

Safety Function: Zero Speed, Safe Limited Speed, Safe Direction

Products: PowerFlex 750 Safe Speed Monitor Option Module / TLS3-GD2 Switch
/ GuardLogix Controller / POINT Guard Safety I/O Modules
Safety Rating: PLd, Cat. 3 to EN ISO 13849.1 2008

LISTEN.
THINK.
SOLVE.®

Important User Information

Solid state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication [SGI-1.1](#) available from your local Rockwell Automation sales office or online at <http://literature.rockwellautomation.com>) describes some important differences between solid state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

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.

	<p>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.</p>
<p>IMPORTANT</p>	<p>Identifies information that is critical for successful application and understanding of the product.</p>
	<p>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.</p>
	<p>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.</p>
	<p>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.</p>

General Safety Information

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

IMPORTANT	This application example is for advanced users and assumes that you are trained and experienced in safety system requirements.
	ATTENTION: A risk assessment should be performed to make sure all task and hazard combinations have been identified and addressed. The risk assessment may require additional circuitry to reduce the risk to a tolerable level. Safety circuits must take into consideration safety distance calculations that are not part of the scope of this document.

Table of Contents

Introduction	4
Safety Function Realization: Risk Assessment	5
Safety Function	5
Safety Function Requirements	6
Functional Safety Description	6
Bill of Material	7
Setup and Wiring	8
Configuration	10
Programming	19
Falling Edge Reset.....	21
Calculation of the Performance Level.....	21
Verification and Validation Plan.....	25
Additional Resources	33

Introduction

This Safety Function application note explains how to wire, configure, and program a Compact GuardLogix® controller and POINT Guard I/O™ module to interface to a PowerFlex™ 750 Safe Speed Monitor Option (-S1) module to perform Safe Speed functions. It is important to note that the safe speed module actually performs the Zero Speed, Safe Limited Speed, and Safe Direction safety functions described in this application note. The GuardLogix safety controller simply requests when the Zero Speed and Safe Limited Speed (SLS) safety functions should be performed. For example, when the SLS keyswitch is rotated, the GuardLogix outputs wired to the PowerFlex 755 SLS inputs are energized to request Safe Limited Speed. Note that Safe Direction is configured in the safe speed module and is always being monitored. The GuardLogix controller has no interaction with the Safe Direction safety function.

The actuators for the safety functions are the Safe Torque Off (STO) channels embedded within the safe speed module. If the PowerFlex 755 STO inputs are de-energized, the motor controlled by the PowerFlex 755 drive will coast to a stop.

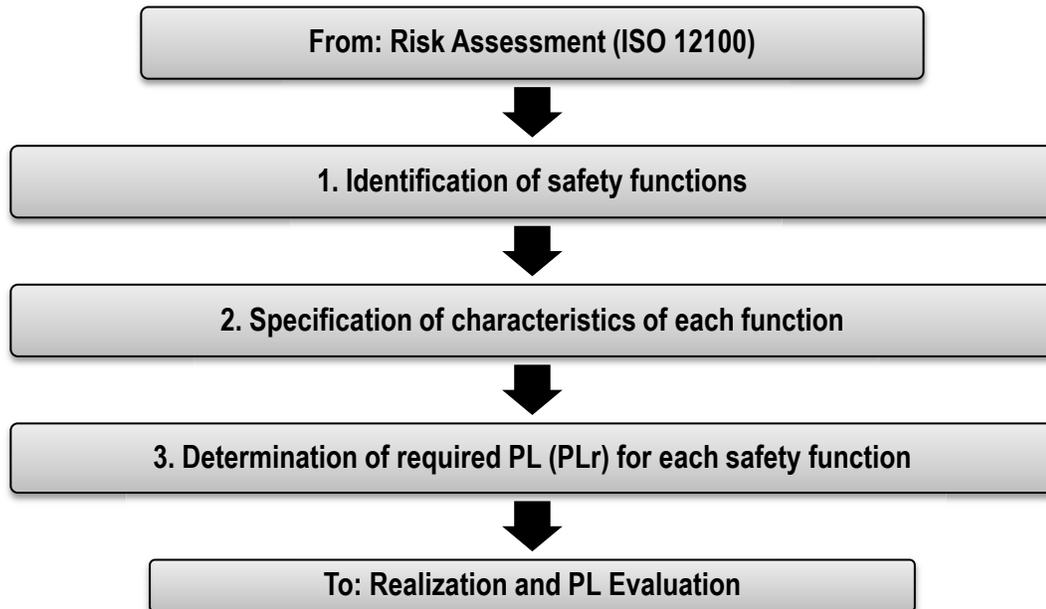
This example uses a Compact GuardLogix controller, but is applicable to any GuardLogix controller.

This example assumes the use of two diverse incremental encoders; one 845H and one 845T that are wired into the PowerFlex 750 Universal Feedback Option module and monitored by the safe speed module. The default MTTFd of 10 years, from ISO-13849, is used. A Diagnostic Coverage of 99% will be obtained from the SISTEMA Library of DC Measures. The DC is based on redundancy (two encoders), diversity (two types of encoders), diagnostics (cross monitoring between encoder signals), and individual power supplies for each encoder.

The SISTEMA calculations shown later in this document would have to be recalculated if different products are used.

Safety Function Realization: Risk Assessment

The required performance level is the result of a risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. For the purposes of this document, the assumed required performance level is Category 3, Performance Level d (Cat. 3, PLd).



Safety Function

The PowerFlex 750 Safe Speed Monitor Option module is capable of performing multiple safety functions simultaneously. In this application note, the following functions are used:

1. Safe Direction

When the safe speed module is configured to monitor the safe direction, a shutdown occurs if the motor attempts to rotate in the dangerous direction.

2. Safe Limited Speed

When Safe Limited Speed has been requested, the safe speed module initiates a shutdown, if the motor exceeds a pre-determined speed (the Safe Max Speed). When at or below the Safe Limited Speed, the door control logic is set to Unlock. You must perform a risk assessment to determine the safe maximum speed for the axis.

3. Standstill (Zero) Speed

When configured for Safe Stop, the safe speed module initiates a safe stop upon deactivation of the SS_In inputs. Standstill Speed is used to declare motion as stopped. The system is at standstill when the speed detected is less than or equal to the configured Standstill Speed. When standstill has been reached, door control logic is set to Unlock. Standstill Position Tolerance defines the position limit in encoder units that is tolerated after standstill has been reached. If the position changes by more than the amount specified by the Standstill Position Tolerance, after standstill

has been reached and the door is unlocked, a fault occurs and the system enters the safe state.

Safety Function Requirements

Limiting and monitoring the speed of a motor to make sure hazardous motion does not exceed a predetermined limit. The safe speed limit must be established such that the operator can avoid the hazardous motion. Monitoring the direction of the motor guards against hazardous motion. The system monitors for Zero (Standstill) Speed so that the door remains closed and locked until hazardous motion is stopped. At such time, the safe speed module unlocks the door by applying power to the guard lock. While the door is open, the system is monitored to prevent an unexpected start-up. When the door is closed, hazardous motion and power to the motor does not resume until a secondary action (start button depressed) occurs.

Faults at the variable speed drive, door interlock switch, encoder, wiring terminals or safety controller will be detected before the next safety demand.

The safety function meets 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, Safe Limited Speed is requested by placing a demand on a safety input interlock. After a user-configured delay (3 seconds in this example) to reach the safe speed, the PowerFlex 750 Safe Speed Monitor Option module begins monitoring the speed and makes sure that the safe speed is not exceeded. If the motor speed is below the configured safe limited speed, the gate is unlocked to allow operator entry into the hazardous area. If the motor speed exceeds the safe speed while the gate is unlocked, then the safe speed module drops out the Safe Torque Off (STO) and the motor coasts to a stop.

If a demand is placed on the Emergency Stop, the safe speed module drops out the STO and the motor coasts to a stop. When Zero Speed is reached, the gate unlocks.

The TLS3-GD2 channels are wired to the safe speed module in the PowerFlex 750 drive. One channel pair is the lock monitoring contacts and the other is the door monitoring contacts. The gate solenoid is wired to the safe speed module as well. The Safe Stop button, Reset button, and Safe Limited Request keyswitch are wired to the POINT Guard input module. Outputs from the POINT Guard output module are wired directly to inputs on the safe speed module. These hardwired signals include the Safe Stop, Safe Limited Speed Request, and a reset signal. The I/O module is connected via CIP Safety over an EtherNet/IP network to the safety controller (SC1). The safety code in SC1 monitors the status of the Emergency Stop and SLS safety inputs using the pre-certified safety instruction Dual Channel Input Stop (DCS). When all safety input interlocks are satisfied, no faults are detected, and the reset push button is pressed, a second certified function block called Configurable Redundant Output (CROUT) controls and monitors feedback for the Safe Stop signal to the PowerFlex 750 drive.

Bill of Material

This application uses these products.

Cat. No.	Description	Quantity
440G-T27181	TLS3-GD2 Power to Release Safety Interlock Switch	1
800FM-G611MX10	800F Reset Push Button - metal, guarded, blue, R, metal latch mount, 1 N.O. contact(s), standard	2
800FM-KM22XM02	2 position keyswitch; metal; maintained; right key removal; 2 N.C. contacts	1
800FP-MT44PX02	800F non-illuminated mushroom operators, twist-to-release, 40 mm, round plastic (Type 4/4X/13, IP66), red, 2 N.C. contacts	1
800F-15YE112	800F Legend Plate, 60 mm round, English: EMERGENCY STOP, yellow with black legend text	1
1768-ENBT	CompactLogix™ EtherNet/IP Bridge Module	1
1768-L43S	Compact GuardLogix Processor, 2.0 MB standard memory, 0.5 MB safety memory	1
1768-PA3	Power Supply, 120/240 VAC input, 3.5 A @ 24V DC	1
1769-ECR	Right end cap/terminator	1
1734-AENT	24V DC ethernet adapter	1
1734-TB	Module base with removable IEC screw terminals	4
1734-IB8S	POINT Guard Safety Input Module	1
1734-OB8S	POINT Guard Safety Output Module	1
1783-US05T	Stratix 2000™ Unmanaged Ethernet Switch	1
20G11RD2P1AA0NNNNN	PowerFlex 750; 480V; 2.1A continuous output rating	1
20-750-S1	PowerFlex 750 Safe Speed Monitor Option Module	1
20-750-UFB-1	PowerFlex 750 Universal Feedback Option Module	1
User specified	845T/845H Incremental Encoders	2

Setup and Wiring

For detailed information on installing and wiring, refer to the publications listed in the [Additional Resources](#) on the back cover.

System Overview

The PowerFlex 750 Safe Speed Monitor Option module monitors two door channels and two lock channels of the TLS3-GD2. The 1734-IB8S module monitors the Safe Stop and Safe Limited Request keyswitch.

Both the safe speed module and the 1734-IB8S module can source the 24V DC for all these channels to dynamically test the signal wiring for shorts to 24V DC and channel-to-channel shorts. If a fault occurs, either or both channels will be set LO, and the system reacts by dropping out the Safe Torque Off (STO). The system resets only after the fault is cleared and the input is cycled.

Shorts to 0V DC (and wire off) are seen as an open circuit by the safe speed module and 1734-IB8S module input and the system will react by dropping out the safety contactors. If the inputs remain discrepant for longer than the discrepancy time, then the PowerFlex 755 drive safety or controller will declare a fault. The system resets only after the fault is cleared and the input is cycled.

The gate solenoid is controlled by the safe speed module.

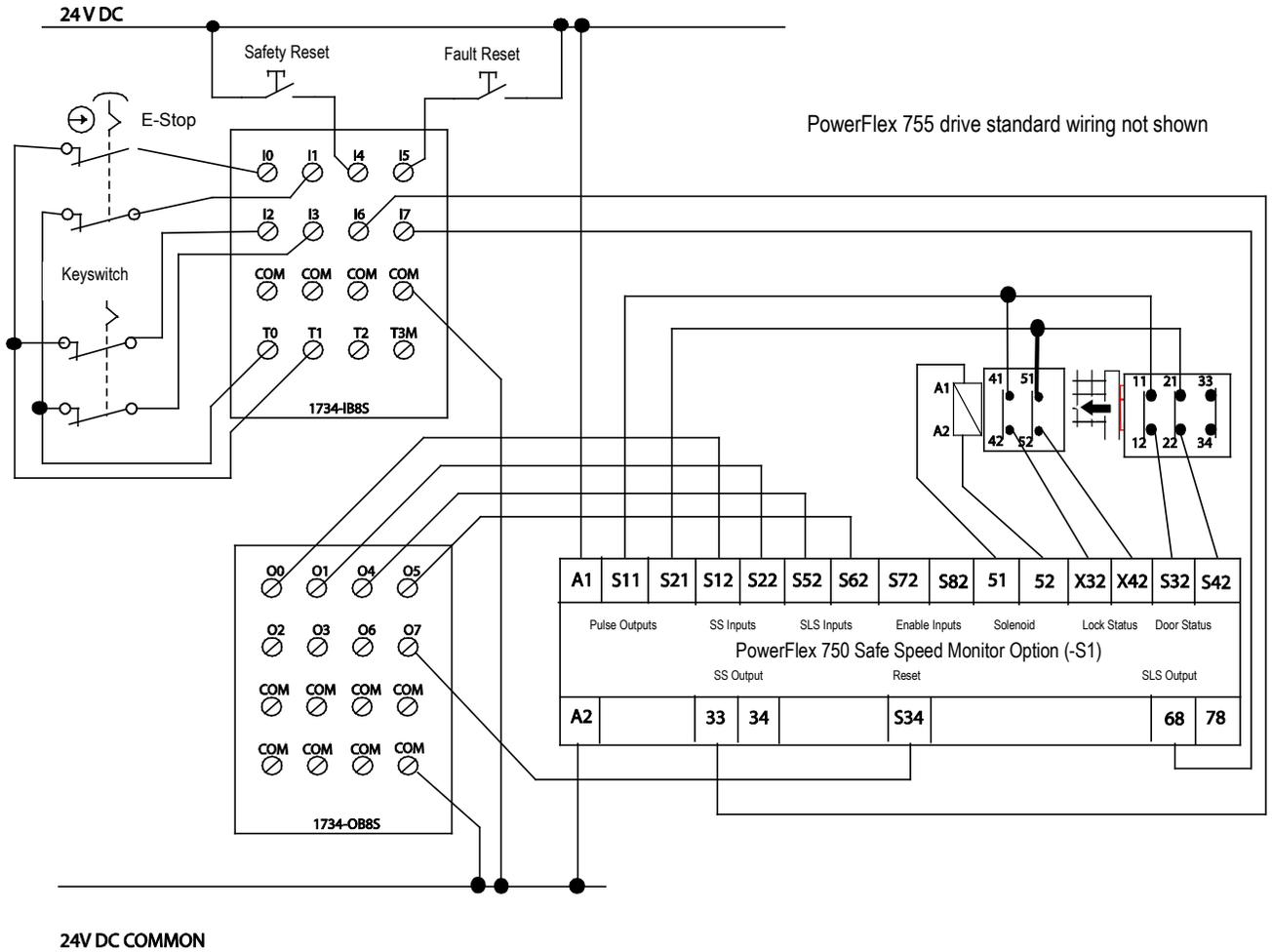
From a Guardlogix controller perspective, Safe Stop (Zero Speed) is a pair of safety outputs wired to the Safe Stop inputs (S12/S22) on the safe speed module. If the Safe Stop inputs ever go LO, a shutdown occurs and the motor coasts to a stop. The GuardLogix controller gets feedback for Safe Stop by using one of the cascading SS outputs (S34/S44) on the safe speed module. These safety outputs cannot restart if the feedback channel is not in the correct state. This feedback is optional. Because the redundant safety outputs are pulse tested, this is no different than wiring a Cat. 4 light curtain to the SS inputs, an architecture that achieves Cat. 4 without feedback.

From a Guardlogix controller perspective, the SLS safety function device is a pair of safety outputs wired to the SLS inputs (S52/S62) on the safe speed module. If the SLS inputs ever go LO, a SLS request is made to the PowerFlex 755 drive. The GuardLogix controller gets feedback for SLS using one of the cascading SLS outputs (S68/S78) on the safe speed module. These safety outputs cannot restart if the feedback channel is not in the correct state. This feedback is optional for the same reasons as stated above.

The system has individual reset buttons for resetting faults and safety outputs. If either of these resets is pressed, a signal is sent from a GuardLogix output to the reset input on the safe speed module (S34).

The reset buttons and the feedback circuits are all wired to the 1734-IB8S module in this example. This is not required for functional safety. These inputs could be wired to a standard input module.

Electrical Schematic



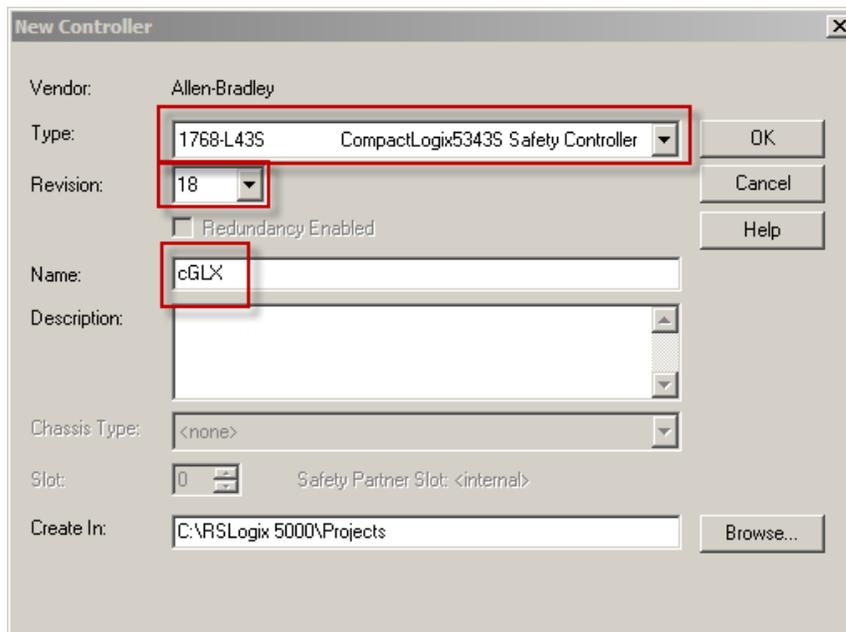
Configuration

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

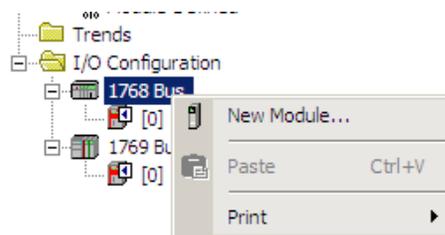
Configure the Controller and Add I/O Modules

Follow these steps:

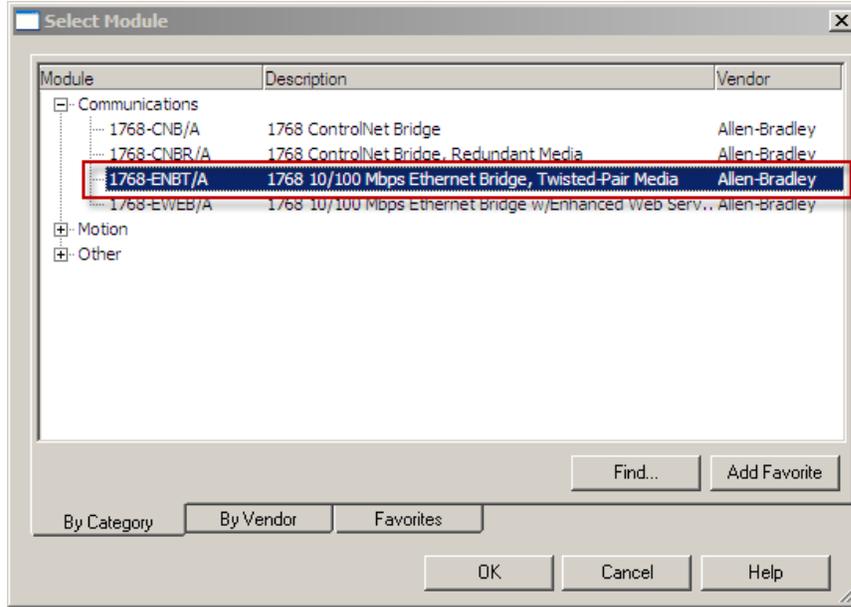
1. In RSLogix 5000 software, create a new project.



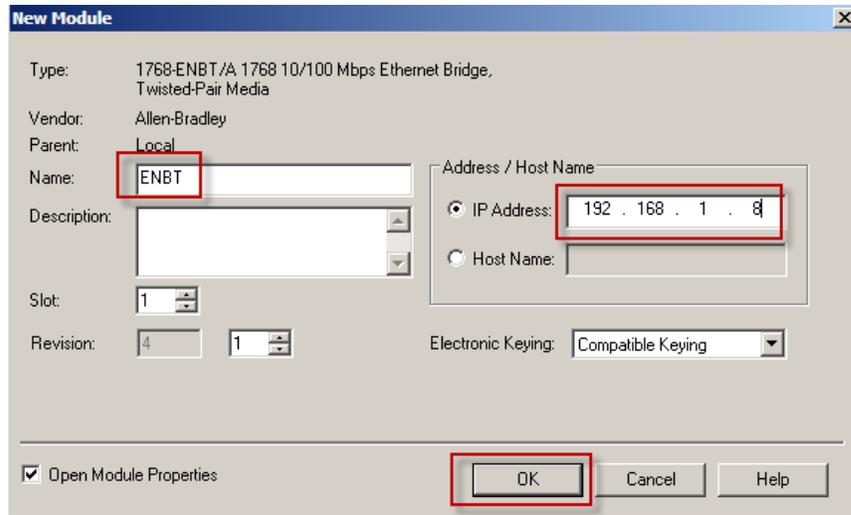
2. In the Controller Organizer, add the 1768-ENBT module to the 1768 bus.



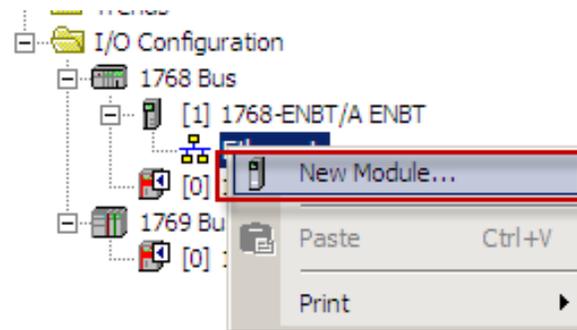
3. Select the 1768-ENBT module and click OK



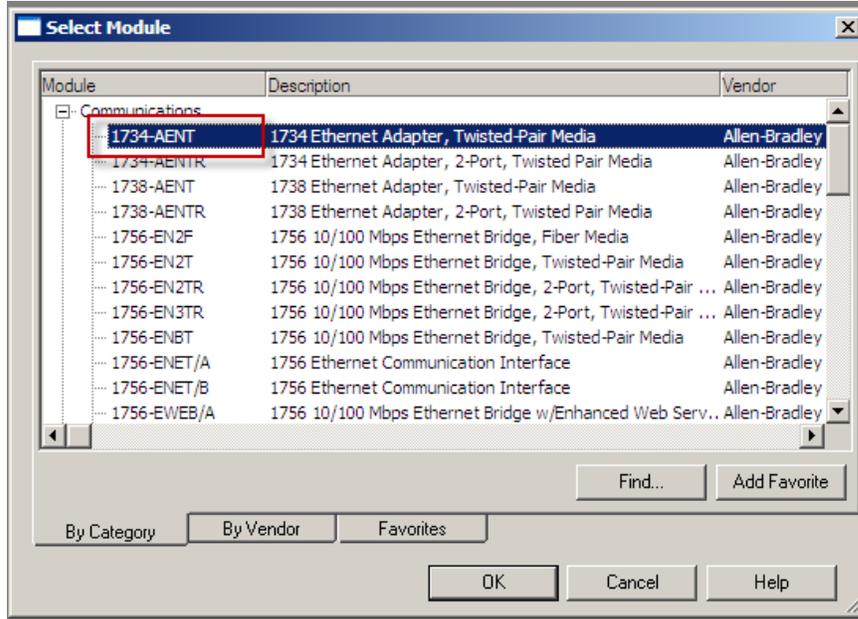
4. Name the module, type its IP address, and click OK.
We used 192.168.1.8 for this application example. Yours may be different.



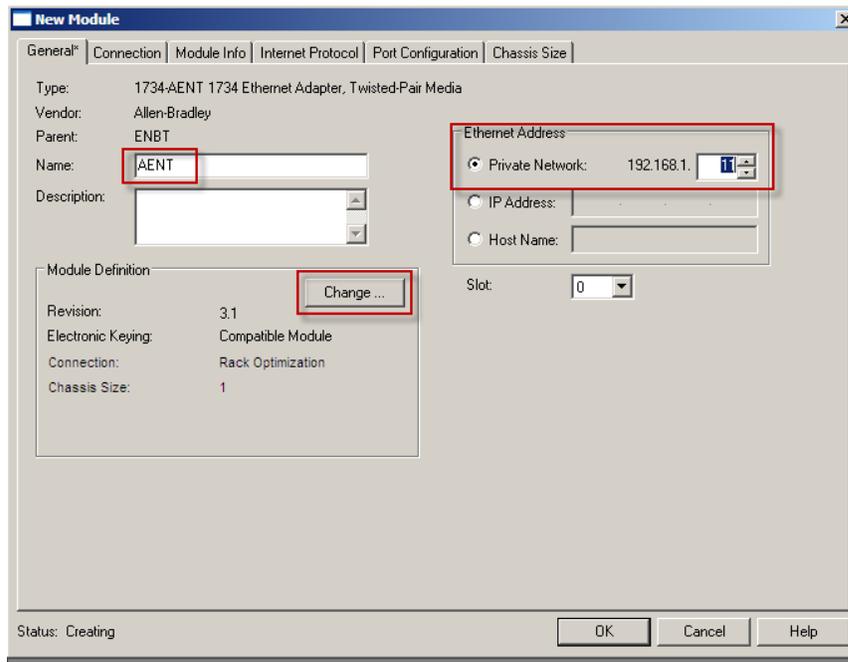
5. Add the 1734-AENT adapter by right-clicking the 1768-ENBT module in the Controller Organizer and choosing New Module.



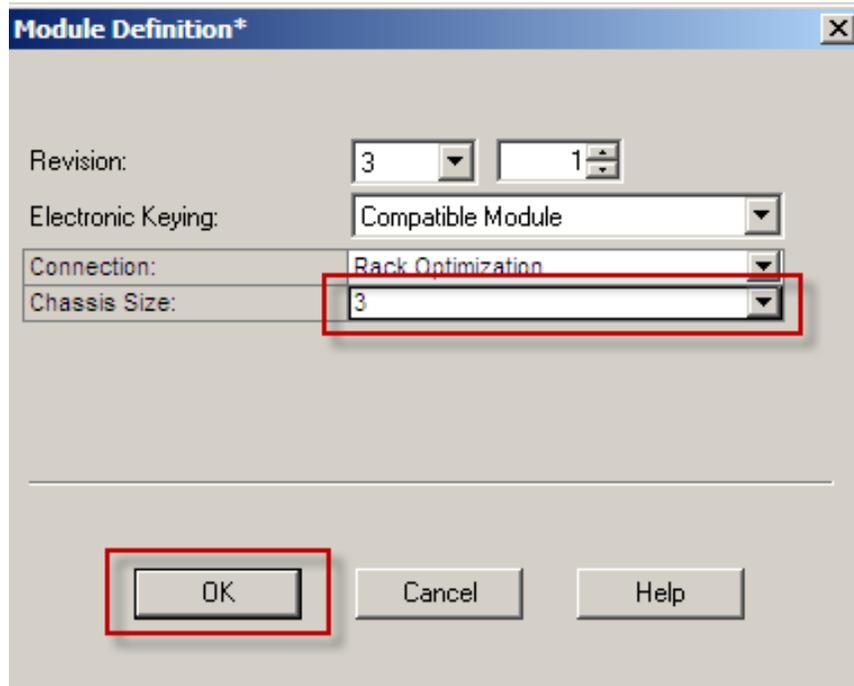
6. Select the 1734-AENT adapter and click OK.



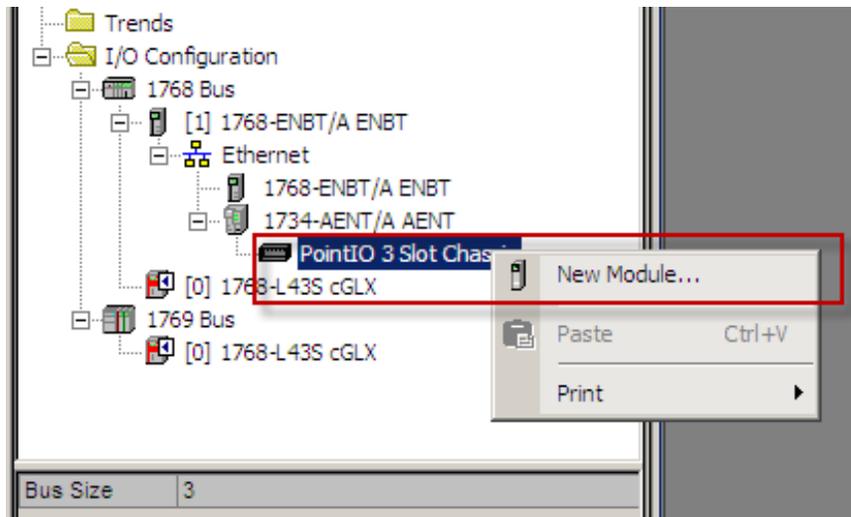
7. Name the module, type its IP address, and click OK.
We used 192.168.1.11 for this application example. Yours may be different.
8. Click Change.



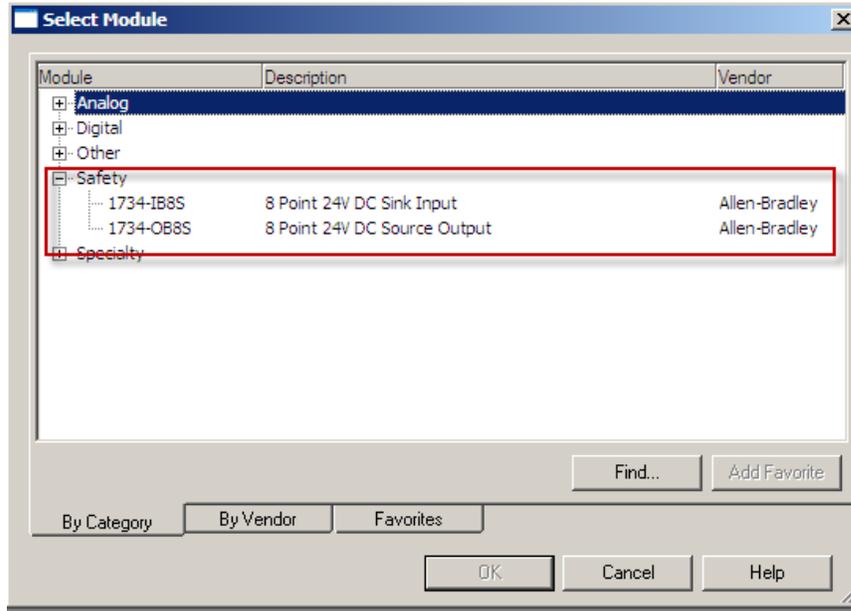
- Set the Chassis Size as 3 for the 1734-AENT adapter and click OK. Chassis size is the number of modules that will be inserted in the chassis. The 1734-AENT adapter is considered to be in slot 0, so for one input and one output module, the chassis size is 3.



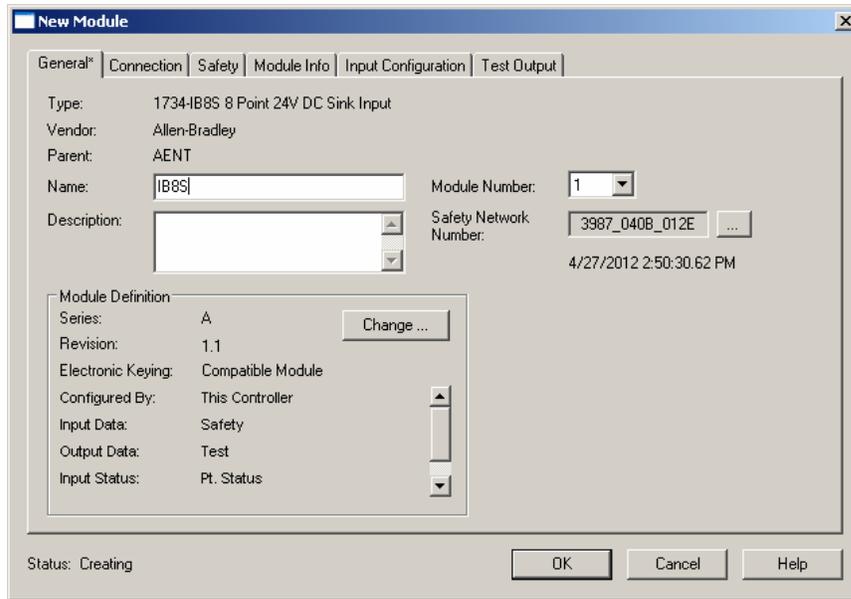
- In the Controller Organizer, right-click the 1734-AENT adapter and choose New Module.



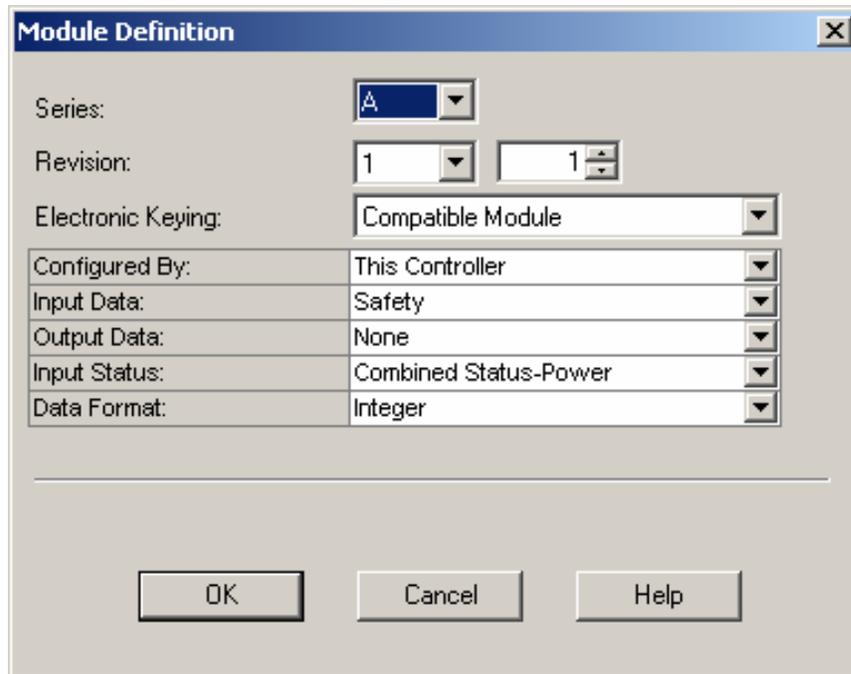
11. Expand Safety, select the 1734-IB8S module, and click OK.



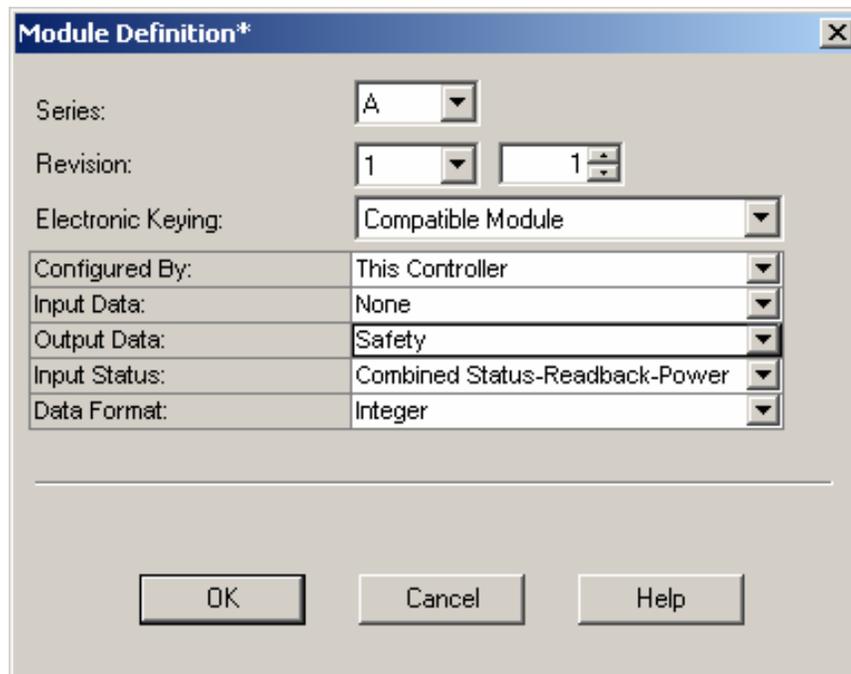
12. In the New Module dialog box, name the device 'IB8S' and click Change.



13. When the Module Definition dialog box opens, change the Output Data to 'None', verify the Input Status is Combined Status-Power', and click OK. Setting the output data to 'None' means that you cannot use the Test Outputs as standard outputs, which is appropriate in this example. This saves one controller connection because we are using only the input connection.



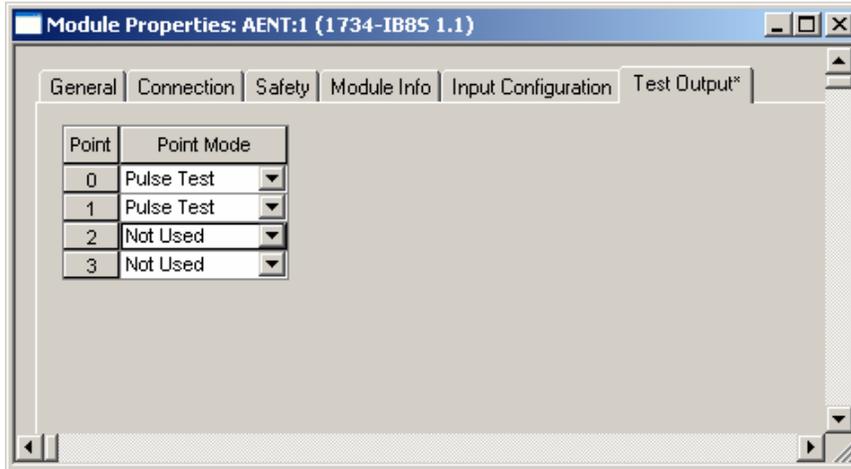
14. Close the Module Properties dialog box by clicking OK.
15. Repeat steps 10...14 to add the 1734-OB8S safety output module.
 - a. Name the module OB8S.
 - b. Choose slot 2.
 - c. Select 'Combined Status-Readback-Power' for Input Status definition



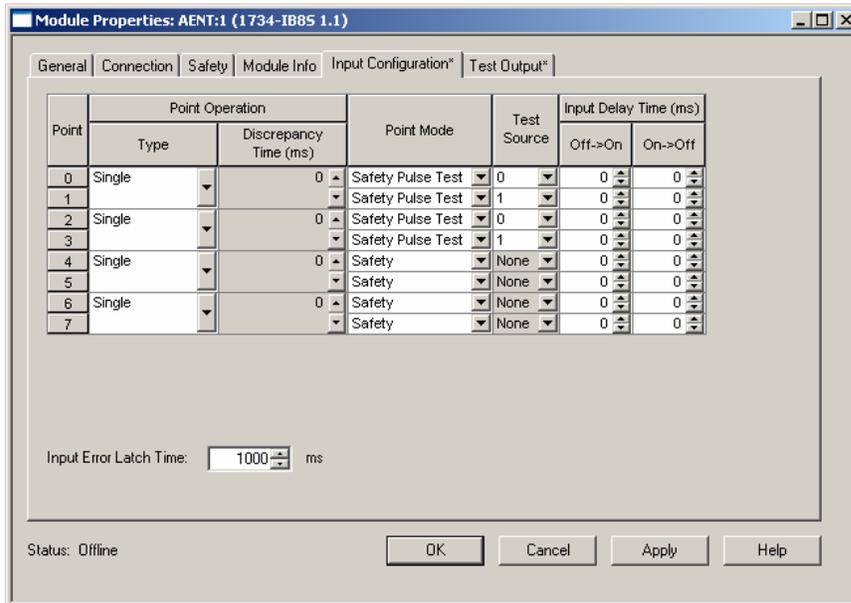
Configure the I/O Modules

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

1. In the Controller Organizer, right-click the 1734-IB8S module and choose Properties.
2. Click Test Output and configure the module as shown. T0 and T1 are used to pulse test the E-Stop and keyswitch.

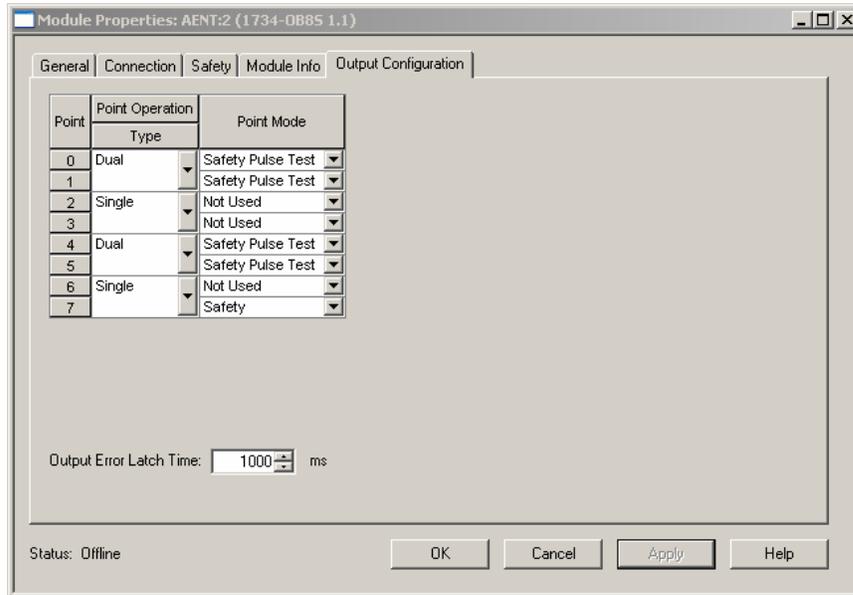


3. Click Input Configuration and configure the module as shown. Inputs 0/1 are the E-Stop channels. Recall that inputs 0/1 are being sourced from test outputs 0/1. Inputs 2/3 are the keyswitch channels. They are also being sourced from test outputs 0/1. Single is used because the discrepancy time diagnostic is done in the Dual Channel Input Stop (DCS) safety instruction in the controller. Inputs 4/5 are the reset buttons. Inputs 6/7 are wired to the safe speed module for Safe Stop (SS) and Safe Limited Speed (SLS) feedback.



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

- Click Output Configuration and configure the module as shown. Outputs 0/1 are controlling the Safe Stop inputs on the safe speed module. Outputs 4/5 are controlling the Safe Limited Speed inputs on the PowerFlex 755 drive. All four of these outputs are configured for pulse testing. Output 7 is driving the reset signal on the safe speed module.



- Click OK.

PowerFlex 750 Safe Speed Monitor Option Module Configuration

The parameters with a red arrow have been configured based on this example architecture. Configure the remainder based on the risk assessment and application requirements.

General Tab

S	N:P.P#	Name	Value
*	1: 6.20	Cascaded Config	Single
→*	1: 6.21	Safety Mode	Lim Speed DM
→*	1: 6.22	Reset Type	Manual
*	1: 6.24	OverSpd Response	42 msec
→*	1: 6.72	SS Out Mode	No Pulse Tst
→*	1: 6.73	SLS Out Mode	No Pulse Tst



Feedback Tab

S	N:P.P#	Name	Value
→ *	1: 6.27	Fbk Mode	Dual S/P Chk
*	1: 6.28	Fbk 1 Type	Incremental
*	1: 6.29	Fbk 1 Units	Rev
*	1: 6.30	Fbk 1 Polarity	Normal
*	1: 6.31	Fbk 1 Resolution	3000
*	1: 6.32	Fbk 1 Volt Mon	0
R	1: 6.33	Fbk 1 Speed	0.0
*	1: 6.34	Fbk 2 Units	Rev
*	1: 6.35	Fbk 2 Polarity	Normal
	1: 6.36	Fbk 2 Resolution	0
	1: 6.37	Fbk 2 Volt Mon	0
	1: 6.38	Fbk 2 Speed	0.0
	1: 6.39	Fbk Speed Ratio	0.00000
	1: 6.40	Fbk Speed Tol	0.0
	1: 6.41	Fbk Pos Tol	0
→	1: 6.42	Direction Mon	Pos Always
	1: 6.43	Direction Tol	10

Stop Tab

S	N:P.P#	Name	Value
→	1: 6.44	Safe Stop Input	2 OSSD 3s
→	1: 6.45	Safe Stop Type	Torque Off
	1: 6.46	Stop Mon Delay	3.0
	1: 6.47	Max Stop Time	15.0
	1: 6.48	Standstill Speed	2.000
	1: 6.49	Standstill Pos	10
	1: 6.50	Decel Ref Speed	1600
	1: 6.51	Stop Decel Tol	50

Limited Speed Tab

S	N:P.P#	Name	Value
→ *	1: 6.52	Lim Speed Input	2 OSSD 3s
*	1: 6.53	LimSpd Mon Delay	3.0
→	1: 6.54	Enable SW Input	Not Used
	1: 6.55	Safe Speed Limit	10.0
	1: 6.56	Speed Hysteresis	0

Door Control Tab

S	N:P.P.#	Name	Value
→*	1: 6.57	Door Out Type	Pwr to Rel
→	1: 6.58	DM Input	2NC
→	1: 6.59	Lock Mon Enable	Enable
→	1: 6.60	Lock Mon Input	2NC
→	1: 6.74	Door Out Mode	Pulse Test



Programming

The Dual Channel Input Stop (DCS) monitors dual-input safety devices whose main function is to stop a machine safely, for example, an E-Stop, light curtain, or safety gate. In this example, one is being used to monitor an E-Stop button, and the other is monitoring the Safe Limited Speed (SLS) keyswitch.

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

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

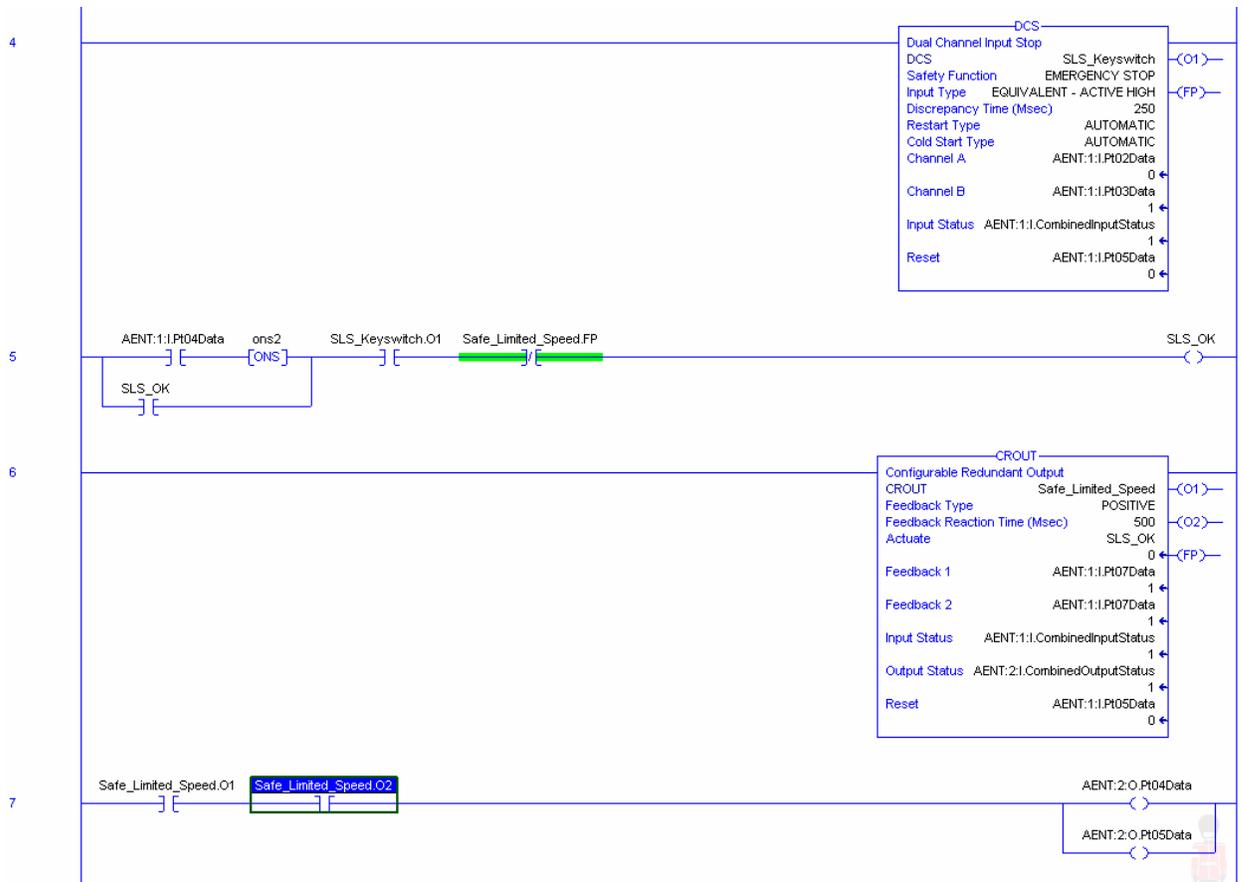
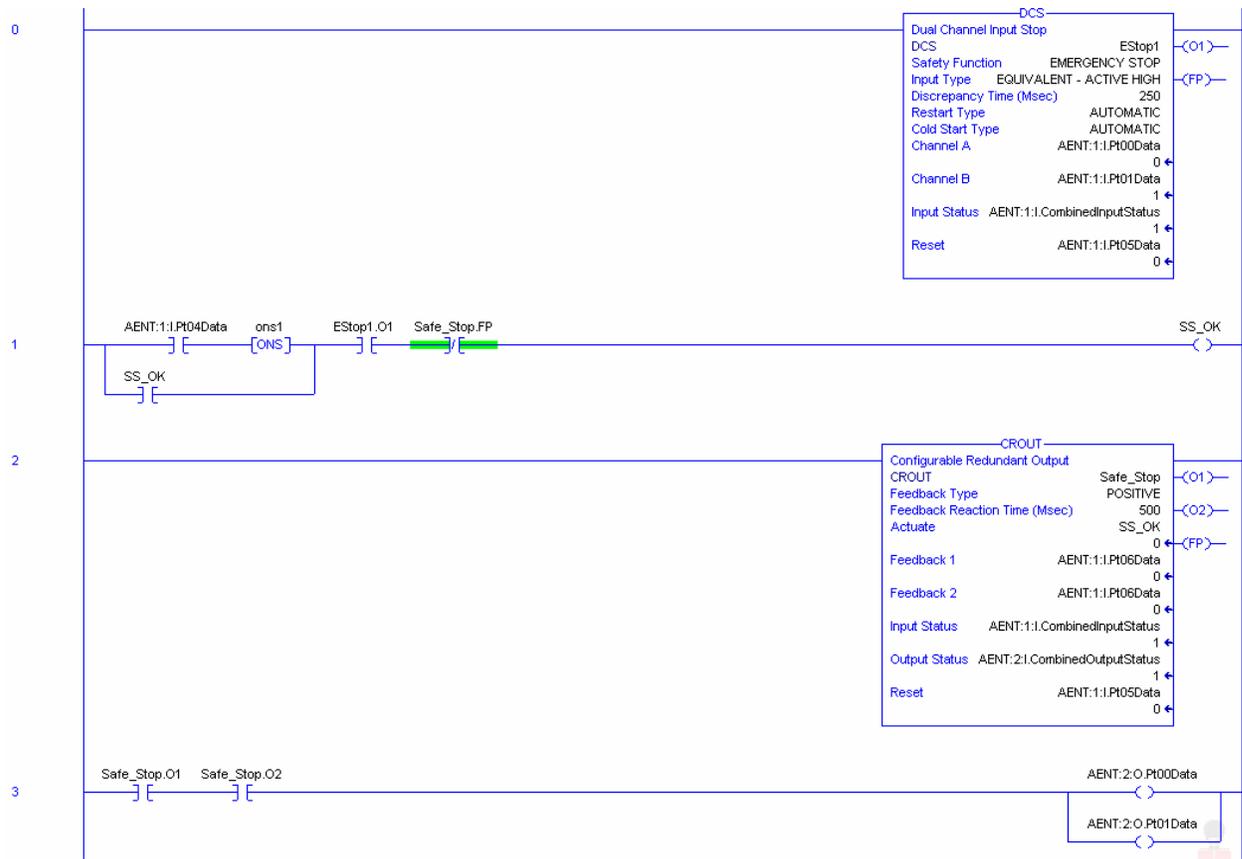
Input status typically represents the channel status of the two input channels. In this example, the 'Combined Input Status' bit goes LO if any of the eight input channels has a fault.

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

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

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

The two output tags from the CROUT instruction are used to drive the safety outputs on the 1734-OB8S module that are wired to the respective solid state inputs on the PowerFlex 750 Safe Speed Monitor Option module.



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 Output Enable rungs.



Calculation of the Performance Level

When configured correctly, these safety functions can achieve a safety rating of PLd according to EN ISO 13849.1 2008.

The functional safety specifications of the project call for a minimum Performance Level of PLd and a minimum structure of Cat. 3.

A PFHd of less than 1.0E-06 for the overall safety function is one of the requirements for PLd.

The measures against Common Cause Failure (CCF) are quantified using the scoring process 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 performed when implementing this example.

Calculations are based on one operation of the Safe Stop per hour; therefore 8760 operations per year.

The individual subsystem values are shown below.

Zero Speed

Safety function

		Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
✓	SB	POINT Guard I/D: 1734-IB85	e	1.34E-10	not relevant	not relevant	not relevant	4	fulfilled
✓	SB	POINT Guard I/D: 1734-OB85	e	1.38E-10	not relevant	not relevant	not relevant	4	fulfilled
✓	SB	Safety PLC: Compact GuardLogix 1768	e	2.1E-10	not relevant	not relevant	not relevant	4	fulfilled
✓	SB	TLS3 GD2 Interlock Switch	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled
✓	SB	Emergency Stop Button	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled
✓	SB	AC Drive: PowerFlex 755 Safe Speed M...	e	2.77E-8	not relevant	not relevant	not relevant	4	fulfilled
✓	SB	Incremental Encoders	d	3.54E-7	65 (fulfilled)	99 (High)	10 (Medium)	3	fulfilled

Safe Limited Speed

The screenshot shows the SIMATIC Manager Safety function interface. The 'Subsystems' tab is active, displaying a table of safety components. The table includes columns for Name, PL, PFH [1/h], CCF score, DCavg [%], MTTFd [a], Category, and Requirements of the category. All requirements are listed as 'fulfilled'.

Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
POINT Guard I/O: 1734-IB8S	e	1.34E-10	not relevant	not relevant	not relevant	4	fulfilled
POINT Guard I/O: 1734-OB8S	e	1.38E-10	not relevant	not relevant	not relevant	4	fulfilled
Keyswitch	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled
Safety PLC: Compact GuardLogix 1768	e	2.1E-10	not relevant	not relevant	not relevant	4	fulfilled
TLS3 GD2 Interlock Switch	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled
AC Drive: PowerFlex 755 Safe Speed M...	e	2.77E-8	not relevant	not relevant	not relevant	4	fulfilled
Incremental Encoders	d	3.54E-7	65 (fulfilled)	99 (High)	10 (Medium)	3	fulfilled

Safe Direction

The screenshot shows the SIMATIC Manager Safety function interface for 'Safe Direction'. The 'Subsystems' tab is active, displaying a table of safety components. The table includes columns for Name, PL, PFH [1/h], CCF score, DCavg [%], MTTFd [a], Category, and Requirements of the category. All requirements are listed as 'fulfilled'.

Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
AC Drive: PowerFlex 755 Safe Speed M...	e	2.77E-8	not relevant	not relevant	not relevant	4	fulfilled
Incremental Encoders	d	3.54E-7	65 (fulfilled)	99 (High)	10 (Medium)	3	fulfilled

The overall safety function value is shown below for each safety function.

Zero Speed

The screenshot shows the SIMATIC Manager Safety function interface for 'Zero Speed'. The 'Subsystems' tab is active, and the 'Determine PL from subsystems' option is selected. The Performance Level (PL) is set to 'd' and the PFH [1/h] is 4.31E-7.

Performance Level (PL): PFH [1/h]:

Safe Limited Speed

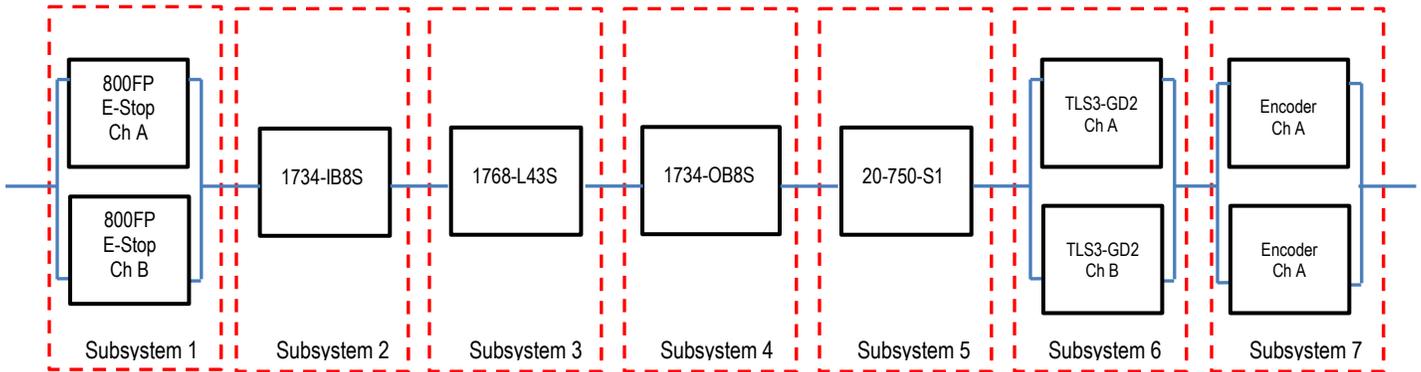
The screenshot shows the SIMATIC Manager interface for configuring the 'Safe Limited Speed' safety function. The title bar includes 'SIMATIC Safety function' and the IFA logo. Below the title bar are navigation tabs: 'Documentation', 'PLr', 'PL', and 'Subsystems'. The 'PL' tab is selected. The main content area has a radio button labeled 'Determine PL from subsystems' which is selected. Below this, there are two input fields: 'Performance Level (PL):' with the value 'd' and 'PFH [1/h]:' with the value '4.31E-7'.

Safe Direction

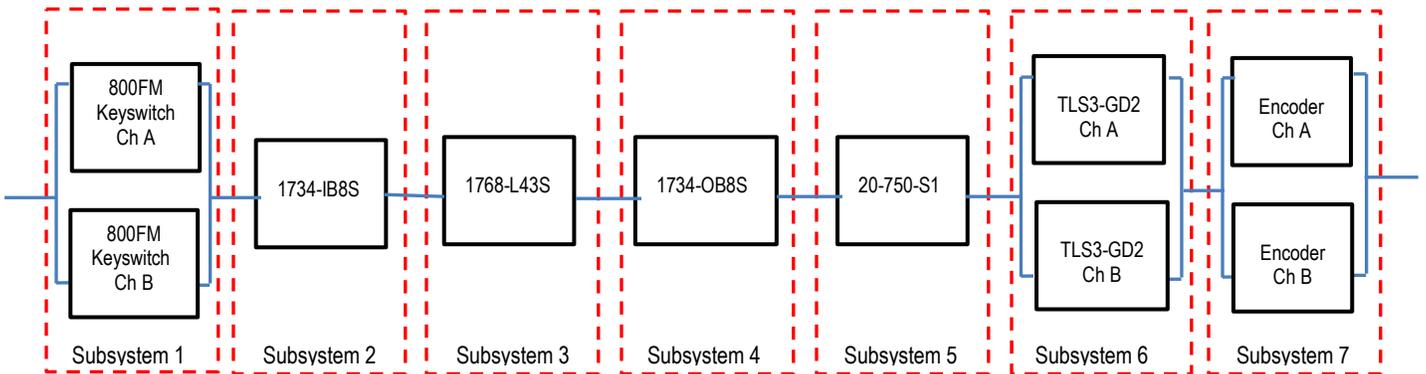
The screenshot shows the SIMATIC Manager interface for configuring the 'Safe Direction' safety function. The title bar includes 'SIMATIC Safety function' and the IFA logo. Below the title bar are navigation tabs: 'Documentation', 'PLr', 'PL', and 'Subsystems'. The 'PL' tab is selected. The main content area has a radio button labeled 'Determine PL from subsystems' which is selected. Below this, there are two input fields: 'Performance Level (PL):' with the value 'd' and 'PFH [1/h]:' with the value '3.82E-7'.

The safety functions can be modeled as shown in the following safety-related block diagram:

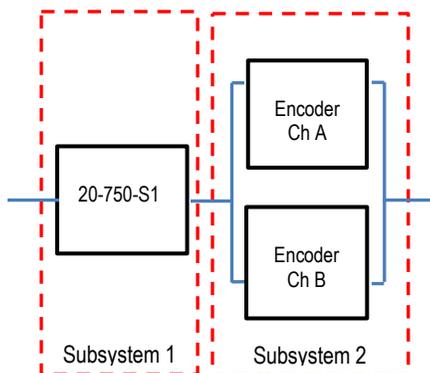
Zero Speed



Safe Limited Speed



Safe Direction



Verification and Validation Plan

Verification and validation play an important role in the avoidance of faults throughout the safety system design and development process. ISO EN 13849-2 sets the requirements for verification and validation by calling for a documented plan to confirm that all of the safety functional requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm it meets the Required Performance Level (PLr) specified. The SISTEMA software tool 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 it meets the specified requirements of the safety function. The safety control system is tested to confirm all of the safety related outputs respond appropriately to their corresponding safety related inputs. The functional test should include normal operating conditions in addition to potential fault inject of failure modes. A checklist is typically used to document the validation of the safety control system.

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

Prior to validating the GuardLogix Safety System, confirm that the safety system and safety application program has been designed in accordance with the GuardLogix System Safety reference manuals (publication [1756-RM093](#) for GuardLogix 5560 and Compact GuardLogix, and publication [1756-RM099](#) for GuardLogix 5570 controllers) and the GuardLogix Application Instruction Safety Reference Manual, publication [1756-RM095](#).

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist

<i>General Machinery Information</i>		
Machine Name/Model Number		
Machine Serial Number		
Customer Name		
Test Date		
Tester Name(s)		
Schematic Drawing Number		
20-750-S1 Configuration Signature ID		
Controller Name		
RSLogix 5000 Safety Signature ID		
Safety Network Number(s)		
RSLogix 5000 Software Version		
Safety Control System Modules	GuardLogix System Modules	Firmware Version
GuardLogix Safety Controller	1768-L43S	
CompactLogix Ethernet Bridge	1768-ENBT	
POINT I/O Ethernet Adapter	1734-AENT	
POINT Guard I/O Input Modules	1734-IB8S	
POINT Guard I/O Output Modules	1734-OB8S	

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

Safety System Configuration and Wiring Verification			
Test Step	Verification	Pass/Fail	Changes/Modifications
1	Verify that the safe speed drive has been wired and configured in accordance with the Safe Speed Monitor Option Module for PowerFlex 750-Series AC Drives Safety Reference Manual, publication 750-RM001 .		
2	Verify the safety system has been designed in accordance with the GuardLogix System Safety Reference Manuals (publication 1756-RM093 for GuardLogix 5560 and Compact GuardLogix, publication 1756-RM099 for GuardLogix 5570).		
3	Verify the safety application program has been designed in accordance with the GuardLogix Application Instruction Safety Reference Manual, publication 1756-RM095 .		
4	Visually inspect the safety system network and I/O to verify that they are wired as documented in the schematics.		
5	Visually inspect the RSLogix 5000 program to verify that safety system network and I/O modules are configured as documented.		
6	Visually inspect the RSLogix 5000 application program to verify suitable safety-certified instructions are utilized. The logic is readable, understandable and testable with the aid of clear comments.		
7	All input devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags window.		
8	All output devices are qualified by cycling their respective actuators. Monitor the status in the RSLogix 5000 Controller Tags window.		

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

Normal Operation Verification - The safety system properly responds to all normal Start, Stop, SLS, E-Stop, Lock and Reset commands.			
Test Step	Verification	Pass/Fail	Changes/Modifications
1	Initiate a Start Command. The drive should energize for a normal machine run condition. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
2	Initiate a Stop command. The drive should de-energize immediately for a normal machine Stop condition. After the preset time delay, verify the door unlocks. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
3	While the system is running, attempt to open the guard door. The door should remain closed and locked. The drive should remain energized for a normal run condition. Verify proper machine status indication and RSLogix 5000 safety application program indication. Repeat for all guard doors.		
4	While the system is stopped, attempt to open the guard door. The door should be unlocked and able to be opened. The drive should remain de-energized for a normal safe condition. Verify proper machine status indication and RSLogix 5000 safety application program indication. Repeat for all guard doors.		
5	While the system is stopped with the guard door open, initiate a Start command. The drive should remain de-energized for a normal safe condition. Verify proper machine status indication and RSLogix 5000 safety application program indication. Repeat for all guard doors.		
6	Initiate a Safe Limited Speed request. The drive should energize and run at the predefined safe limited speed. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
7	Initiate a Reset command. The drive should remain de-energized. Verify proper machine status indication and RSLogix 5000 safety application program indication.		

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

Abnormal Operation Validation - The safety system properly responds to all foreseeable faults with corresponding diagnostics.

PowerFlex 750 Safe Speed Monitor Option Module SLS Door Monitoring and Lock Input Tests

Test Step	Validation	Pass/Fail	Changes/Modifications
1	While the system is running, remove the Door Monitor Channel 1 wire from the safe speed (SLS) module. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2.		
2	While the system is running, short the Door Monitor Channel 1 of the safe speed (SLS) module to +24V DC. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2		
3	While the system is running, short the Door Monitor Channel 1 of the safe speed (SLS) module to 0V DC. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2.		
4	While the system is running, short the Door Monitor Channels 1 and 2 of the safe speed (SLS) module. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and Channel 2 wiring.		
5	While the system is running, short Channel 1 to Test Source 1 of the safe speed (SLS) module. Open the guard door. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 wiring and repeat for Channel 2.		
6	While the system is running, remove the Lock Monitor Channel 1 wire from the safe speed (SLS) module. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2.		

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

Abnormal Operation Validation - The safety system properly responds to all foreseeable faults with corresponding diagnostics.

PowerFlex 750 Safe Speed Monitor Option Module SLS Door Monitoring and Lock Input Tests

Test Step	Validation	Pass/Fail	Changes/Modifications
7	While the system is running, short the Lock Monitor Channel 1 of the safe speed (SLS) module to 24V DC. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2.		
8	While the system is running, short the Lock Monitor Channel 1 of the safe speed (SLS) module to 0V DC. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and repeat for Channel 2.		
9	While the system is running, short the Lock Monitor Channels 1 and 2 of the safe speed (SLS) module. The drive should de-energize. Verify proper machine status indication and RSLogix 5000 safety application program indication. Verify that the drive is unable to reset and restart with a fault. Restore Channel 1 and Channel 2 wiring.		

GuardLogix Controller and Safety I/O Network Tests

Test Step	Validation	Pass/Fail	Changes/Modifications
1	While the system is running, remove the Ethernet network connection between the safety I/O module and the controller. The drive should de-energize. Verify proper machine status indication and I/O Connection Status in the RSLogix 5000 safety application program.		
2	Restore the safety I/O module network connection and allow time to reestablish communication. Verify the Connection Status bit in the RSLogix 5000 safety application program. Repeat for all safety I/O module connections.		
3	While the system is running, switch the controller out of Run mode. The drive should de-energize. Return the keyswitch back to Run mode. The drive should remain de-energized. Verify proper machine status indication and RSLogix 5000 safety application program indication.		

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

PowerFlex 750 Safe Speed Monitor Option Module SS and SLS Control and Lock Output Tests			
Test Step	Validation	Pass/Fail	Changes/Modifications
1	Initiate a Start command. The drive should energize for a normal machine run condition. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
2	While the system is running, remove Channel 1 SS Input from the safe speed (SLS) module. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		
3	While the system is running, short Channel 1 SS Input of the safe speed (SLS) module to 24V DC. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		
4	While the system is running, short Channel 1 SS Input of the safe speed (SLS) module to 0V DC. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		
5	While the system is running, short Channels 1 and 2 SS Input of the safe speed (SLS) module. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and 2 wiring.		
6	While the system is running, remove Channel 1 SLS Input from the safe speed (SLS) module. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		
7	While the system is running, short Channel 1 SLS Input of the safe speed (SLS) module to 24V DC. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		

GuardLogix & PowerFlex 750 Safe Speed with Guard Locking Safety Function Verification and Validation Checklist (continued)

PowerFlex 750 Safe Speed Monitor Option Module SS and SLS Control and Lock Output Tests			
Test Step	Validation	Pass/Fail	Changes/Modifications
8	While the system is running, short Channel 1 SLS Input of the safe speed (SLS) module to 0V DC. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and repeat for Channel 2.		
9	While the system is running, short Channels 1 & 2 SLS Input of the safe speed (SLS) module. The Drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore Channel 1 and Channel 2 wiring.		
10	While the system is stopped, remove the safety output to the door lock solenoid. The door should remain locked and the drive should remain de-energized. Verify proper machine status indication and RSLogix 5000 safety application program indication.		
PowerFlex 750 Safe Speed Monitor Option Module SS and SLS Control and Lock Output Tests			
Test Step	Validation	Pass/Fail	Changes/Modifications
11	While the system is running, remove the SS Output status of the safe speed (SLS) module. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore wiring.		
12	While the system is running, remove the SLS Output status of the safe speed (SLS) module. The drive should de-energize. Attempt a Reset command. The system should not restart or reset. Verify proper machine status indication and RSLogix 5000 safety application program indication. Restore wiring.		

Additional Resources

For more information about the products used in this application, refer to these resources.

Resource	Description
Compact GuardLogix Controllers User Manual, publication 1768-UM002	Provides information on configuring, operating, and maintaining Compact GuardLogix controllers.
POINT Guard I/O Safety Modules Installation and User Manual, publication 1734-UM013	Provides information on installing, configuring, and operating POINT Guard I/O modules.
GuardLogix 5560 Controller Systems Safety Reference Manual, publication 1756-RM093	Provides detailed requirements for achieving and maintaining safety ratings with the GuardLogix 5560 and Compact GuardLogix controller systems.
GuardLogix 5570 Controller Systems Safety Reference Manual, publication 1756-RM099	Provides detailed requirements for achieving and maintaining safety ratings with the GuardLogix 5570 controller systems.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides detailed information on the GuardLogix Safety Application Instruction Set.
Safety Accelerator Toolkit for GuardLogix Systems Quick Start Guide, publication IASIMP-QS005	Provides a step-by-step guide to using the design, programming, and diagnostic tools in the Safety Accelerator Toolkit.

[Safety Products Catalog](#)

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

For More Information on
Safety Function Capabilities, visit:

discover.rockwellautomation.com/safety

Rockwell Automation, Allen-Bradley, GuardLogix, RSLogix 5000, CompactLogix, Stratix 2000, POINT Guard I/O, and Rockwell Software are trademarks of Rockwell Automation, Inc. Trademarks not belonging to Rockwell Automation are property of their respective companies.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

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

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

Publication SAFETY-AT027D-EN-E – March 2013

Supersedes Publication SAFETY-AT027C-EN-E – January 2013

Copyright © 2013 Rockwell Automation, Inc. All rights reserved. Printed in U.S.A.