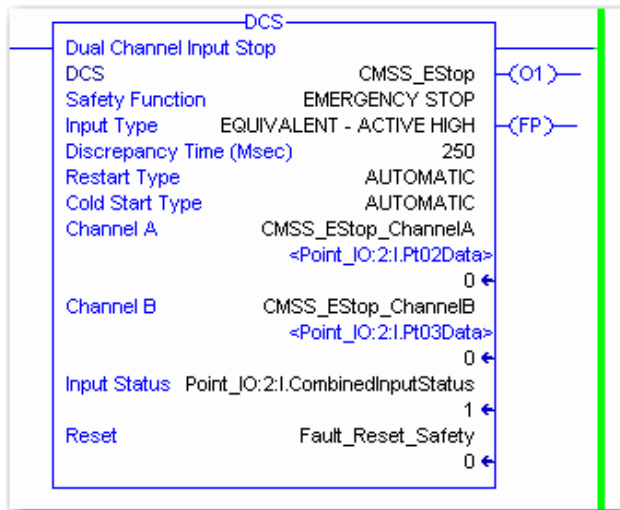


To show the features of this instruction, we need to change the configuration of the EStop channel pair from Equivalent to Single. This allows the DCS instruction to check for discrepancy rather than the safety IO module.

- Click **Apply** > **Yes** > **Yes** at the prompts
- Press **OK** to close the Module Properties dialog box
- Cycle the flashing red selector switch on the demo case
- Locate the DCS instruction on rung 0.



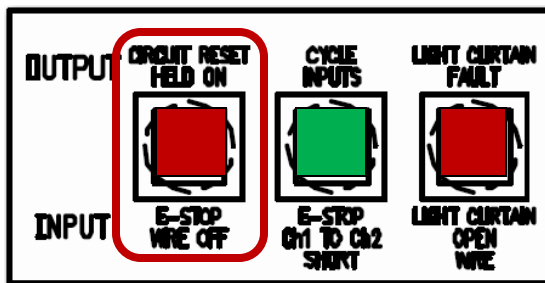
- Press the EStop labeled **Emergency Stop** (lower) on the demo case.



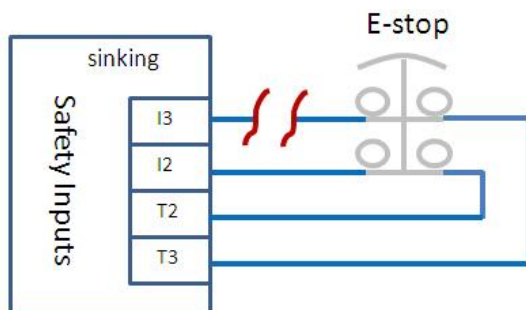
- Release the lower Emergency stop button on the demo case.

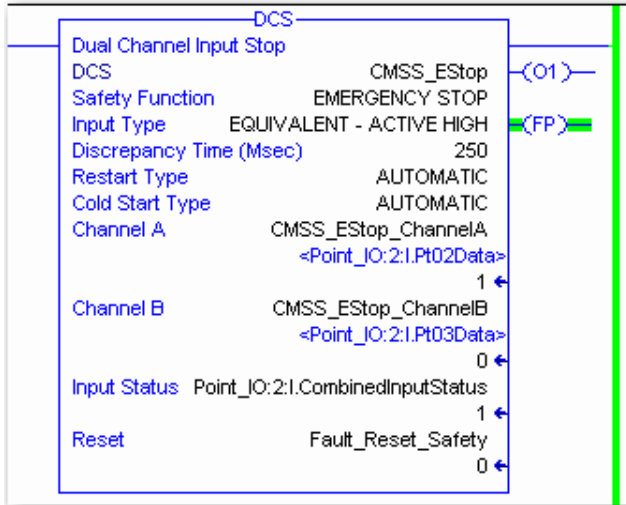
When you cycle the Emergency Stop button on the demo case, notice that the output O1 simply follows the state of the button.

- To simulate a discrepancy fault, press the **E-STOP WIRE OFF** button on the demo case:



Channel B of the Emergency Stop button drops out (input 3 on the IB8S in slot 2):





The channels are now diverse, and if they remain diverse until the 3 second discrepancy timer expires, the DCS declares a fault.

15. Release the **E-STOP WIRE OFF** button on the demo case.
16. Cycle the flashing red selector switch to reset the fault on the DCS instruction.
The fault remains until the wire OFF is repaired, and the fault reset is cycled.

17. Cycle the Emergency Stop button (flashing).

Notice that the DCS output O1 does not go HI until the Emergency Stop button is cycled to prove that the fault has been fixed.

To summarize, the DCS instruction monitors dual channel devices and sets the output when both channels are in the active state (HI), and proper restart actions are completed. If the channels are not equivalent for longer than the discrepancy time, a fault is declared.

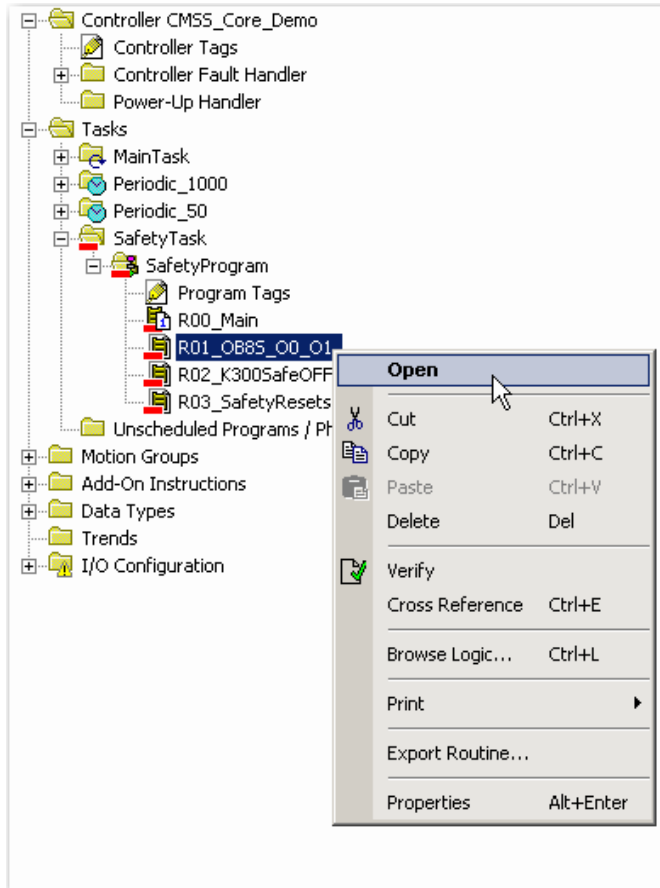
Many of the other safety input instructions simply build onto this base functionality.

18. Go back to the **IB8S_Slot2** and configure inputs 2 and 3 as Equivalent. Verify that the discrepancy time is configured for 3000ms.
19. Click **Apply > Yes > Yes** at the prompts.
20. Close the **IB8S_Slot 2** module properties window using **OK**.
21. Cycle the flashing red fault reset selector switch.

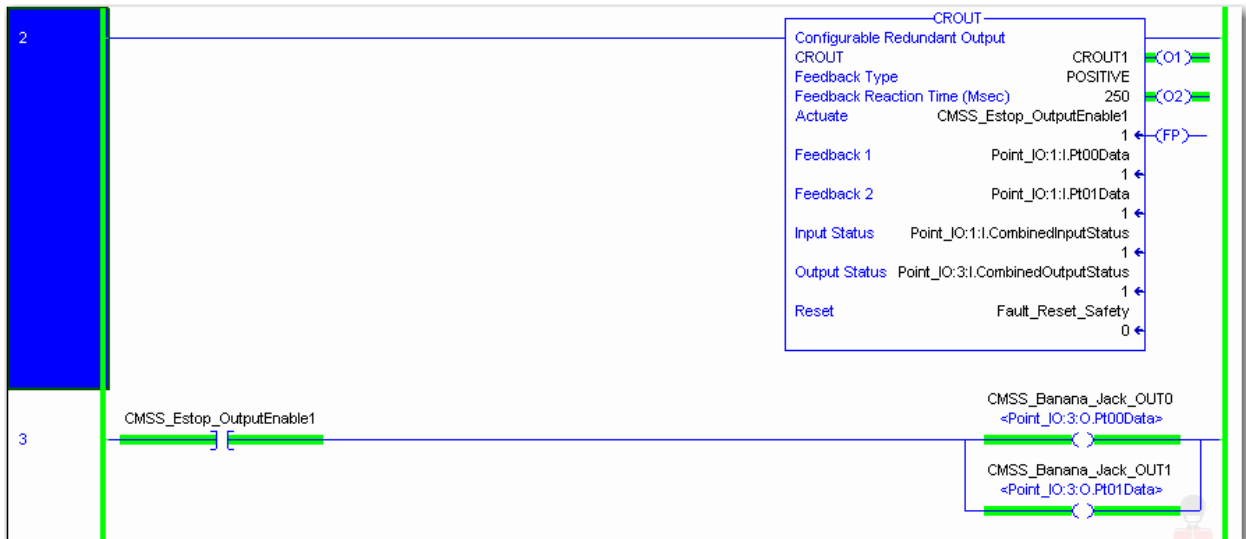
Safety Output Instructions CROUT

There actually is only one (1) safety output instruction, **CROUT**. That is because as far as the controller is concerned, it simply energizes two (2) outputs and monitors feedback. That happens to be exactly what safety relays do as well. Essentially, the CROUT has the same functionality as a safety relay. When the outputs are commanded HI the feedback is expected to follow within a configurable reaction time. If the feedback ever switches unexpectedly, the CROUT instruction faults.

1. If not already open, open the **R01_OB8S_00_01** safety routine:

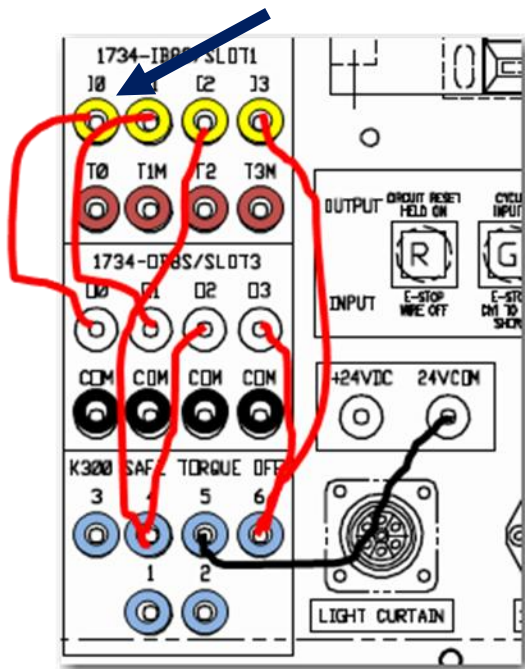


2. Scroll to rung 2 where the CROUT instruction is located.
3. Press the flashing green fault reset button to energize the safety outputs.



This CROUT instruction is being used to drive Safety Outputs O0 and O1 on the white banana jacks. We have already connected cables from those outputs to safety inputs I0 and I1 on the yellow banana jacks. These are the feedback signals for the CROUT. Since the instruction is configured for POSITIVE feedback, the feedback is LO when the outputs are LO and HI when the outputs are HI.

4. Pull off the banana jack cable going to I0 on the 1734-IB8S module to simulate a feedback fault.



If either of the feedback signals unexpectedly drops out, the CROUT will fault. Why did Feedback 2 also go LO? Because when the instruction faulted, the outputs were dropped out. This causes both feedback channels to drop out as well. In summary, the CROUT instruction duplicates the safety functions of a safety relay, controlling dual outputs and monitoring up to two (2) feedback channels.

5. Re-attach the banana jack cable to I0.
6. Cycle the red fault reset to clear the fault.
7. Press the green circuit reset button to turn the CROUT outputs back on.
8. Press the flashing yellow button to start drive motion.
9. Close the **R01_OB8S_O0_O1** routine.

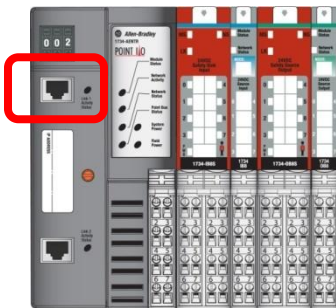
Safety Performance without Sacrificing Productivity through Diagnostics

In this section you will learn about the diagnostic features of a GuardLogix safety system that will keep your safety system up and running.

CIP Safety Diagnostics

CIP safety connections are between the safety controller (CompactGuardLogix) and safety IO modules (PointGuard). The status of each safety connection is a 'ConnectionFaulted' tag that can be easily monitored by your code and displayed on an HMI for your maintenance personnel.

1. Pull the Ethernet cable out of the 1734-AENT:



Pulling the Ethernet cable breaks all three safety IO connections.

2. On the PanelView Plus, select 'IB8S-Slot1' by pressing on the point icon below the text (circled below):



Each of the three safety IO faceplates indicates a fault.

3. Select the yellow flashing alarm bell:



The error is a connection Fault.

4. Select the [?] on the right hand side of the menu bar.



The probable cause is that the safety connection between GuardLogix controller and module has been broken.

5. Re-insert the Ethernet cable (top port).

When the cable is re-inserted, notice that the motor does not restart automatically.

Information: After the CIP safety connection is re-established (be patient, the red fault reset switch will start flashing when the connection is re-established), the connection faults clear on the faceplate(s)

6. Close the 1734-IB8S slot 1 window:



7. Cycle the red flashing selector switch.

All the faults clear. The only remaining issue on the HMI is 1734-IB8S slot 2. It is flashing because demand reset is required to clear demands on this faceplate. Select this faceplate and press 'demand reset' if you want to clear this indication.

8. Press the Flashing green fault reset button to restart the motor.

9. Press the flashing yellow button to start motion

A manual reset is required to restart the motor because the safety output interlocks were logically dropped out due to this fault.

Safety Input Diagnostics

From a safety perspective, it is critical that a safety input operates properly when a demand is placed on it. This is typically accomplished using redundancy and diagnostics. Redundant channels allow you to tolerate a single fault, and diagnostics allow you to detect that fault and keep your machine from restarting with that fault.

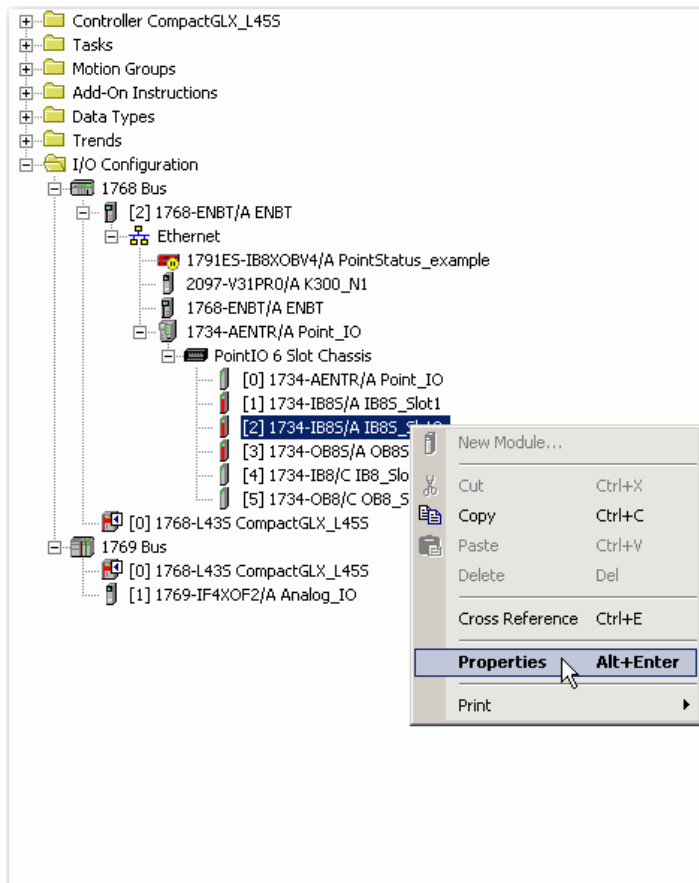
Traditional safety systems consist of a safety relay with multiple safety input devices wired in series. There is little wrong with this from a safety standpoint because a safety relay has redundancy and diagnostics, but it leaves much to be desired from a monitoring standpoint, which can adversely affect availability.

Many customers add a third contact and wire that back to a PLC so they know which safety device has a demand placed on it. But the third contact does nothing to help in the event of an actual wiring or device fault.

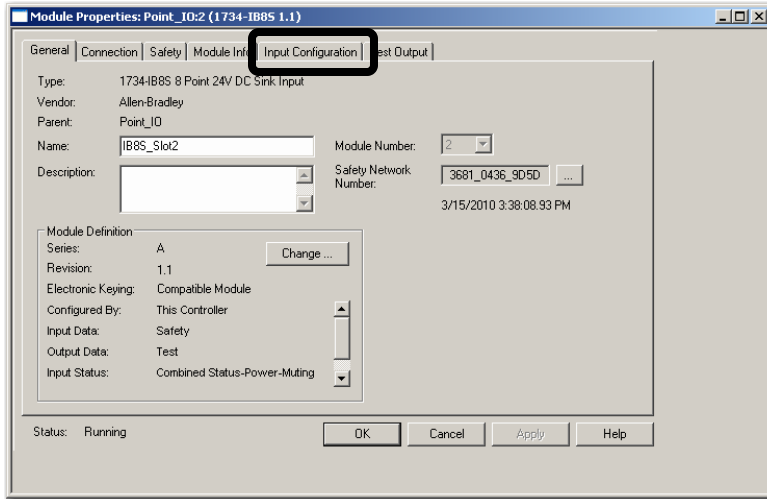
By wiring each individual safety input to a separate input channel in the traditional PLC fashion, you can provide granular diagnostics for your operators and maintenance personnel. If the machine stops, HMIs can instantly direct maintenance personnel to the proper device, reducing MTTR (Mean Time to Repair).

Safety Input Diagnostics when configured for Single Channel

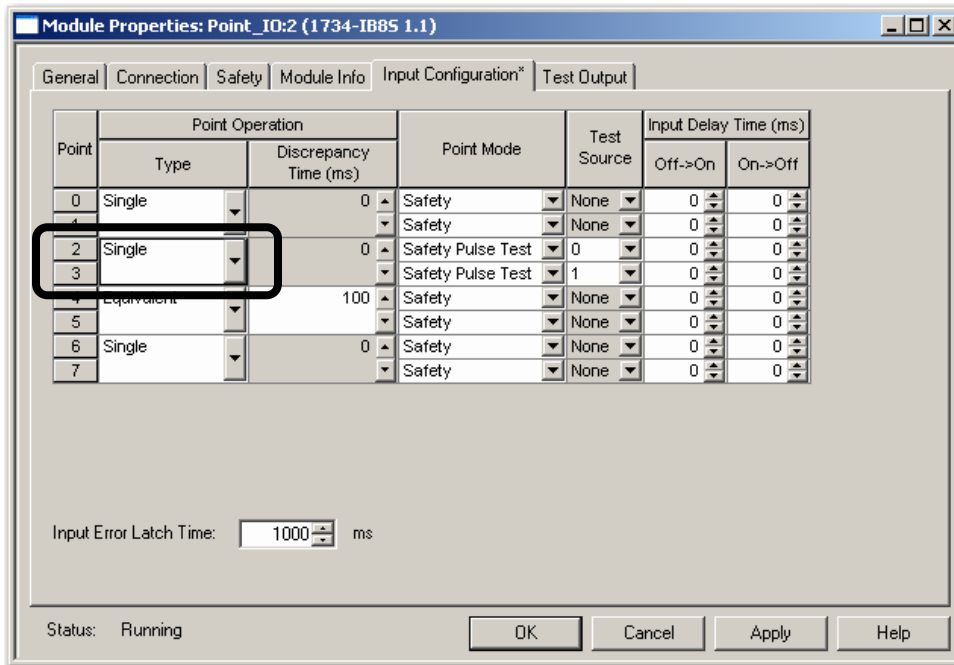
1. Within RSLogix 5000 software, right click on the 1734-IB8S in slot 2 and select *Properties*:



2. Select the *Input Configuration* tab (circled below)



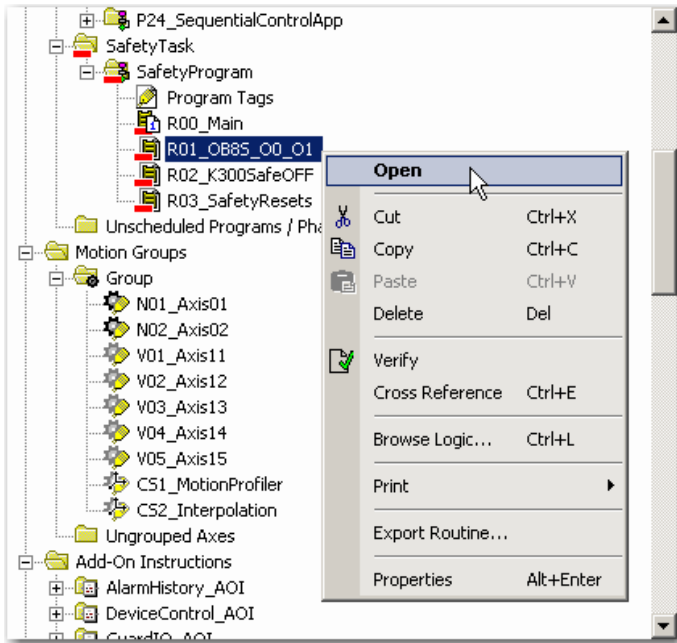
3. Change channels 2/3 to Single (as circled below)



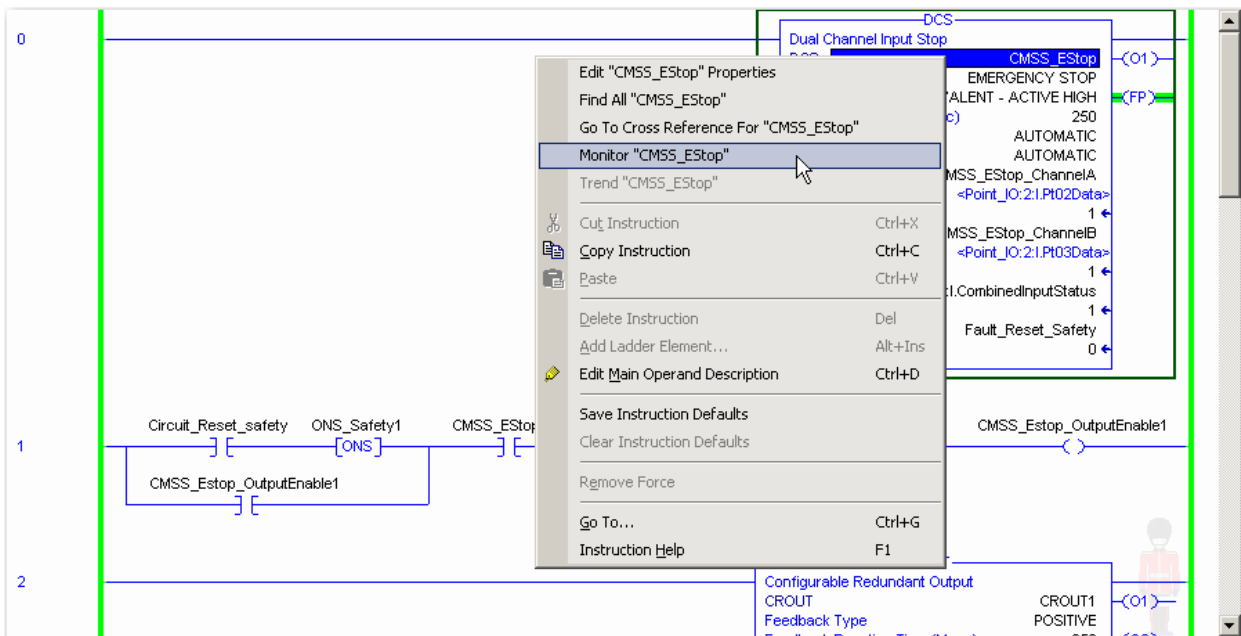
Once configured for single channel, discrepancy faults can be detected by the certified dual channel safety instructions that make it easy to diagnose and annunciate fault(s) on your HMI.

4. Click **Apply** > **Yes** > **Yes** at the prompts.

5. Right-click **R01_OB8S_O0_01** in the safety task and select **Open**.

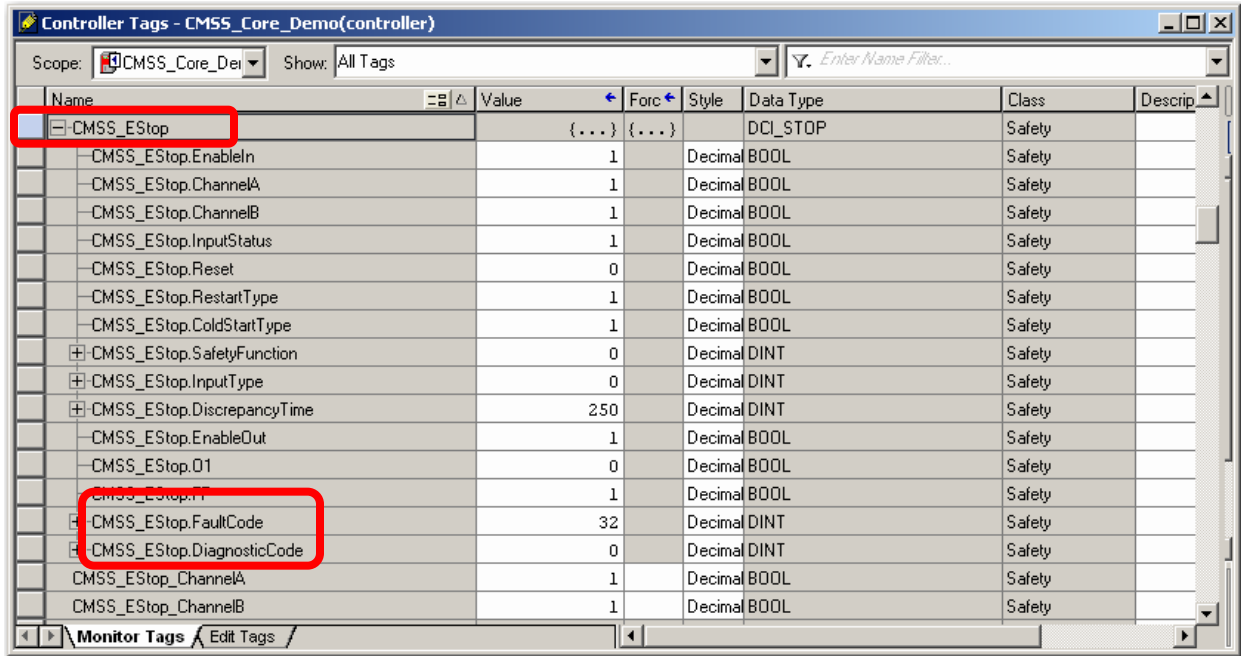


6. Right click on the tag **CMSS_EStop** in the DCS instruction on rung 0, and Select **Monitor CMSS_EStop**



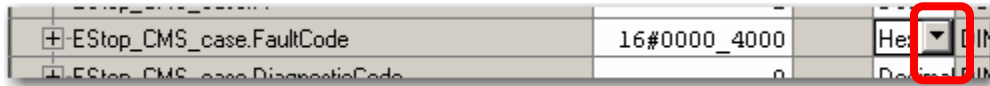
The instruction used to monitor the Emergency Stop button is a DCS, Dual Channel Stop.

- Expand tag **CMSS_EStop** (this is the first tag in the list):



These instructions have predefined tags that include fault codes and a FP (Fault Present) status bit. No explicit messaging is required to obtain these fault codes.

- Locate the tag called **CMSS_EStop.FaultCode** and change the style to HEX. Click on the window circled below and select Hex from the pulldown.

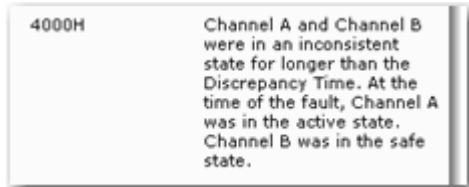


You are going to monitor the fault code tag within this DCS instruction. The fault codes in the user's manual are shown in Hex.

- Cycle red selector switch so that the motor is running with no faults.
- Press flashing green reset button to reset the fault code.

11. EStop wire OFF to generate a **discrepancy fault**

When the E-Stop wire off button is pressed, the normally dual equivalent channels go to diverse states; one HI and one LO. The safety system stops the motor because one of the E-Stop channels went LO. Note that this is the same condition that would occur if there was a short around one of the contacts when a demand is placed on the device. The discrepancy fault code 4000h indicates precisely that channel A was HI while channel B was LO, which is correct since the wire OFF affects channel B.



12. Press the Flashing red EStop DCS icon on the HMI:



13. Press the Fault button on the bottom of the HMI screen:



The DCS instruction faceplate for the Emergency Stop button provides the same information to the operator. It provides the exact description of the 4000h code as found in the user's manual.

14. Close the instruction faceplate on the HMI using the [X] in the top right corner.

15. Press EStop wire OFF button again to fix the fault.

When the wire off is fixed, the channels both return to HI and are equivalent. But the safety system will not allow the motor to restart because it assumes one of the contacts still has a short around it.

16. Cycle flashing red fault reset switch to clear the fault code.

17. Cycle the Emergency Stop button (flashing).

You must prove that the short around the contact has been fixed by cycling the safety input through the safe state; which occurs when both channels go LO.

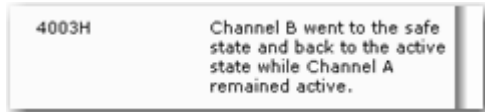
18. Press flashing green circuit reset button to restart the safety outputs.

Then the safety system will allow you to restart the motor. Note that the 1734-IB8S module in slot 2 detected no faults during this procedure. All it knows is that channel 3 went LO.

19. Press the EStop Wire OFF button (note it is a maintained button).

20. Press the EStop Wire OFF button again within 3 seconds to generate a **Channel Cycled fault**.

The Channel cycle fault code 4003h indicates precisely that channel B cycled while channel A was steady. Recall the wire off button affects channel B of the Emergency Stop button.



21. Press the Flashing red EStop DCS icon on the HMI:



22. Press the Fault button on the bottom of the HMI screen:



The DCS instruction faceplate for the Emergency Stop button indicates that there is a channel cycle fault as well. Note that it provides the exact description of the 4003h code as found in the user's manual. Again, note that the 1734-IB8S module in slot 2 detected no faults during this procedure. All it knows is that channel 3 went LO and then back HI.

23. Close the instruction faceplate on the HMI using the [X] in the top right corner.

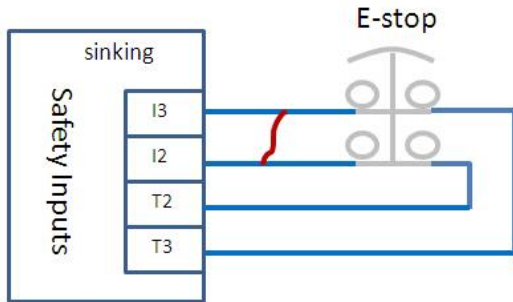
24. Cycle the flashing red selector switch to clear the fault code.

25. Cycle the Emergency Stop button (flashing).

26. Press the flashing green reset PB .

27. Press ch-ch short button to create a **pulse test fault**.

When the pulse test fault occurs, the safety I/O module does detect this fault because pulse testing is h/w f/w based within the module itself. When the *EStop ch1 to ch2 short* button is pressed, a short is created between the two channels (channel 2 & 3 in slot2).



This fault is detected by the next pulse test. The EStop channel LEDs 2 and 3 are solid red, indicating a fault.

28. Press the 1734-IB8S slot2 image on the HMI screen to call up the 1734-IB8S faceplate.



29. Press the flashing yellow alarm bell on the HMI screen.



The HMI indicates 'External Test Signal Error', which means the pulse test detected the fault.

30. Select the [?] on the right hand side of the menu bar.



The second probable cause, a channel-to-channel short (short circuit between input signal lines) matches the actual fault.

31. Close the IB8S window on the HMI.

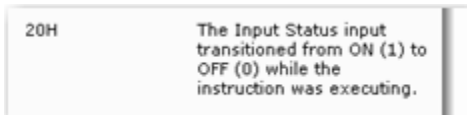
32. Press the Flashing red EStop DCS icon on the HMI.



33. Press the Fault button on the bottom of the HMI screen:



The DCS instruction, on the other hand, monitored the input channel status bit(s) of the 1734-IB8S module and declared a fault of 20h because this bit unexpectedly changed during normal execution.



34. Close the instruction faceplate on the HMI using the [X] in the top right corner.

35. Press ch-ch short button again to fix the fault.

36. Cycle the Emergency Stop button (flashing).

To recover from this fault, the safety IO module must sense the input channels in the safe state; both LO. This will require a cycle of the EStop button after the wiring fault has been fixed.

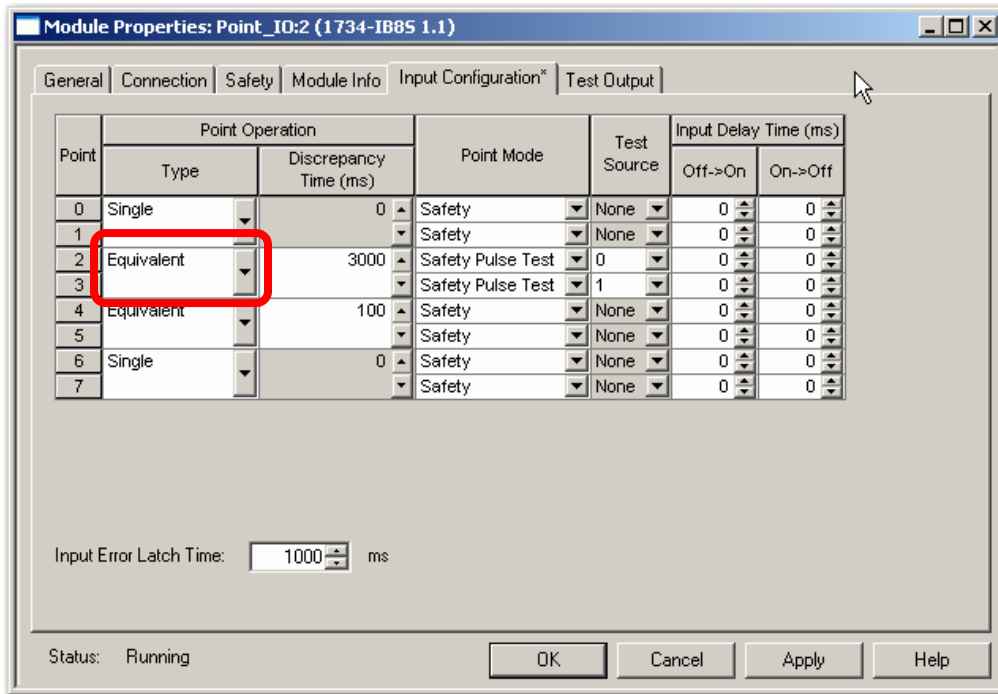
37. Cycle red flashing circuit reset button.

38. Press flashing green fault reset button.

39. Close the Controller Tags window using [x] in top right corner of window.

40. Close the safety task **R01_OB8S_00_01** using the [x] in the top tight corner of the window.

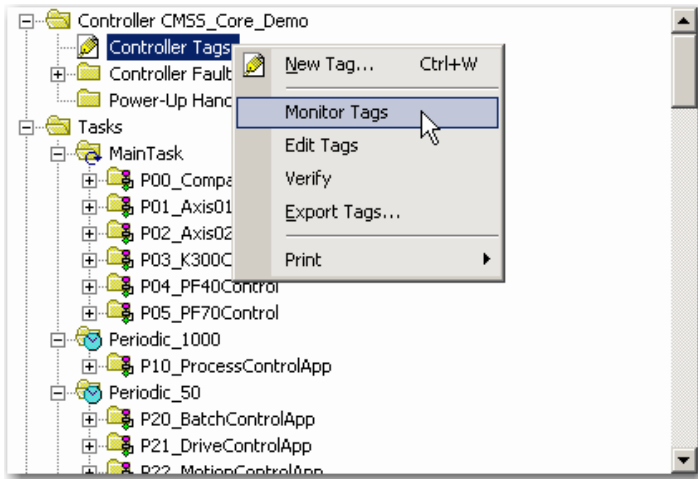
41. Change Input Configuration for channels 2 & 3 back to Equivalent. Verify that the discrepancy time is set for 3000ms.



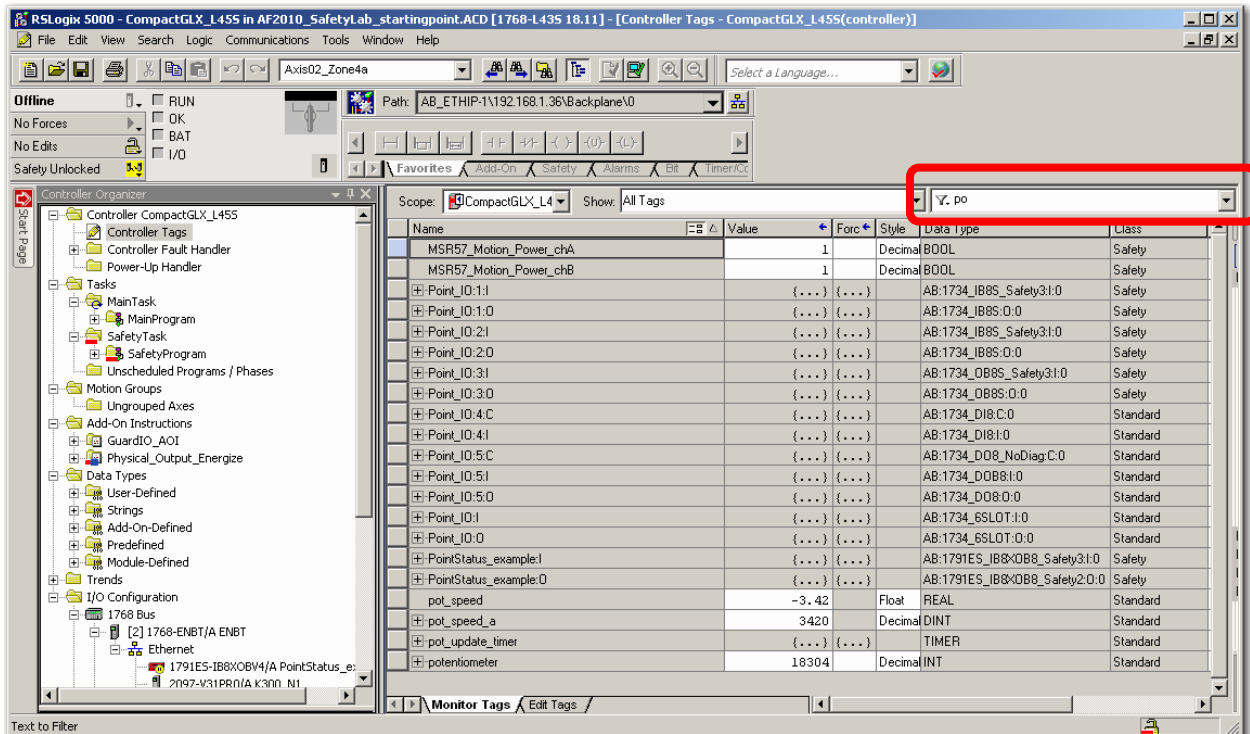
42. Click **Apply** > **Yes** > **Yes** at the prompts.
43. Close the 1734-IB8S Module Properties window using **OK**.
44. Cycle red flashing fault reset button.
45. Press the flashing green button.
46. Press the flashing yellow button.

Fault detection when configured for Dual Channel

1. Within RSLogix 5000 software, right click on *Controller Tags* and select *Monitor Tags*:



2. Enter 'po' in the filter (circled below):



3. Expand *Point_IO:2:I* (5th tag in the list):

	MSR57_Motion_Power_chA	1		Decimal	BOOL	Safety
	MSR57_Motion_Power_chB	1		Decimal	BOOL	Safety
	⊕ Point_IO:1:I	{...}	{...}		AB:1734_IB8S...	Safety
	⊖ Point_IO:1:O	{...}	{...}		AB:1734_IB8S...	Safety
	⊖ Point_IO:2:I	{...}	{...}		AB:1734_IB8S...	Safety
	Point_IO:2:I.RunMode	1		Decimal	BOOL	Safety
	Point_IO:2:I.ConnectionFaulted	0		Decimal	BOOL	Safety
	Point_IO:2:I.Pt00Data	1		Decimal	BOOL	Safety
	Point_IO:2:I.Pt01Data	1		Decimal	BOOL	Safety
	Point_IO:2:I.Pt02Data	1		Decimal	BOOL	Safety
	Point_IO:2:I.Pt03Data	1		Decimal	BOOL	Safety
	Point_IO:2:I.Pt04Data	0		Decimal	BOOL	Safety
	Point_IO:2:I.Pt05Data	0		Decimal	BOOL	Safety
	Point_IO:2:I.Pt06Data	0		Decimal	BOOL	Safety
	Point_IO:2:I.Pt07Data	0		Decimal	BOOL	Safety
	Point_IO:2:I.Muting01Status	1		Decimal	BOOL	Safety
	Point_IO:2:I.Muting03Status	1		Decimal	BOOL	Safety
	Point_IO:2:I.InputPowerStatus	0		Decimal	BOOL	Safety
	Point_IO:2:I.CombinedInputStatus	1		Decimal	BOOL	Safety

When configured for dual channel, the module detects all faults and updates the combined (or Point) status bit(s) implicitly to inform us that there is a fault somewhere in the safety system. The combined status bit points your operator to the correct module.

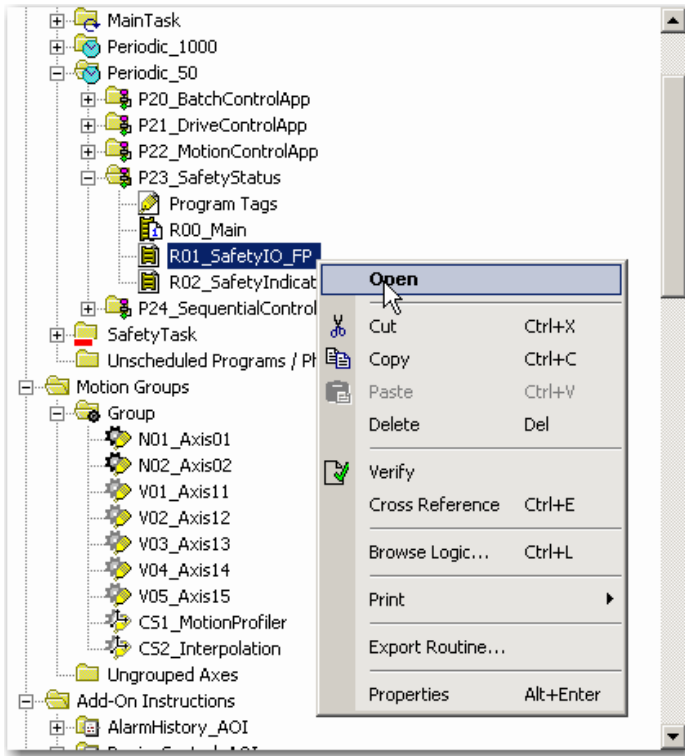
4. Push EStop wire OFF button on demo case to generate a discrepancy fault.

A low combined Input Status bit indicates at least one input channel on the PointGuard module in slot 2 is faulted. Looking at the LEDs on the module backs this up. Channels 2 and 3 in slot 2 are red. This status bit can be used to trigger explicit messages to get the actual fault codes for each channel in slot 2. This enables us to reduce the amount of implicit data traffic, and only explicitly request fault codes when a fault actually exists.

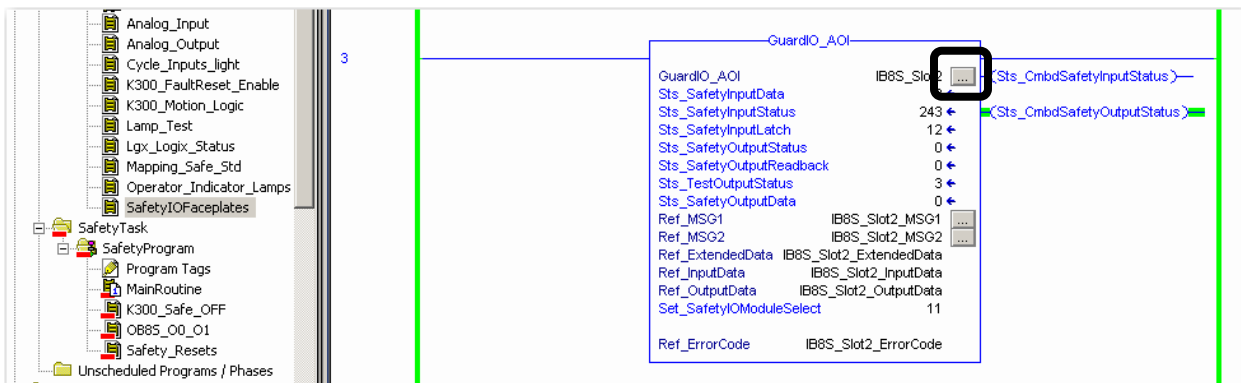
The message instruction(s) are within the GuardLogix Safety Accelerator AOIs that provide the data that drives the faceplates shown on the HMI. These AOIs and faceplates are available for download on the sample code site.

When the EStop wire OFF is pressed, both LEDs on channels 2/3 of 1734-IB8S in slot 2 go LO immediately, but only after the 3 second discrepancy time is a fault declared and the LEDs turn RED.

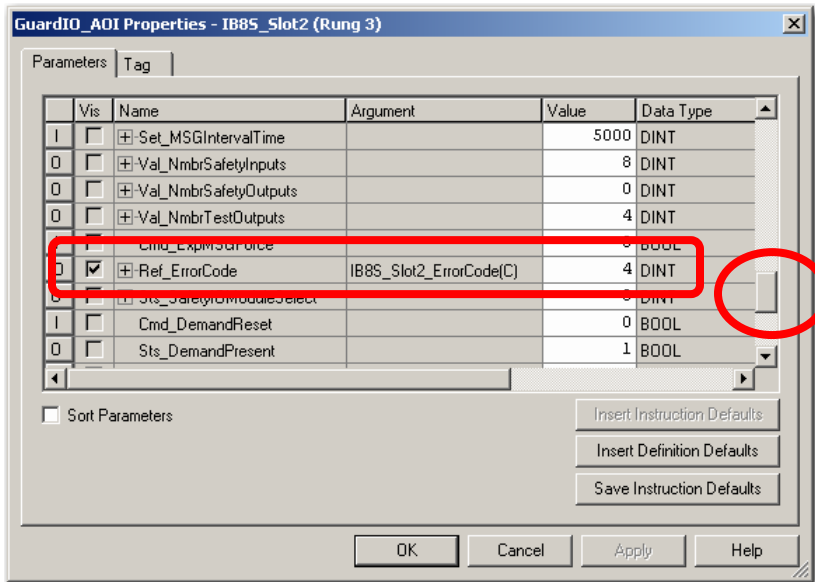
5. Within RSLogix 5000 software, call up the standard task **R01_SafetyIO_FP**. Right click on **R01_SafetyIO_FP** and select *Open*



6. Use the [down arrow] key to go to rung 3.
7. Click on the configuration dialog to the right of the naming tag (circled below):



- Scroll down until you see the tag called *Ref_ErrorCode*. It is easy to find, because the argument column is *IB8S_Slot2_ErrorCode*. Tip: Note the location of the scroll bar (circled below):



The error code 4 is a Discrepancy error.

- Press the Flashing red EStop DCS icon on the HMI:



- Press the Fault button on the bottom of the HMI screen:



Because this fault was masked from the safety instruction, the EStop DCS instruction faceplate only knows the combined status bit went LO.

- Close the instruction faceplate on the HMI using the [X] in the top right corner.

12. Press the 1734-IB8S slot2 image on the HMI screen to call up the 1734-IB8S faceplate:



13. Press the flashing yellow alarm bell on the HMI screen.



The PointGuard input module faceplate indicates the actual fault, a discrepancy error, because when in dual channel mode the faults are detected by the module.

14. Close the IB8S window on the HMI.
15. Fix the fault (wire off) by pushing the EStop wire off button again, so that it returns to the normal position.
16. Cycle the EStop button (should be flashing red) to prove that the device fault has been fixed.

The error code is 0 (no faults)

17. Cycle the flashing red switch to reset the instruction fault.
18. Press the green flashing reset button to restart the safety outputs.
19. Press the EStop Wire OFF button (note it is a maintained button).
20. Press the EStop Wire OFF button again within 3 seconds to generate a **Channel Cycled fault**.

The Channel cycle fault is not distinguishable from a discrepancy fault by the module diagnostics, so the same fault code of 4 appears in the explicit message. That is one advantage of the instruction diagnostics, they are slightly more granular.

21. Cycle the Emergency Stop button (flashing) which clears the fault code on the module.
22. Cycle the flashing red selector switch to clear the instruction fault code.
23. Press the flashing green reset PB to restart the safety outputs.
24. Press the EStop ch-ch short button to generate a **Pulse Test Fault**.
25. Press the 1734-IB8S slot2 image on the HMI screen to call up the 1734-IB8S faceplate.



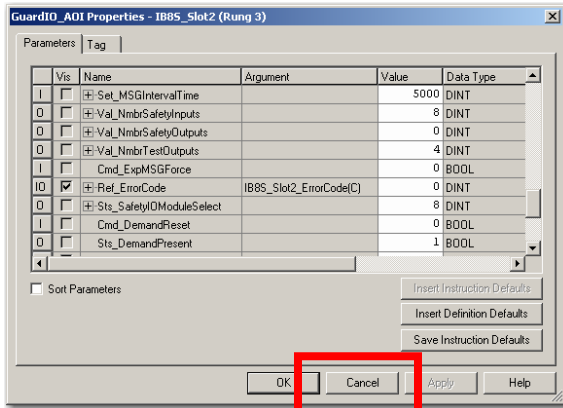
26. Press the flashing yellow alarm bell on the HMI screen.



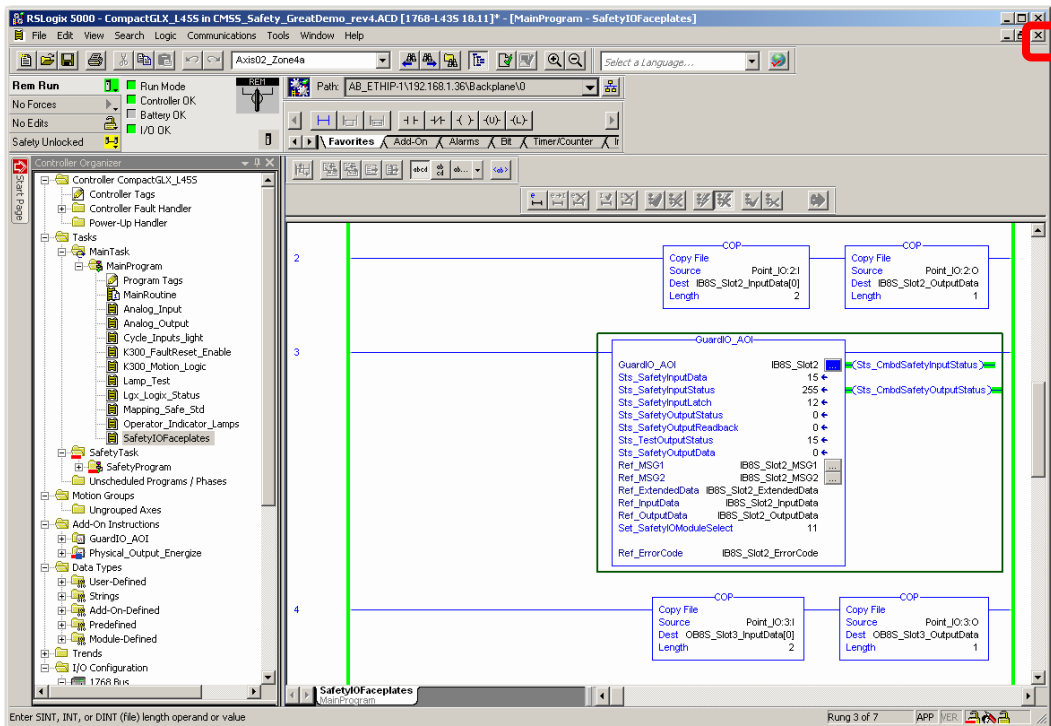
The channel to channel short causes error code 2, External Test Signal Error, which is another way of saying pulse test fault.

27. Close the IB8S window on the HMI.
28. Fix the fault by pushing the EStop ch-ch short button again so that it returns to the normal position.
29. Cycle the EStop button (should be flashing red) to prove that the device fault has been fixed.
30. Cycle the flashing red switch to clear the instruction fault.
31. Press the green flashing reset button to restart the safety outputs.
32. Press the yellow flashing button to start drive motion.

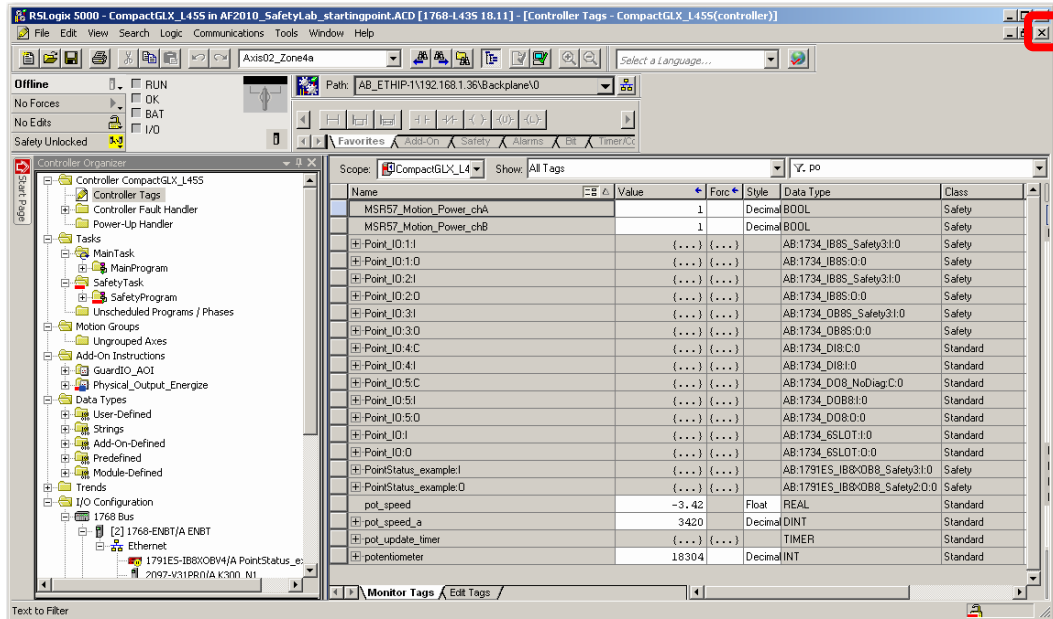
33. Close the GuardIO_AOI Properties window using **Cancel**.



34. Close the **R01_SafetyIO_FP** editor window:



35. Close the Controller Tags window:



In summary, when using Dual configuration for safety inputs, the module detects faults, and so explicit messaging needs to be used to obtain the fault codes.

Safety Output Diagnostics

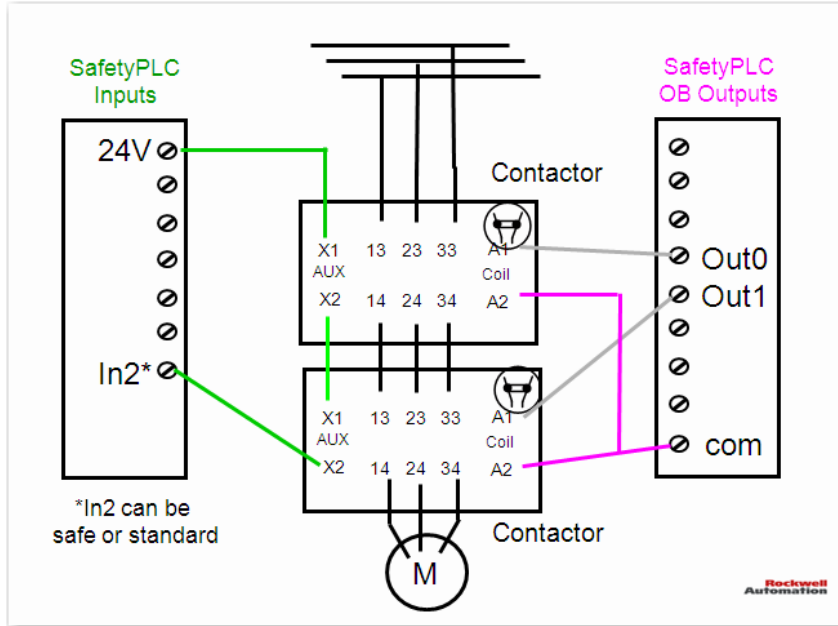
From a safety perspective, nothing is more critical than the machine going to the safe state when requested to do so. This is typically handled using redundancy (two paths to shut off the load) and monitoring (feedback). One fault can be tolerated due to redundancy. Monitoring is used to detect whether both paths dropped out the load, and to keep the machine from restarting if only one path was successful.

Auxiliary Feedback

The most common type of safety output device in discrete manufacturing are contactors. Two contactors in series are typically used to drop out the load. The contactors typically have a mechanically linked auxiliary feedback contact that is used for monitoring. If either contactor welds shut, then the auxiliary feedback remains open, and the feedback circuit remains LO. If the feedback is LO, then do not restart.

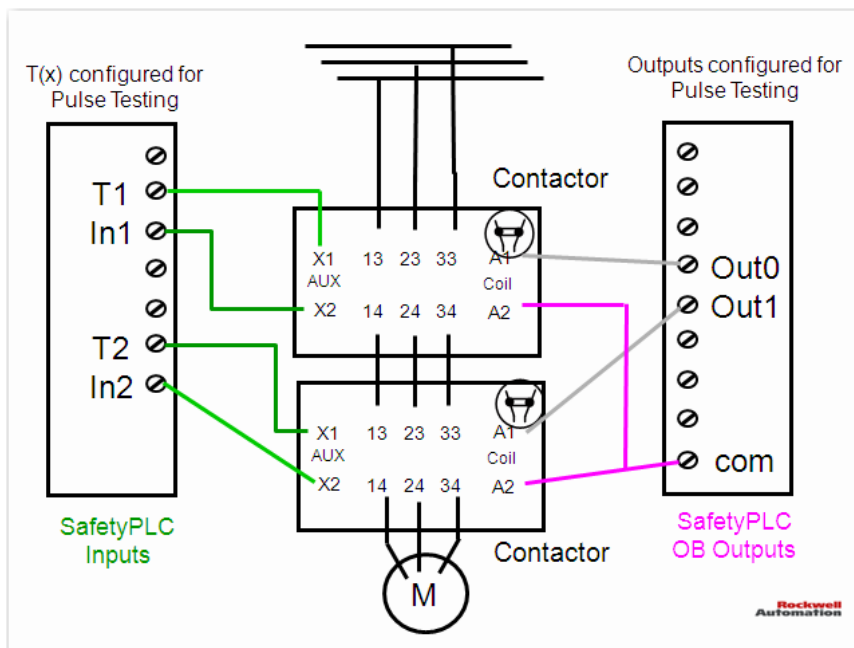
Single channel FB

If a single channel feedback circuit is used, we can detect if either of the contactors failed to drop out, but do not know which one failed. Note that a single channel feedback meets all relevant safety standards.



Dual channel FB

For improved diagnostics and availability, two feedback channels can be used, simply wiring to two inputs in a PLC system. Now we can determine which contactor has welded shut.



Output Pulse Testing

Channel to channel shorts on safety output pairs are difficult to detect because placing a demand on the output channel(s) does not help with detection. Although operating with the channel to channel short is not a dangerous state, one additional short to 24Vdc, in addition to the ch-ch short, could create a dangerous failure. Pulse testing is an effective method of detecting this fault between demands on the safety system.

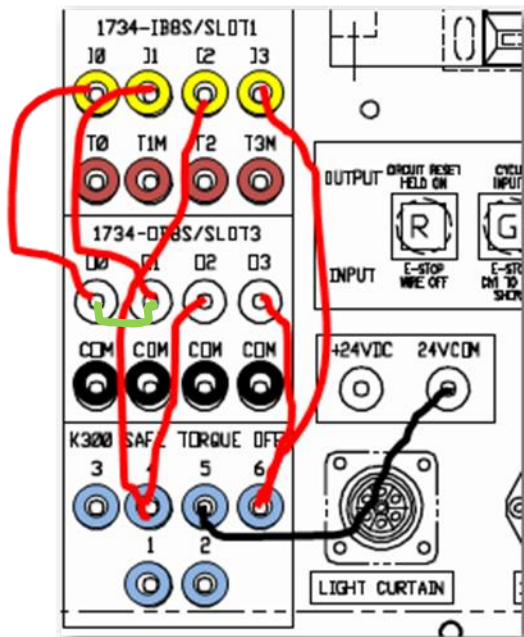
1. Call up the faceplate for OB8S Slot 3:



2. Select [OUT 0-7]:



3. Place a jumper cable between Safety Output 0 and Output 1 on the OB8S banana jacks. It is shown in green below.



When the jumper is placed between outputs 0 and 1, the next pulse test will detect the short because there is a secondary path to 24Vdc. This pulse tests occur every 600ms, and the duration of each pulse test is 400us. Only solid state devices

may be affected by such a quick pulse. Output channels 0 & 1 have red LEDs on the OB8S in slot 3 as well as the HMI faceplate.

4. Press the flashing yellow alarm bell on the HMI faceplate:



An output ON error means that the output had 24Vdc on its terminal when it should have been OFF.

5. Press the question mark button:



One probable cause is that the output is shorted to a power source (24Vdc), which is exactly the result of the jumper.

6. Press the right arrow:



The Recommend Action is to check the wiring to repair the fault.

7. Remove the jumper cable to fix the fault.

After 20 seconds, the output error latch time, the faults clear because both items required to reset the output fault have been met. The output error latch time has expired, and the outputs have been set logically LO (safe state).

8. Cycle the flashing red selector switch.
9. Press the flashing green reset button.
10. Press the yellow button to start motion.
11. Close the OB8S faceplate on the HMI.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846