Safety Chain Solution

Guard Monitoring with Coded Magnetic Switches, Safety Module, and Variable Speed Drive

STO, Performance Level PL e

05/2020

SCS1204.01

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

QUALIFICATION OF PERSONNEL

Only appropriately trained persons who are familiar with and understand the contents of the present documentation and all other pertinent product documentation as well as all documentation of all components and equipment of the machine/process in which the Safety Chain Solution is used are authorized to work on and with this Safety Chain Solution.

The qualified person must be a certified expert in safety engineering.

The qualified person must be able to detect possible hazards that may arise from parameterization, modifying configurations, settings, and wiring, and generally from mechanical, electrical, or electronic equipment. The qualified person must be able to understand the effects that modifications to configurations, settings, and wiring may have on the safety of the machine/process.

The qualified person must be familiar with and understand the contents of the risk assessment as per ISO 12100 and/or any other equivalent assessment as well as all documents related to such risk assessment or equivalent assessments for the machine/process.

The qualified person must be familiar with the standards, provisions, and regulations for the prevention of industrial accidents, which they must observe when designing, implementing, and maintaining the machine/process.

The qualified person must be thoroughly familiar with the safety-related applications and the non-safety-related applications used to operate the machine/process in which the Safety Chain Solution is employed.

INTENDED USE

The Safety Chain Solution described in the present document is a combination of products intended to perform a safety-related function in a machine/process according to the present document, to the specified related documents, and to all other documentation of the components and equipment of the machine/process.

The Safety Chain Solution may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data.

Prior to using the Safety Chain Solution, you must perform a risk assessment as per ISO 12100 in view of the planned application. Based on the results of the risk assessment, all necessary safety-related measures must be implemented.

Since the Safety Chain Solution is used as a component in an overall machine or process, you must ensure the safety of persons by means of the design of this overall machine or process.

Operate the products only with the specified cables and accessories. Use only genuine accessories and spare parts.

Any use other than the use explicitly permitted as described herein is prohibited and may result in unanticipated hazards.

About the Book

At a Glance

Document Scope

The Safety Chain Solution described in the present document is a combination of safety-related Schneider Electric products used to implement a safety-related function for a machine as per ISO 13849-1.

The present document delineates the interaction of the products and summarizes various safety-related and non-safety-related characteristics of these products.

In addition, the present document provides information on a number of non-safety-related products that can be used to complement the Safety Chain Solution.

The present document is not intended as a substitute for and is not to be used for determining the suitability of the Safety Chain Solution for any specific application. It is the sole responsibility of any user, machine designer, system integrator, or other party using the Safety Chain Solution in any way whatsoever to determine such suitability for any specific application or use thereof in compliance with all applicable regulations, standards, and directives, and in compliance with all pertinent documentation of all products used in such application. Neither Schneider Electric nor any of its affiliates or subsidiaries are responsible or liable for misuse of the information contained herein.

Validity Note

The present document is valid for the safety-related products comprising the Safety Chain Solution. Refer to Related Documents *(see page 7)* for information on the corresponding User Guides and additional documentation.

The Schneider Electric Machine Safety website at *www.schneider-electric.com/machinesafety* contains references to standards, specifications, and guides to assist you in understanding and determining the validity of the information in this document.

The technical characteristics of the devices described in the present document also appear online. To access the information online, visit the Schneider Electric website at *www.schneider-electric.com*.

The characteristics that are presented in the present document should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the document and online information, use the online information as your reference.

For product compliance and environmental information (RoHS, REACH, PEP, EOLI, etc.), go to *www.schneider-electric.com/green-premium*.

Related Documents

Documents for safety-related products:

Title of documentation	Reference number
XCS DMC / DMP / DMR (EAC) Coded Magnetic Switches, Instruction Sheet	*AAV82775*
XPSUS Safety Module, User Guide	*EIO0000003487*
XPSUS Safety Module, Instruction Sheet	*PHA71847*
ATV340 Variable Speed Drive, Installation Manual	*NVE61069*
ATV340 Variable Speed Drive, Programming Manual	*NVE61643*
ATV340 Variable Speed Drive, Embedded Safety Function Manual (STO)	*NVE64143*

Documents for non-safety-related, associated products:

Title of documentation	Reference number
XPSUEP Extension Module for Safety Module, User Guide	*EIO0000003509*
XPSUEP Extension Module for Safety Module, Instruction Sheet	*PHA71854*

Title of documentation	Reference number
XB4 XB4B, XB5A, ZB4B, ZB5A Push Buttons, Instruction Sheet	*65013-037-26*
XVU••• Modular Tower Lights, Instruction Sheet	*HRB1831101*
Modicon M221 Logic Controller, Hardware Guide	*EIO0000001384*

You can download these technical publications and other technical information from our website at *www.schneider-electric.com/en/download*.

Product Related Information

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Where 24 Vdc or Vac is indicated, use PELV power supplies conforming to IEC 60204-1.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to this equipment.
- Use only the specified voltage when operating this equipment and any associated products.

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines.[1]
- Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

⚠ WARNING

INSUFFICIENT AND/OR INEFFECTIVE SAFETY-RELATED FUNCTIONS

- Perform a risk assessment as per ISO 12100 and/or other equivalent assessment and appropriately consider all applicable regulations and standards that apply to your machine/process before using the Safety Chain Solution.
- In your risk assessment, verify that the Safety Chain Solution meets all requirements regarding the Safety Integrity Level (SIL), the Performance Level (PL), and any other safety-related requirements and capabilities applicable to your machine/process.
- In your risk assessment, consider all pertinent manuals and documentation of all products used in the Safety Chain Solution.
- Verify that modifications to parameter values, settings, wiring, and any other type of modification to your machine/process, do not compromise or reduce the Safety Integrity Level (SIL), Performance Level (PL) and/or any other safety-related requirements and capabilities applicable to your machine/process.
- After modifications of any type whatsoever, commission or recommission the machine/process in compliance with all regulations, standards, and process definitions applicable to your machine/process.
- During commissioning or recommissioning of the machine/process, verify the correct operation and effectiveness of all safety-related functions and non-safety-related functions by performing comprehensive tests for all operating states, for the defined safe state of the Safety Chain Solution and the defined safe state of your machine/process, and for all potential error situations.
- Do not include any wiring information, programming or configuration logic, parameter values, or any other type of settings described in the present document in your machine/process without thoroughly testing your entire application.
- Ensure that your overall machine/process in which the Safety Chain Solution is used is properly certified and/or approved according to all standards, regulations, and directives applicable at the installation site of the machine/process.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

IEC 61800-5-2 defines the safety-related sub-function Safe Torque Off (STO) for adjustable speed electrical power drive systems (PDS). STO corresponds to a stop with stop category 0 as per IEC 60204-1.

As opposed to a stop with stop category 1 as per IEC 60204-1 which actively decelerates the motor to a standstill (power available to the motor to achieve the stop) before power is removed, a stop with STO (stop category 0) immediately removes power to the motor. Consequently, the motor coasts down to a standstill. Coasting down is subject to the external forces interacting with the load, such as inertia and gravity.

⚠ WARNING

INSUFFICIENT AND/OR INEFFECTIVE SAFETY-RELATED FUNCTIONS

- Verify that your risk assessment takes into account all potential consequences that can arise from coasting down of the motor from its maximum velocity and under maximum load conditions to a standstill.
- Take into account that the defined safe state of the Safety Chain Solution (STO active, power to motor removed) does not necessarily coincide with the safe state of your machine/process as identified in your risk assessment.
- Use this Safety Chain Solution only in conjunction with all necessary additional safety-related measures and/or equipment such as appropriate distances between the guards and hazardous machine parts and/or additional external brakes if your risk assessment shows that the defined safe state of this Safety Chain Solution and the defined safe state of your machine/process do not coincide.
- Verify that the safe state of your machine/process as defined by you in your risk assessment can be reached under all conditions and in all operating states, including all potential error situations.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING
UNINTENDED EQUIPMENT OPERATION • Only use software approved by Schneider Electric for use with this equipment. • Update your application program every time you change the physical hardware configuration. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in this manual, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2015	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2015	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive* (*2006/42/EC*) and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Standards Relating to the Safety Chain Solution

The following list provides an overview of the standards that relate to the Safety Chain Solution:

Standard	Title
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
ISO 13849-1:2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
ISO 13849-2:2012	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 14120:2015	Safety of machinery - Guards - General requirements for the design and construction of fixed and movable guards
IEC 60204-1:2016	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
IEC 60947-5-1:2016	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
IEC 61800-5-2:2016	Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional

Do not consider this list to be exhaustive. For example, additional standards, regulations, and directives may apply to the design of your specific application and your implementation of the Safety Chain Solution. The fact that a given standard is included in the table does not imply that any of the individual products of the Safety Chain Solution or the Safety Chain Solution as a whole meet the requirements of such standard. Consult the User Guides of the products and visit the Schneider Electric website at *www.schneider-electric.com* for product certifications which detail compliance with specific standards, regulations, and directives.

Chapter 1
Function Principle, Applications and Hardware Overview

What Is in This Chapter?

This chapter contains the following topics:

Function Principle

Function Principle of the Safety Chain Solution

The Safety Chain Solution monitors two movable guards as per ISO 14119/14120 to restrict access to the zone of operation of a machine while the machine is in operation. The Safety Chain Solution implements a safety-related stop function as per ISO 13849-1. This safety-related stop function is triggered if a guard is opened.

Each guard is equipped with a coded magnetic switch. The outputs of the coded magnetic switches are connected to the inputs of a safety module.

The outputs of the safety module are connected to two safety-related inputs of a variable speed drive.

As long as the guards are closed, access to the zone of operation is restricted as provided by your risk assessment and the corresponding design of your specific application.

When one of the guards is opened, for example, to allow for machine operator access to the zone of operation, the outputs of the coded magnetic switch mounted to this guard change state.

The changed signal state of the coded magnetic switch is detected by the safety module. In response, the safety module deactivates its outputs.

This causes the variable speed drive connected to the safety module to trigger a stop with stop category 0 of the motor as per IEC 60204-1 via its integrated safety-related sub-function Safe Torque Off (STO).

If the safety module or the variable speed drive detect errors such as indeterminable signal states, or short circuits or cross circuits at the inputs, STO is triggered or STO remains activated if it had already been triggered before the error was detected.

Refer to the chapter Safety-Related Design and Structure *(see page 20)* for additional information on the design, monitoring, and diagnostics features of the Safety Chain Solution.

Function Principle of Complementary, Non-Safety-Related Components

The Safety Chain Solution comprises complementary, non-safety-related components.

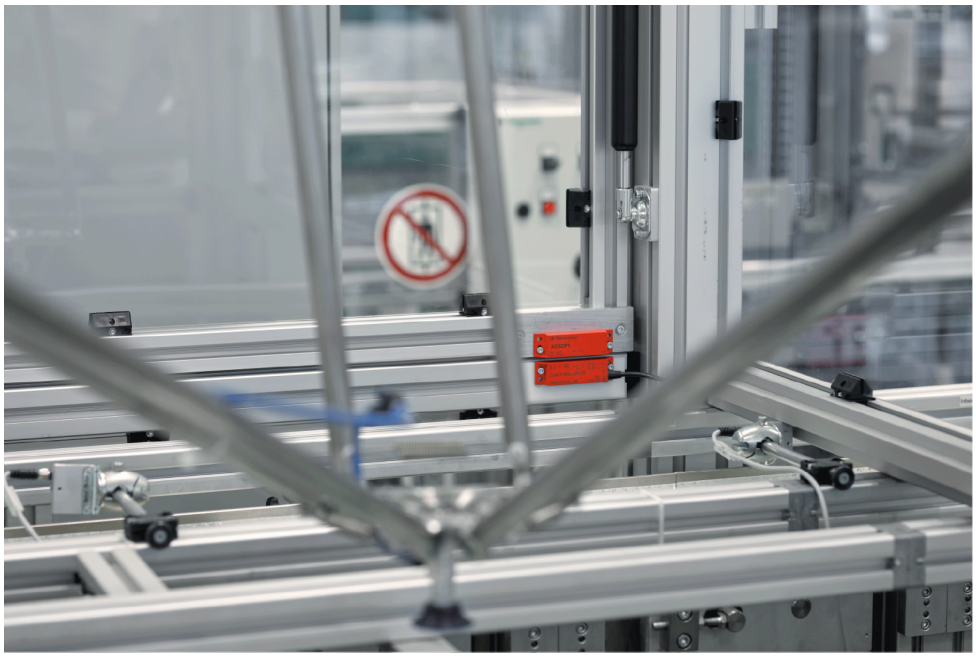
The safety module is equipped with an extension module providing additional safety-related outputs. In the Safety Chain Solution, these outputs are used for non-safety-related purposes. A signaling unit is connected to the outputs of the extension module. The signaling unit indicates the state of the guards by means of a green light (guard closed) and a red light (guard open).

A push-button is used to provide a start/restart signal for the safety module (manual start/restart). The machine can only start/restart if the guards are closed, and if the start/restart push-button is pressed (external start/restart condition), and if no errors are detected.

Status information and diagnostics information on the safety module is available to, for example, a logic controller via a binary, non-safety-related output of the safety module. This status information can be evaluated, for example, for predictive maintenance. EcoStruxure™ Machine Expert - Basic 1.0 SP1 or greater provides an application example (template xSample_PreventaSupport).

Typical Applications

Typical Applications



The Safety Chain Solution is typically used in assembly machines, packaging machines and similar compact machines that require frequent access to the zone of operation.

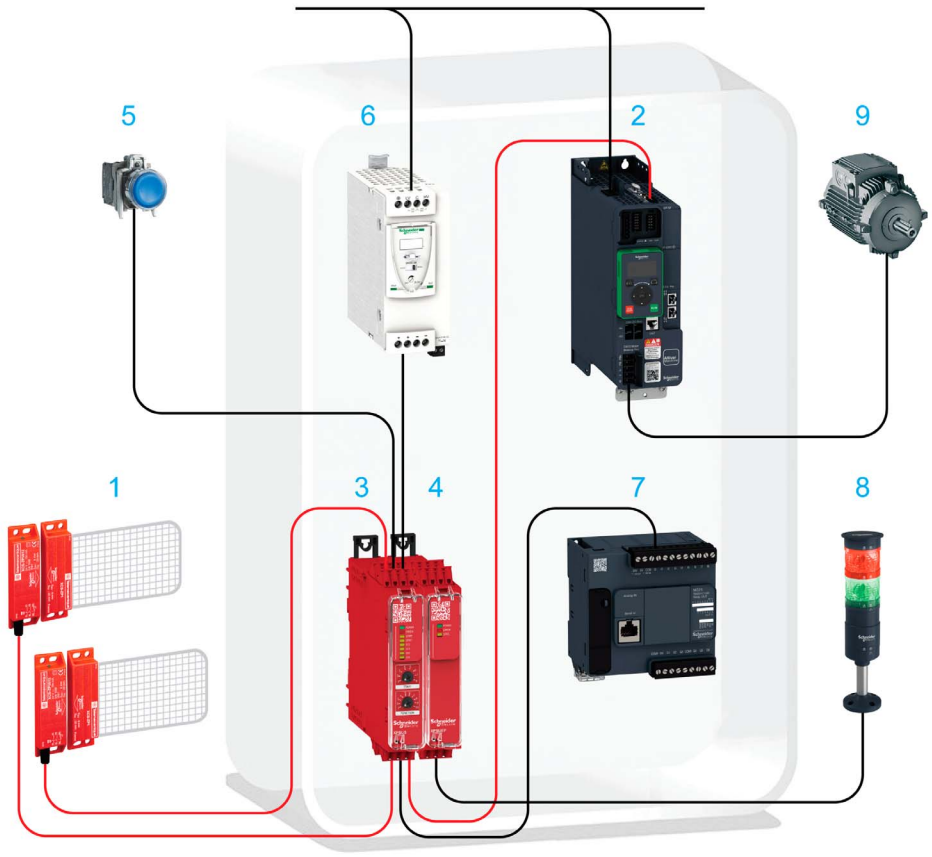
Such machines need to be suitable for stops with stop category 0, that is, the time after removal of power to the motor and coasting of the load to standstill is sufficiently short (refer to Defined Safe State and Safety-Related Sub-Function Safe Torque Off (STO) *(see page 22)* for details).

Hardware Overview

Hardware Overview

Hardware Overview

The Safety Chain Solution comprises the following devices:



Safety-related connections are represented by red lines, non-safety-related connections by black lines.

The following table identifies the safety-related devices of the Safety Chain Solution:

Number	Device	Remarks
1	XCSDMP590L01M12	Two coded magnetic switches with antivalent outputs (one NO, one NC each)
2	ATV340U07N4E	Variable speed drive with integrated safety-related sub-function STO
3	XPSUS12A•	Safety module

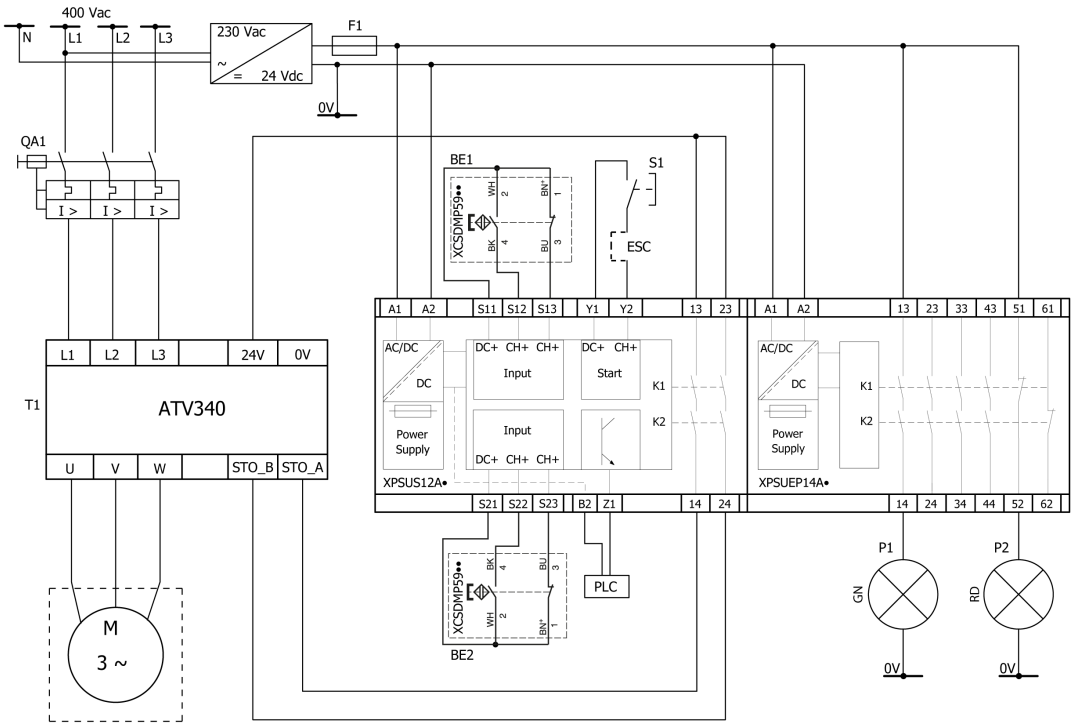
The following table identifies the non-safety-related devices of the Safety Chain Solution:

Number	Device	Remarks
4	XPSUEP14•	Extension module with additional outputs for safety module XPSUS12A• The extension module provides safety-related outputs. However, in this Safety-Chain Solution, they are used for non-safety-related purposes.
5	Harmony XB4	Push-button for manual start/restart. This push-button is used to provide the signal to exit the defined safe state of the Safety Chain Solution. It does not start/restart the overall machine or process.
6	ABL•••	Power supply
7	M221 Logic controller	Digital input connected to status output of safety module
8	XVU••• Modular Tower Lights	Signaling unit with red and green lights
9	Motor	-

Chapter 2
Wiring

Wiring Diagram

Wiring Diagram



Legend:

Designation	Device and remarks
ESC	Optional external start/restart condition
S1	Pushbutton XB4 for manual start/restart
PLC	M221 logic controller (connect the logic controller to terminal B2 of the safety module to obtain a common reference potential)

Refer to the user guides *(see page 7)* of the corresponding devices for additional information on electrical installation and technical data such as further wiring diagrams, wire cross sections, tightening torques, maximum cable lengths, fuse ratings, etc.

Wiring Information

The wiring must meet the requirements of IEC 60204-1. You must take all necessary measures against short circuits as specified by ISO 13849-2, table D.4 and by all other standards, regulations, and electrical code requirements applicable to your application.

The start/restart pushbutton is connected to the start/restart input Y1/Y2 of the safety module. The start/restart input of the safety-module is not safety-related. Install the start/restart pushbutton outside the zone of operation in a position that allows the operator to verify that no persons are in the zone of operation and no hazards are present before the start/restart pushbutton is pressed. Ensure that all necessary organizational measures are taken (such as, but not limited to, operator training, efficient access control to manually operated equipment, or hazard signs), as determined by your risk assessment.

Chapter 3
Safety-Related Design and Defined Safe State

What Is in This Chapter?

This chapter contains the following topics:

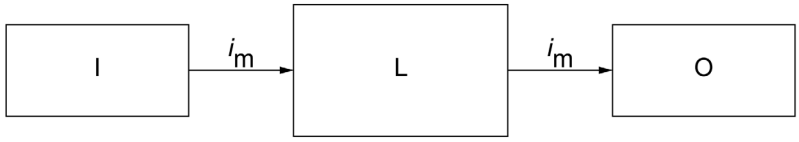
Safety-Related Design and Structure

Overview

The Safety Chain Solution is a combination of safety-related parts of a control system as defined by ISO 13849-1. A safety-related part of a control system is a part that responds to safety-related input signals and generates safety-related output signals. The following sections describe the structure of the Safety Chain Solution as well as various design features and monitoring/diagnostic functions implemented to achieve the safety-related capabilities.

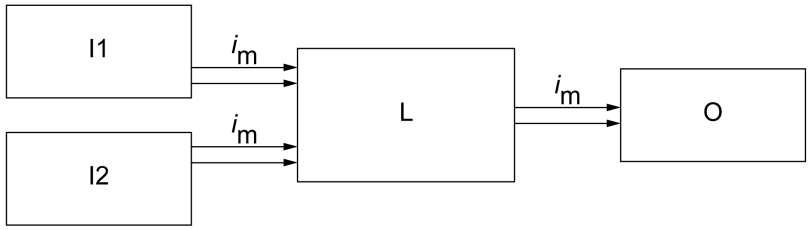
Dual-Channel Structure

As defined by ISO 13849-1, a functional channel in a control system is a channel consisting of an input device, a logic or processing device, and an output device. The following figure provides an overview of these safety-related parts of a control system:



I = Input
im = Interconnecting means
L = Logic
O = Output

The Safety Chain Solution provides dual-channel operation. It uses two redundant functional channels as illustrated in the following figure.



Each coded magnetic switch represents one input device (I1 and I2). The safety module represents the logic unit (L). The variable speed drive represents the output device (O).

Note that I1-L-O and I2-L-O are two separate functional channels, each of them being redundant.

Redundancy

The components of the Safety Chain solution meet the redundancy requirements for dual-channel operation.

- Coded magnetic switches
  Each coded magnetic switch provides two antivalent outputs: one normally closed contact and one normally open contact.
- Safety module
  The safety module has redundant safety-related inputs, independent processing units featuring cross-monitoring, and redundant safety-related outputs for dual-channel operation.
- Variable speed drive
  The variable speed drive provides two signal inputs for the safety-related sub-function STO. In addition, it uses two independent logic units with cross-monitoring to process STO.
- Wiring
  The signal cables for the wiring between the coded magnetic switches and the safety module and the variable speed drive are redundant.

Monitoring for Synchronous Signal Behavior and Consistent Signal States

- Safety module: Monitoring for synchronized activation of inputs
  The safety module monitors for synchronized operation of the two antivalent output contacts of each coded magnetic switch. If the two output contacts of a coded magnetic switch are not activated (NO closes, NC opens) within the synchronization time of 0.5 seconds, the safety-related outputs of the safety module are not activated. In such a case, the safety-related sub-function STO remains triggered and the Safety Chain Solution stays in the defined safe state.
- Safety module: Monitoring for consistent input signal states
  If the safety module detects identical states of the input signal from the coded magnetic switch (NO closed and NC closed or NO open and NC open) outside of the synchronization time, it triggers the safety-related sub-function STO.
- Variable speed drive: Monitoring for consistent input signal states
  If the level at one of the inputs STO_A and STO_B changes to 0 V, the safety-related sub-function STO is triggered. If the level at the other input does not change to 0 V within one second as well, an error is detected. The Safety Chain Solution remains in the defined safe state (STO active) until the cause of the error is removed and the variable speed drive is power cycled.
  The variable speed drive only deactivates the safety-related sub-function STO if the levels at the inputs STO_A and STO_B change to 24 V within less than one second.

Dynamization of Inputs for Cross Circuit Detection

- Safety module
  The safety module uses dynamization for detection of cross circuits between two of its safety-related inputs, or between one of its safety-related inputs and of its start/restart input, or of a cross circuit to an external power supply unit or to ground. Dynamization is implemented by means of periodically generated test pulses at the control outputs of the safety-related inputs and the start/restart input.
  If the safety module detects a cross circuit, the safety-related sub-function STO is activated or remains active and the Safety Chain Solution transitions to or stays in its defined safe state until the cause of the error is removed and the safety module is power cycled.

Defined Safe State and Safety-Related Sub-Function Safe Torque Off (STO)

Defined Safe State of the Safety Chain Solution

In the defined safe state of the Safety Chain Solution, the safety-related sub-function STO as per IEC 61800-5-2 is active. No torque-producing power is provided to the motor.

IEC 61800-5-2 defines the safety-related sub-function Safe Torque Off (STO) for adjustable speed electrical power drive systems (PDS). STO corresponds to a stop with stop category 0 as per IEC 60204-1.

As opposed to a stop with stop category 1 as per IEC 60204-1 which actively decelerates the motor to a standstill (power available to the motor to achieve the stop) before power is removed, a stop with STO (stop category 0) immediately removes power to the motor. Consequently, the motor coasts down to a standstill. Coasting down is subject to the external forces interacting with the load, such as inertia and gravity.

Depending on your application, STO may not be sufficient to remove all hazards. For example, the available rotational or axial distance required to come to a complete standstill by coasting down may not be sufficient at a specific load. This could result in collisions of machine parts. In addition, the distance between the guard and hazardous machine parts must be sufficiently great so that a machine operator can only reach such parts after the coasting period has finished. Such distances are specified, for example, in ISO 13855.

⚠ WARNING

INSUFFICIENT AND/OR INEFFECTIVE SAFETY-RELATED FUNCTIONS

- Verify that your risk assessment takes into account all potential consequences that can arise from coasting down of the motor from its maximum velocity and under maximum load conditions to a standstill.
- Take into account that the defined safe state of the Safety Chain Solution (STO active, power to motor removed) does not necessarily coincide with the safe state of your machine/process as identified in your risk assessment.
- Use this Safety Chain Solution only in conjunction with all necessary additional safety-related measures and/or equipment such as appropriate distances between the guards and hazardous machine parts and/or additional external brakes if your risk assessment shows that the defined safe state of this Safety Chain Solution and the defined safe state of your machine/process do not coincide.
- Verify that the safe state of your machine/process as defined by you in your risk assessment can be reached under all conditions and in all operating states, including all potential error situations.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Relationship Between Defined Safe State of the Safety Chain Solution and Safe State of Your Machine/Process

Relationship Between Defined Safe State of the Safety Chain Solution and Safe State of Your Machine/Process

Take into account that the defined safe state of the Safety Chain Solution is not necessarily identical to the defined safe state of your overall machine or process. For example, a stop with stop category 0 may imply that no torque-producing power is supplied but that the load is still in the process of coasting down to a standstill while access to the zone of operation is already possible, depending on your specific application. You must therefore meticulously align the defined safe state of the Safety Chain Solution and the defined safe state of your overall machine or process as determined by your risk assessment.

Typically, the defined safe state of a machine is a complete stop of machine functions identified to be hazardous. This means that you have to consider, among other things, the overall stopping performance as per, for example, ISO 13855, in your risk assessment and machine design.

ISO 13855 defines the overall stopping performance as T = t1 + t2 with:

- T = Overall stopping performance of entire system
- t1 = Maximum time between actuation of safeguard and output signal of output device reaching the deactivated state (this corresponds to the total response time of the Safety Chain Solution; within this response time, the Safety Chain Solution reaches its defined safe state)
- t2 = Stopping time, which is the maximum time required to terminate hazardous machine functions after the output device has reached the deactivated state (this corresponds to the time between reaching the defined safe state of the Safety Chain Solution and reaching the safe state of your machine as defined by, for example, your risk assessment)

A required minimum distance between the guard and the closest point of your machine presenting a potential hazard is a function of, among other things, the overall stopping performance, represented by S = (K x T) + C with:

- S = Minimum distance between guard closest point of your machine presenting a potential hazard
- K = Approach speed (different values apply, for example, walking speed or approach speed of a hand)
- T = Overall stopping performance of entire system
- C = Intrusion distance (corresponds to an additional distance that may be required depending on, for example, the resolution of the detection capabilities of a sensor and specific parts of the body to be detected such as an arm)

NOTE: Additional standards, regulations, and directives may apply to the determination of the stopping performance, required distances and other parameters determining the safe state of your machine/process. Perform such calculations and design your machine in compliance with all applicable standards, regulations, and directives.

Chapter 4
Characteristics and Safety-Related Calculations

Characteristics and Calculations

Data Functional Safety of Components of Safety Chain Solution

The following table lists specific safety-related technical data of the individual components of the Safety Chain Solution. Values that are not contained in the technical data of a component, but need to be calculated are explained in footnotes.

Characteristic	Coded magnetic switch XCSDMP590L01M12	Safety module XPSUS12A•	Variable speed drive ATV340U07N4E, STO
Maximum Performance Level (PL), Category (as per ISO 13849-1:2015)	PL e, Category 4	PL e, Category 4	PL e, Category 3
Mean number of cycles until 10% of the components fail dangerously (B_{10D}) (as per ISO 13849-1:2015)	50000000	n/a	n/a
Probability of Dangerous Failure per hour (PFH_D) in 1/h (as per ISO 13849-1:2015)	9.06×10^{-10} (1)	1.13×10^{-9}	3.00×10^{-10}
Mean Time To Dangerous Failure ($MTTF_d$) in years (as per ISO 13849-1:2015)	2500 (2)	>30	7000
Average Diagnostic Coverage (DC_{avg}) (as per ISO 13849-1:2015)	99 % (3)	≥99 %	90 %
Lifetime	20	20	20
Response time in ms	3.5 (4)	<20	<10

(1) Determined according to ISO 13849-1, table K.1 with category 4 at DC_{avg} = high and $MTTF_D$ limited to the appropriate value.
(2) Value calculated on the basis of the assumed number of cycles for the overall Safety Chain Solution and reduced according to applicable category for determination of PFH_D as per ISO 13849-1, table K.1.
(3) Assumed value based on plausibility check performed by safety module as per ISO 13849-1, annex E, table E.1.
(4) Calculated on the basis of the frequency of 150 Hz specified for the component. This value is also valid for the other coded magnetic switches of the XCSDMC, XCSDMP, and XCSDMR ranges with two antivalent contacts. Therefore, the other coded magnetic switches with two antivalent contacts of these ranges can be used for this Safety Chain Solution as well. No new calculation of the safety-related values is required.

NOTE: Refer to the user guides *(see page 7)* of the individual devices for additional data on functional safety.

Calculations and Data Functional Safety of Overall Safety Chain Solution

The following table summarizes the assumptions serving as a basis for the calculation of the functional safety data of the overall Safety Chain Solution:

Characteristic	Value
Number of operations of safety-related function per hour	6
Number of hours of machine operation per day (h_{op})	24
Number of days of machine operation per year (d_{op})	365
Number of operations of safety-related function per year (n_{op})	52560

On the basis of these assumption, the Safety Chain Solution achieves the following functional safety data:

Characteristic	Value
Performance Level (PL) (as per ISO 13849-1:2015)	e

Characteristic	Value
Probability of Dangerous Failure per hour (PFH_D) in 1/h (as per ISO 13849-1:2015)	2.34×10^{-9}
Total response time between request of safety-related function and activation of STO in ms (corresponds to t1 *(see page 23)*)	<33.5

NOTE: If you modify any of the input values for the calculation, you must re-perform the calculation.

NOTE: The calculations are available as a SISTEMA project on the Schneider Electric Machine Safety website at *www.schneider-electric.com/machinesafety*. SISTEMA is the Safety Integrity Software Tool for the Evaluation of Machine Applications available at *IFA*. Depending on the settings you use in SISTEMA (such as number of decimals), the values may slightly differ from the values listed in the present document.

The Performance Level specified for the Safety Chain Solution is only achieved if your implementation of the Safety Chain Solution meets all applicable requirements as per ISO 13849-1.

In your implementation of the Safety Chain Solution, use the required “well-tried safety principles” as defined by ISO 13849-2, table D.2.

The measures against Common Cause Failures (CCF) taken in your implementation of the Safety Chain Solution must reach a score of at least 65 according to Annex F, ISO 13849-1, for example, segregation/separation (15), protection against overvoltage (15), environmental (EMC) (25), environmental (immunity to environmental influences other than EMC) (10).

Environmental Conditions

Your implementation of the Safety Chain Solution must meet the following environmental conditions:

Characteristic	Coded magnetic switch XCSDMP590L01M12	Safety module XPSUS12A•	Variable speed drive ATV340U07N4E, STO
Ambient temperature, operation	-25 ... 85 °C (-13 ... 185 °F)	-25 ... 55 °C (-13 ... 131 °F)	-15 ... 50 °C (5 ... 122 °F) With derating: 50 ... 60 °C (122 ... 140 °F)
Ambient humidity, operation	n/a	5 ... 95 %, no condensation	5 ... 95 %, no condensation
Maximum installation altitude above mean sea level	n/a	2000 m (6562 ft)	1000 m (3281 ft) With current derating of 1 % per 100 m (328 ft): 1000 ... 2000 m (3281 ... 6,562 ft)
Degree of protection	IP67	Terminals: IP20 Housing: IP40	IP20
Installation required in control cabinet (degree of protection)	No	Yes (IP54)	Yes (IP54)

NOTE: Refer to the user guides *(see page 7)* of the individual devices for additional environmental conditions to be met for storage and transportation.

Chapter 5
Configuration and Parameterization

Configuration and Parameterization of Safety-Related Components

Coded Magnetic Switches

The coded magnetic switches do not require configuration. The output signal is available after correct installation of the coded magnetic switches and wiring of the outputs to the specified inputs of the safety module.

Safety Module - Application Function Selector

Set the application function selector of the safety module to position 5 (monitoring of guards as per ISO 14119/ISO 14120 with coded magnetic switches). This application function uses synchronization *(see page 21)* and dynamization *(see page 21)*.

Safety Module - Start/Restart Function Selector

Set the start/restart function selector to position 1 or to position 2.

- Position 1: Manual start/restart with dynamization, without startup test
- Position 2: Manual start/restart with dynamization, with startup test

The startup test is used to verify correct operation of the sensors. It provides additional diagnostics within the Safety Chain Solution. When the safety module is powered on, the safety-related inputs of the safety module must be deactivated and activated before the safety-related outputs can be activated. This is achieved by opening all guards and then closing all guards.

Variable Speed Drive

The safety-related sub-function STO of the variable speed drive does not require configuration or parameterization. STO is available after correct installation of the variable speed drive and wiring of the two inputs `STO_A` and `STO_B` to the specified outputs of the safety module.