

E-stop String Safety Function

Products: 800F E-stop, Guardmaster Single-input Safety Relay, 100S Safety Contactors

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



Topic	Page
Summary of Changes	3
General Safety Information	3
Introduction	4
Use Sample Project Files	4
Safety Function Realization: Risk Assessment	5
Emergency Stop (E-stop) Safety Function	5
Safety Function Requirements	5
Functional Safety Description	6
Bill of Material	6
Setup and Wiring	6
Configuration	9
Calculation of the Performance Level	9
Verification and Validation Plan	12
Additional Resources	12

Important User Information

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

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

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

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

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

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

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

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



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



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

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

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



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



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



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

Summary of Changes

This publication contains new and updated information as indicated in the following table.

Topic	Pages
Added new SISTEMA graphics to the section titled Calculation of the Performance Level.	9...11
Updated the section titled Functional Safety Data Required for Determining the Performance Level of Electromechanical Devices.	11
Attached an updated SISTEMA file to this publication:	Attachments pane

General Safety Information

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

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



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

Safety Distance Calculations



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

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

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

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

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

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

Introduction

This application technique describes how power is removed from a hazard when a safety system detects that an E-stop has been actuated.

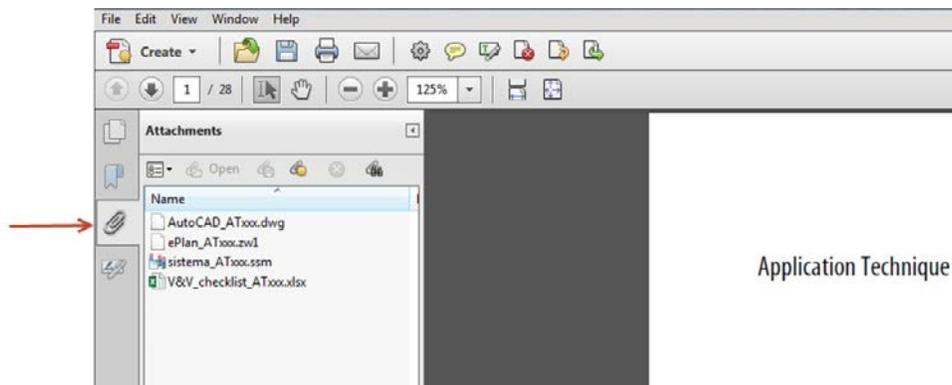
ISO 13849-1 directs that when devices are connected in a series, such as the three E-stops used in this application technique, the function of each device is evaluated as a separate safety function. In this application technique, the three E-stops are evaluated as three, identical E-stop safety functions.

Use Sample Project Files

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

To access these files, follow these steps.

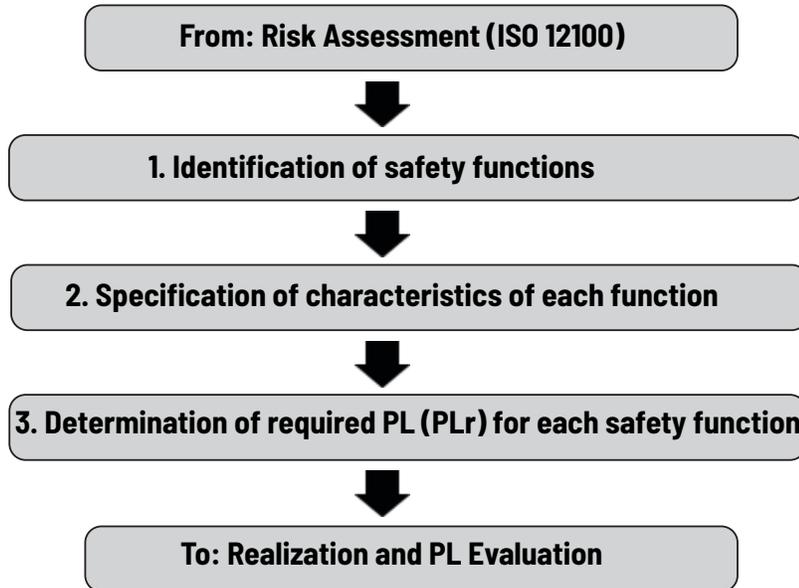
1. If you are viewing the PDF file in a browser and do not see the Attachments link , download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link .
3. Right-click and save the desired file.



4. Open the file in the appropriate application.

Safety Function Realization: Risk Assessment

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



Emergency Stop (E-stop) Safety Function

This application technique includes three safety functions:

- E-stop function 1
- E-stop function 2
- E-stop function 3

Safety Function Requirements

When you press any one of the series-wired E-stops, this action stops and prevents hazardous motion by removal of power to the motor. When you reset the E-stop button, hazardous motion and power to the motor do not resume until a secondary action (pressing the Start button) occurs. Faults at the E-stop button, wiring terminals, or safety relay are detected before the next safety demand. The emergency stop functions are complementary to any other safeguards on the machine and do not reduce the performance of other safety-related functions. The safety functions in this example are able to connect and interrupt power to motors rated up to 9 A, 600V AC.

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

Functional Safety Description

Three E-stop buttons are connected in a series to the Guardmaster® single-input safety relay. One channel runs through the three E-stops between pulsed output S11 and input S12, and the other channel runs between pulsed output S21 and input S22. The safety relay monitors the pulse stream at each input to confirm that each E-stop channel is in a proper state. When you press any E-stop button, these two circuits are interrupted. The Guardmaster single-input safety relay responds to this circuit interruption by opening its safety contacts (13...14 and 23...24), which de-energizes the coils of K1 and K2. With power removed, the hazardous motion coasts to a stop (stop category 0). The hazardous motion cannot be started until the E-stop is released, and then the reset button is pressed and released.

To confirm the proper state of the two 100S safety contactors before permitting a start or reset, run 24V power in a series through an N.C. auxiliary contact on each 100S contactor to the Reset button of the Guardmaster single-input safety relay. If a safety contact of one or both 100S contactors is welded closed, the corresponding auxiliary N.C. contact is held open, which breaks the 24V circuit to the Reset button.

The Guardmaster single-input safety relay in this application example is configured for monitored manual (MM) reset. When the E-stop inputs are in the proper state and the two 100S contactors are properly de-energized, pressing and releasing the Reset button results in the Guardmaster single-input safety relay energizing the two 100S safety contactors. If you press the Reset button for less than 0.250 seconds, or longer than 3 seconds, the safety relay does not reset. This feature prevents unintentional reset and thwarts 'tie-down' of the Reset button.

Bill of Material

This application technique uses these products.

Cat. No.	Description	Quantity
800F-TYP3	800F one-hole enclosure E-stop station, plastic, PG, twist-to-release, 40 MM, non-illuminated, 2 N.C.	2
800F-BX10	N.O. status contact (add one to each 800F-TYP3)	2
800FM-G611MX10	800F push button, metal, guarded, blue, R, metal latch mount, 1 N.O. contact, no N.C. contact, standard, standard pack	2
440R-S12R2	Guardmaster single-input safety relay (SI), 1 dual-channel universal input, 1 N.C. solid-state auxiliary output	1
100S-C09EJ23C	MCS 100S-C safety contactor, 9A, 24V DC	2

Setup and Wiring

For detailed information on how to install and wire the products in this safety function, refer to the publications in [Additional Resources on page 12](#).

System Overview

The pulsed outputs of the Guardmaster single-input safety relay (terminals S11 and S21) are run separately through the E-stop contact strings (E-stop 1 to E-stop 2 to E-stop 3) to input terminals S12 and S22, respectively. This configuration enables the Guardmaster single-input safety relay to detect a loose wire, a short to 24V, a short to GND, and cross channel faults. There is the possibility that a contact in one of the E-stops could fail closed and that this failure could be masked by the operation of the other E-stops. This masking reduces the effective Diagnostic Coverage (DCAvg) of each E-stop. This lower DCAvg reduces the maximum performance level of each of the three E-stop safety functions to PLd and the category structure becomes CAT 3.

The Guardmaster single-input safety relay responds to E-stop inputs and detected E-stop circuit faults by opening its safety contacts (13...14 and 23...24), and this action de-energizes the coils of K1 and K2. The Guardmaster single-input safety relay cannot be reset until the E-stop is released, or the fault is corrected. In some cases, the E-stop has to be pressed and released before the Guardmaster single-input safety relay can be reset. After some faults, the safety relay must be power-cycled once the fault is cleared before it can be reset.

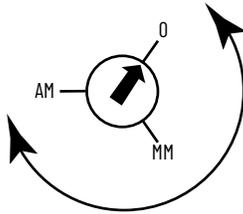
The Guardmaster single-input safety relay monitors itself for any internal faults. When a fault is detected, the Guardmaster single-input safety relay responds by opening its safety contacts (13...14 and 23...24), and this action de-energizes the coils of the K1 and K2 contactors. Some internal faults can be cleared by power-cycling the Guardmaster single-input safety relay. In other cases, the Guardmaster single-input safety relay must be replaced.

The Guardmaster single-input safety relay monitors the 100S contactors for welded contacts via feedback from two N.C. contacts in a series, one from each 100S, in its reset circuit. If a contact of a 100S is welded, the N.C. contact is held open, which breaks the reset circuit.

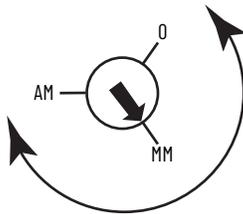
Configuration

The Guardmaster single-input safety relay must be configured for a monitored manual (MM) reset.

1. With power off, turn the configuration switch to 0.



2. Apply power to the safety relay.
After the power-up test, the PWR status indicator flashes red.
3. Turn the configuration switch to MM.



The IN 1 status indicator blinks the new setting.



The position is set when the PWR status indicator is solid green.

4. To lock in the configuration, cycle power to the safety relay.
Configuration must be confirmed before operation. A white space, which is on the face of the relay, is provided to record the device setting.

Calculation of the Performance Level

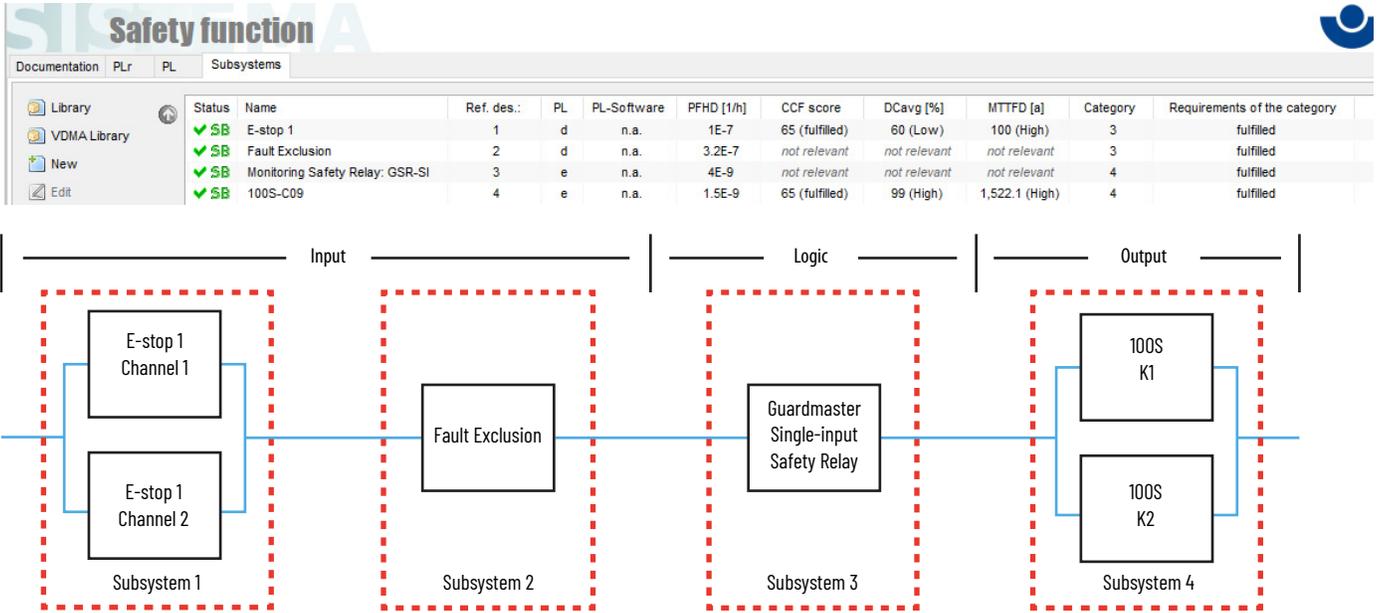
When properly implemented, each of the three E-stop safety functions can achieve a safety rating of category 3, Performance Level d (cat. 3, PLd), according to ISO 13849-1: 2015, as calculated by using the Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA).

The SISTEMA file that is referenced in this safety function application technique is attached to this document. For instructions on how to access the attachments, see [Use Sample Project Files on page 4](#).

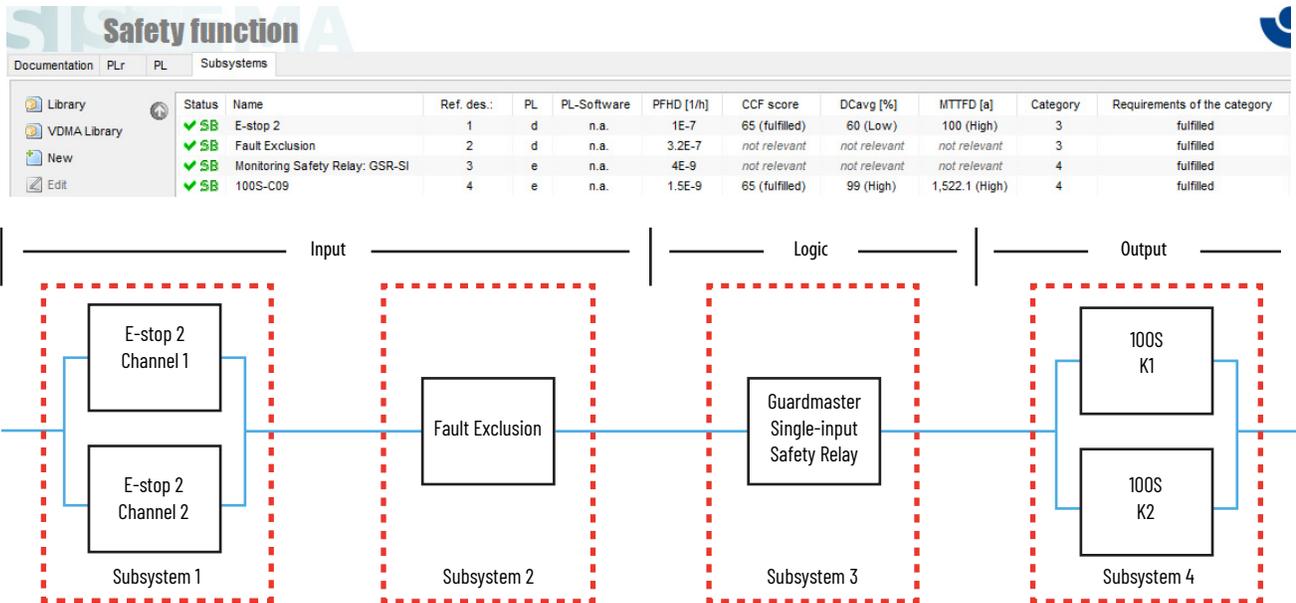
The PFH for electromechanical subsystems may be calculated differently based on the version of ISO 13849 supported by SISTEMA. ISO 13849-1:2015, which changed the maximum MTTFd from 100 to 2500 years, is supported starting in version 2.0.3 of SISTEMA. As a result, the same SISTEMA data file that is opened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

Project SISTEMA					
Documentation		Safety functions			
	Status	Name	Type	PLr	PL
New	✓ SF	E-stop 1	Emergency stop function	d	d
Edit	✓ SF	E-stop 2	Emergency stop function	d	d
Delete	✓ SF	E-stop 3	Emergency stop function	d	d

E-stop 1 can be modeled as follows.

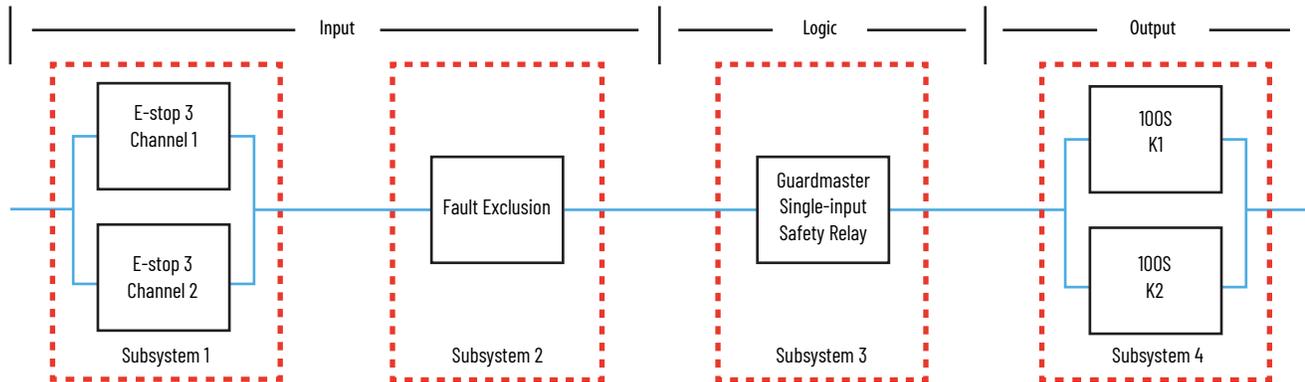


E-stop 2 can be modeled as follows.



E-stop 3 can be modeled as follows.

Safety function											
Documentation PLr PL Subsystems											
Library	Status	Name	Ref. des.:	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
VDMA Library	✓SB	E-stop 3	1	d	n.a.	1E-7	65 (fulfilled)	60 (Low)	100 (High)	3	fulfilled
New	✓SB	Fault Exclusion	2	d	n.a.	3.2E-7	not relevant	not relevant	not relevant	3	fulfilled
Edit	✓SB	Monitoring Safety Relay: G...	3	e	n.a.	4E-9	not relevant	not relevant	not relevant	4	fulfilled
	✓SB	100S-C09	4	e	n.a.	1.5E-9	65 (fulfilled)	99 (High)	1,522.1 (High)	4	fulfilled



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

Because these devices are electromechanical devices, the safety contactor data includes the following:

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

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

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

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

The DCavg for each E-Stop subsystem is entered as 60% to take into account the possible masking of faults due to the E-stops being connected in series.

Detection of a single fault can be masked when multiple E-stops with redundant contacts are connected in series to the same safety logic device. The fault is masked from the logic device by actuation of the other devices (E-stops) in series with the faulty device. The fault can be undetected. The possible fault and fault exclusion are identified in the safety function documentation with the Fault Exclusion subsystem.

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

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

If the maximum number of operations of an electromechanical emergency stop device is in accordance with IEC60947- 5-5, regarding the mechanical aspects of the device, exclusion of the possible fault of the single actuator of that device failing to

switch the two channels properly is allowed per EN ISO 13849-2, Annex D, Table D8. Therefore, single types of devices, properly applied, are not limited and can achieve Performance Level e.

The emergency stop function is a complementary protective measure which is intended to be used in conjunction with other safeguarding measures and protective devices to sufficiently reduce risk. The design of the emergency stop functions shall not impair the effectiveness of other safety functions or protective devices in the system. The actual number of operations (NOP) is used for the purposes of the MTTFd calculation in this document.

Verification and Validation Plan

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

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

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

Before validating the system, confirm that the Guardmaster safety relay has been wired and configured in accordance with the installation instructions.

For a validation checklist, see the attached spreadsheet. For instructions on how to access the attachments, see [Use Sample Project Files on page 4](#).

Additional Resources

These documents contain more information about related products from Rockwell Automation.

Resource	Description
Guardmaster Safety Relay SI Installation Instructions, publication 440R-IN042	Provides information on how to install, configure, and program the Guardmaster single-input safety relay.
Guardmaster Safety Relays User Manual, publication 440R-UM013	Provides instructions on how to install, configure, and troubleshoot the Guardmaster single-input safety relay.
Lifeline™ 5 Cable-pull Safety Switch Installation Instructions, publication 440E-IN008	Provides instructions on how to install, configure, and maintain the Lifeline 5 cable-pull safety switch.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines on how to install a Rockwell Automation industrial system.
Safety Solutions website, http://marketing.rockwellautomation.com/safety-solutions/en/	Provides information about Rockwell Automation safety products.
Product Certifications website, rok.auto/certifications	Provides declarations of conformity, certificates, and other certification details.

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

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Safety Function Capabilities

Visit rok.auto/safety for more information on our Safety System Development Tools, including [Safety Functions](#).

Allen-Bradley, expanding human possibility, Guardmaster, Lifeline, Rockwell Automation, and SensaGuard are trademarks of Rockwell Automation, Inc. Trademarks not belonging to Rockwell Automation are property of their respective companies.

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

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

Connect with us.    

rockwellautomation.com ————— expanding **human possibility**[®]

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

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

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

UNITED KINGDOM: Rockwell Automation Ltd. Pitfield, Kiln Farm Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917