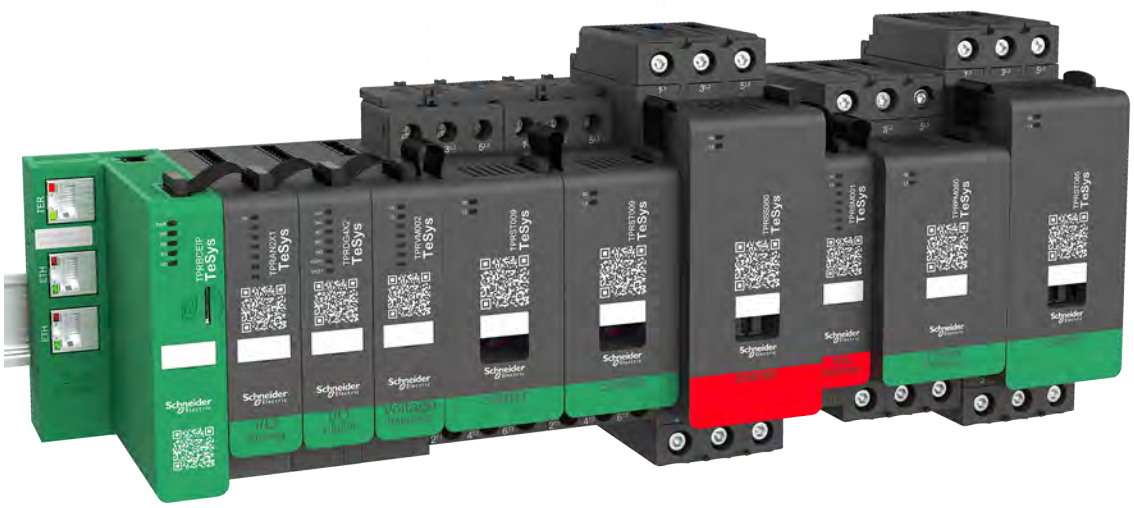
TeSys™ island

Functional Safety Guide

Instruction Bulletin

This instruction bulletin describes the TeSys island functional safety features.

8536IB1904EN
Release date: 06/2019



www.schneider-electric.com

Legal Information

Table of Contents

Hazard Categories and Special Symbols

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 bulletin or on the equipment to warn of hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either 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 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.

NOTE: Provides additional information to clarify or simplify a procedure.

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, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

About the Book

Document Scope

Use this document to learn more about the following TeSys™ island functional safety features:

- general understanding
- key aspects to consider
- performances
- hardware description
- typical configurations
- sample architectures
- standards references

Validity Note

This instruction bulletin is valid for all TeSys™ island configurations. The availability of some functions described in this bulletin depends on the communication protocol used and the physical modules installed on the island.

For product compliance with environmental directives such as RoHS, REACH, PEP, and EOLI, go to *www.se.com/green-premium*.

For technical characteristics of the physical modules described in this bulletin, go to *www.se.com*.

The technical characteristics presented in this bulletin should be the same as those that appear online. We may revise content over time to improve clarity and accuracy. If you see a difference between the information contained in this bulletin and online information, use the online information.

Related Documentation

Table 1 - Related Documentation

Document Title	Description	Document Number
TeSys™ island System Guide	Introduces and describes the main functions of TeSys island	8536IB1901
TeSys™ island Installation Guide	Describes the mechanical installation, wiring, and commissioning of TeSys island	8536IB1902
TeSys™ island Operating Guide	Describes how to operate and maintain TeSys island	8536IB1903
TeSys™ island Functional Safety Guide	Describes the Functional Safety features of TeSys island	8536IB1904
TeSys™ island Third Party Function Block Guide	Contains the information needed to create function blocks for third party hardware	8536IB1905
TeSys™ island EtherNet/IP™ Function Block Library Guide	Describes the TeSys island library used in the Rockwell Software® Studio 5000® environment	8536IB1914
TeSys™ island EtherNet/IP™ Quick Start Guide	Describes how to quickly integrate TeSys island into the Rockwell Software Studio 5000 environment	8536IB1906
TeSys™ island DTM Online Help Guide	Describes how to install and use various functions of TeSys island configuration software and how to configure the parameters of TeSys island	8536IB1907
TeSys™ island Product Environmental Profile	Describes constituent materials, recyclability potential, and environmental impact information for the TeSys island.	ENVPEP1904009
TeSys™ island Product End of Life Instructions	Contains end of life instructions for the TeSys island	ENVEOLI1904009
TeSys™ island Instruction Sheet, Bus Coupler	Describes how to install the TeSys island bus coupler	MFR44097
TeSys™ island Instruction Sheet, Starters and Power Interface Modules, Size 1 and 2	Describes how to install size 1 and 2 TeSys island starters and power interface modules	MFR77070
TeSys™ island Instruction Sheet, Starters and Power Interface Modules, Size 3	Describes how to install size 3 TeSys island starters and power interface modules	MFR77085
TeSys™ island Instruction Sheet: Input/Output Modules	Describes how to install the TeSys island analog and digital I/O modules	MFR44099
TeSys™ island Instruction Sheet: SIL Interface and Voltage Interface Modules	Describes how to install the TeSys island voltage interface modules and SIL interface modules	MFR44100

Terminology Derived from Standards

The technical terms, terminology, and the corresponding descriptions in this instruction bulletin normally use the terms or definitions in the relevant standards.

In the area of TeSys™ island this includes, but is not limited to, terms such as error, error message, failure, fault, fault reset, protection, safe state, safety function, safety related, warning, warning message, and so on.

Among others, these standards include:

- **EN ISO 13849-1:** Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

- **EN ISO 13849-2:** Safety of machinery – Safety-related parts of control systems – Part 2: Validation
- **IEC 61508:** Functional safety of Electrical / Electronic / Programmable Electronic safety-related systems
- **EN 62061:** Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- **IEC 61511:** Functional safety – Safety instrumented systems for the process industry sector
- **EN 60204-1:** Safety of machinery – Electrical equipment of machines – Part 1: General requirements
- **IEC 61000-6-7:** Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations
- **IEC 60664-5:** Insulation coordination for equipment within low-voltage systems – Part 5: Comprehensive method for determining clearances and creepage distances equal to or less than 2 mm
- **IEC 60947-4-1:** Low-voltage switchgear and control gear – Part 4-1: Contactors and motor-starters – Electromechanical contactors and motor-starters
- **IEC 60947-5-1:** Low-voltage switchgear and control gear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices
- **IEC 60947-7-1:** Low-voltage switchgear and control gear – Part 7-1: Ancillary equipment – Terminal blocks for copper conductors
- **IEC 60947-7-2:** Low-voltage switchgear and control gear – Part 7-2: Ancillary equipment – Protective conductor terminal blocks for copper conductors
- **EN 50205:** Relays with forcibly guided (mechanically linked) contacts
- **IEC TR 62380:** Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment

Functional Safety Terminology

ATTENTION

The functional safety terminology used in this instruction bulletin is defined below.

Term	Standard	Definition
Fault Tolerance	IEC 61511–1	Ability of a functional item to continue to perform a required function in the presence of faults or errors
Safe State	IEC 61511-1	State of the process when safety is achieved
	IEC 61800-5–2	State of the PDS(SR)[1] when safety is achieved
Safe Stop	IEC 61800-5-2	The Safe Stop functions are defined as: • **Safe Stop 1 (SS1)** ◦ Safe Stop 1 deceleration controlled: SS1-d initiates and controls the motor deceleration rate within selected limits to stop the motor and performs the STO function (see 4.2.3.2) when the motor speed is below a specified limit; or ◦ Safe Stop 1 ramp monitored: SS1-r initiates and monitors the motor deceleration rate within selected limits to stop the motor and performs the STO function when the motor speed is below a specified limit; or ◦ Safe Stop 1 time controlled SS1-t initiates the motor deceleration and performs the STO function after an application specific time delay.
Safety Function	IEC 61800-5-2	Function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the equipment or machinery driven by the PDS(SR)[1], in respect of a specific hazardous event
Safety Integrity Level (SIL)	IEC 61508	The standard IEC 61508 defines four Safety Integrity Levels (SILs) for safety functions: SIL 1 is the lowest integrity level and SIL 4 is the highest. A hazard analysis and risk assessment serves as a basis for determining the required safety integrity level.
Safety Related System	IEC 61800-5-2	Designated system that both • implements the required safety functions necessary to achieve or maintain a safe state for the equipment or machinery driven by the PDS (SR)[1]; and • is intended to achieve, on its own or with other risk reduction measures, the necessary safety integrity for the required safety functions
Subsystem	IEC 61800-5-2	Part of the top-level architectural design of a safety-related system, failure of which results in failure of a safety-related function

EC Declaration of Conformity

The EC Declarations of Conformity for TeSys™ island can be obtained on *www.schneider-electric.com*.

1. Safety related power drive systems

Precautions

Read and understand the following precautions before performing any procedures in this guide.

⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified electrical personnel.
- Turn off all power supplying this equipment before working on or inside this equipment.
- Use only the specified voltage when operating this equipment and any associated products.
- Always use a properly rated voltage sensing device to confirm power is off.
- Use appropriate interlocks where personnel and/or equipment hazards exist.
- Power line circuits must be wired and protected in compliance with local and national regulatory requirements.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices per NFPA 70E, NOM-029-STPS, or CSA Z462 or local equivalent.

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

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- For complete instructions about functional safety, refer to the *TeSys™ island Functional Safety Guide*, 8536IB1904.
- Do not disassemble, repair, or modify this equipment. There are no user serviceable parts.
- Install and operate this equipment in an enclosure appropriately rated for its intended application environment.
- 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.

⚠ **WARNING:** This product can expose you to chemicals including Antimony oxide (Antimony trioxide), which is known to the State of California to cause cancer. For more information go to *www.P65Warnings.ca.gov*.

Qualified Personnel

Only appropriately trained persons who are familiar with and understand the content of this guide and all other related product documentation are authorized to work on and with this product.

The qualified person must be able to detect possible hazards that may arise from modifying parameter values and generally from mechanical, electrical, or electronic equipment. The qualified person must be familiar with the standards, provisions, and regulations for the prevention of industrial accidents, which they must observe when designing and implementing the system.

The use and application of the information contained in this guide requires expertise in the design and programming of automated control systems. Only you,

the user, machine builder, or integrator, can be aware of all the conditions and factors present during installation, setup, operation, and maintenance of the machine or process, and can therefore determine the automation and associated equipment and the related safeties and interlocks which can be effectively and properly used.

When selecting automation and control equipment, and any other related equipment or software, for a particular application, you must also consider applicable local, regional, or national standards and/or regulations.

Pay particular attention to conform to any safety information, electrical requirements, and normative standards that apply to your machine or process in the use of this equipment.

Intended Use

The products described in this instruction bulletin, together with software, accessories, and options, are starters for low-voltage electrical loads, intended for industrial use according to the instructions, directions, examples, and safety information contained in this document and other supporting documentation.

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

Before using the product, you must perform a hazard analysis and risk assessment of the planned application. Based on the results, appropriate safety-related measures must be implemented.

Since the product is used as a component of a machine or process, you must ensure the safety of persons by means of the overall system design.

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

Any use other than the use explicitly permitted is prohibited and can result in unanticipated hazards.

TeSys™ island Functional Safety Overview

Island Concept

TeSys™ island is an innovative digital load management solution—providing data for higher machine efficiency and ease of servicing, and allowing faster time to market.

TeSys island is a modular, multifunctional system providing integrated functions inside an automation architecture, primarily for the direct control and management of low-voltage loads. TeSys island can switch, help protect, and manage motors and other electrical loads up to 80 A (AC3) installed in an electrical control panel.

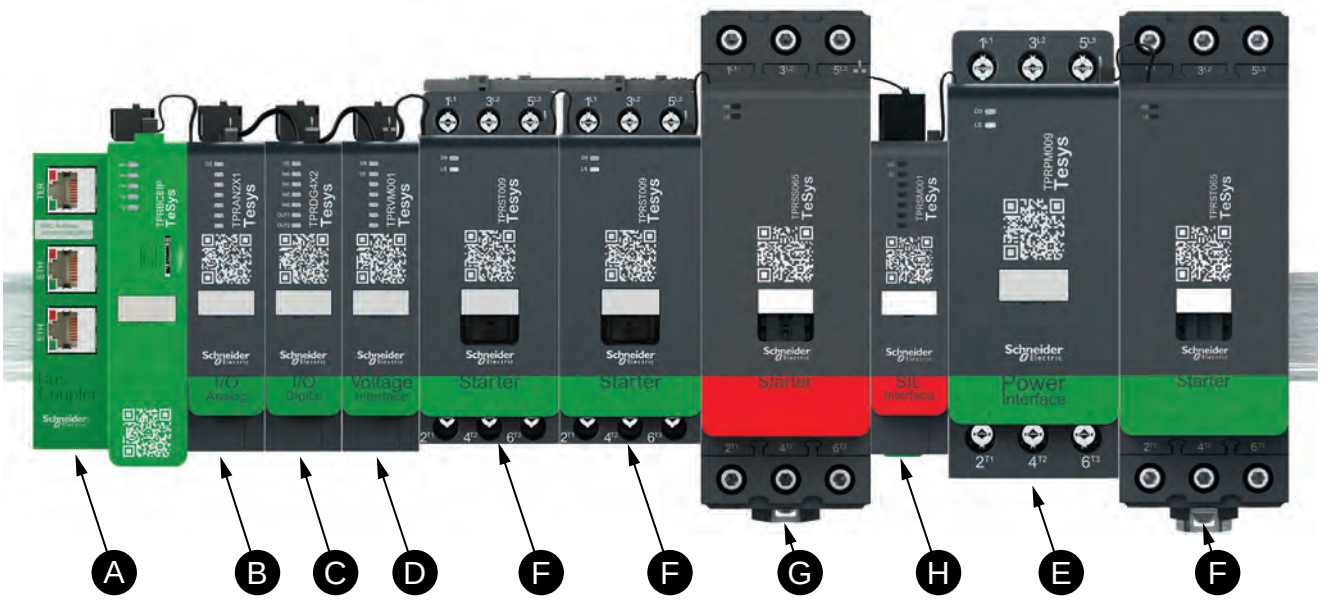
This system is designed around the concept of TeSys Avatars. These Avatars

- Represent both the logical and physical aspects of the automation functions
- Determine the configuration of the island

The logical aspects of the island are managed with software tools, covering all phases of product and application lifecycle: design, engineering, commissioning, operation, and maintenance.

The physical island consists of a set of devices installed on a single DIN rail, and connected together with flat cables providing the internal communication between modules. The external communication with the automation environment is made through a single bus coupler module, and the island is seen as a single node on the network. The other modules include starters, power interface modules, analog and digital I/O modules, voltage interface modules, and SIL (Safety Integrity Level according to standard IEC 61508) interface modules, covering a wide range of operational functions.

Figure 1 - TeSys island Overview



A	Bus Coupler	E	Power Interface Module
B	Analog I/O Module	F	Standard Starter
C	Digital I/O Module	G	SIL Starter
D	Voltage Interface Module	H	SIL Interface Module

Functional Safety in TeSys island

TeSys™ island provides specific avatars and physical devices to build configurations for Stop Category 0 and Stop Category 1 functions according to EN 60204-1. TeSys avatars are digital representations of the physical modules on the island, however, the TeSys island safety function relies only on electro-mechanical hardware components. The specific devices are the SIL starter and SIL interface module. Another important concept is the SIL group: a set of avatars that are associated to one SIL interface module and follow the same safety function. Multiple SIL groups are possible within an island.

TeSys island must be integrated with other safety-related elements in a broader safety-related system to help ensure the functional safety of a machine or a system/process.

TeSys island Functional Safety Characteristics

TeSys™ island provides Functional Safety features in compliance with these specific conditions:

- *Standards and Certified Characteristics, page 13*
- *Operating Conditions, page 14*
- *Single-Channel Architecture (ISO 13849), page 14*
- *Stop Categories (EN 60204-1), page 15*
- *Categories (ISO 13849), page 15*
- *Acceptance Test, page 16*

Standards and Certified Characteristics

TeSys island follows these directives and standards:

- Machinery Directive 2006/42/CE:
  - EN ISO 13849-1: 2015
  - EN 62061: 2005
- Functional safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508 edition 2: 2010
- Functional safety – Safety instrumented systems for the process industry sector: IEC 61511 edition 2: 2016
- TeSys island Stop Category 0 and Stop Category 1 functions follow EN 60204-1.

In single channel, the highest performances for those functions are:

- Performance Level “d” Category 2 in compliance with EN ISO 13849-1
- SIL 2 capability in compliance with IEC 61508 Ed 2 and IEC 61511 Ed 2
- SIL CL 2 capability in compliance with EN 62061 Ed 1

TeSys island is designed to support different functional safety performance levels and safety integrity levels depending on its wiring architecture.

TeSys island is compliant with the following functional safety characteristics:

Table 2 - Functional Safety Characteristics

Function	Safety-related stop function
Fallback position	Open contactor
Response time (worst case)	145 ms
Stop Category EN 60204-1	Cat. 0/Cat. 1
Machinery Directive	Yes
TeSys island system architecture	Single channel
Performance Level EN ISO 13849-1	PL c, d
Category EN ISO 13849-1	Cat 1, 2
SIL CL EN 62061	SIL CL 2
SIL IEC 61508/IEC 61511	SIL 2

The certificate for functional safety is accessible on *www.se.com/tesys/*.

NOTE: For certification relating to functional aspects, only a TeSys island suitable for use in safety-related applications will be considered, not the complete system into which it is integrated to help to ensure the functional safety of a machine or a system/process.

Operating Conditions

TeSys™ island is designed to durably sustain the following conditions. Other conditions may apply to specific modules as described in their data sheet document, available on *www.se.com/tesys*.

- 40 °C (104 °F) ambient temperature
- 400/480 V motor
- 50% humidity
- 80% load
- Horizontal mounting orientation
- All inputs activated
- All outputs activated
- 24 hours/day, 365 days/year run time

Single-Channel Architecture (ISO 13849)

TeSys island is applicable to single-channel architectures in which a detected fault can lead to the loss of the safety function.

Stop Categories (EN 60204-1)

The stop category relates to the way the driven load is de-energized and depends on the external safety-related sub-system that triggers the Stop function. An external safety-related sub-system can be implemented with devices such as the Preventa™ XPS modules.

Stop Category 0

Stop Category 0 is defined as stopping the machine motion by immediate removal of electrical power from the machine actuators. Stop Category 0 is an uncontrolled stop.

Stop Category 1

Stop Category 1 is defined as stopping the machine motion with electrical power maintained to the machine actuators during the stop process. Power is removed when the stop is complete. Stop Category 1 is a controlled stop.

Categories (ISO 13849)

Wiring categories relate to the way the external Preventa™ XPS module (or equivalent) is wired, and to the associated additional level of control over the safety function.

Wiring Category 1

A single detected fault may lead to the loss of the safety function and no diagnostic coverage is required.

The safety-related sensor element can be directly wired to the SIL-IN/SIL Common inputs. The Mirror In/Mirror Out inputs are not used. For more information on wiring the SIL-IN/SIL Common inputs, see *Safety-Related Sensor Element, page 20*.

Wiring Category 2

The safety-related sensor element is wired to a Preventa XPS module (or equivalent). The Preventa XPS module (or equivalent) outputs are wired to the SIL-IN/SIL Common inputs of the SIL interface module.

To meet the requirement for Category 2, the mirror contact feedback (Mirror In/Mirror Out) must be monitored by a Preventa XPS module (or equivalent) that performs external diagnostic monitoring of the mirror contact. If the mirror contact does not open on stop, the next restart is prevented to all SIL starters in the SIL group.

Implementing Indirect Monitoring for Category 2

In order to reach category 2 requirements for diagnostic coverage (DC>60%), external monitoring of the group status should be implemented to trigger a secondary mechanism to stop the machine (breaker shunt trip, etc.) or to prevent access to dangerous areas (guard lock).

Each SIL group has five states associated with it to indicate the operational state. State 0 indicates there is not a SIL group present in this slot. TeSys island supports up to 10 SIL groups in the island.

SIL group status for Safe Stop 0 function:

- 0 = SIL group not present in system configuration
- 1 = SIL group impacted by Avatar Device Event
- 2 = Safe Stop Command received, SIL starters not open yet
- 3 = Safe Stop Command successfully issued, all SIL starters are open
- 4 = Safe Stop Command issued to only one SIM input channel (jumper or SIM input wiring is causing an issue), but SIL starters did successfully open
- 5 = Normal operation, SIL starters can be open or closed

State 5 is the normal run state, and State 3 is the normal Safe Stop state. State 1 indicates a firmware or communication issue with a SIL starter. States 2 and 4 indicate Safe Stop related problems with the SIM, SIL Starters or Safe Stop wiring. Indirect monitoring should look for states 2 or 4 to persist for longer than the actuation time of a Safe Stop and use the status information to trigger a secondary mechanism to stop the machine (breaker shunt trip, etc.).

To read the SIL group status, the external monitoring must use the SystemDiagnostics function block. Each SIL group in the system has an output on this function block for its SIL group status, labeled on the function block as “SafeStopMsgGrp *n*,” where *n* is the SIL group number in the island. The SIL group status follows the enumeration shown above.

Diagnostic Monitoring

As the diagnostic monitoring occurs immediately upon demand of the safety function, the overall time to detect the fault and to bring the machine to a non-hazardous condition should be shorter than the time to reach the hazardous area.

According to ISO 13849-2, 9.2.3, for Category 2: The $MTTF_d$ of the monitoring equipment should be greater than half of the $MTTF_d$ of the logic. The contribution of the TeSys island to the $MTTF_d$ of the diagnostic monitoring is $MTTF_d$ > 100 years.

Acceptance Test

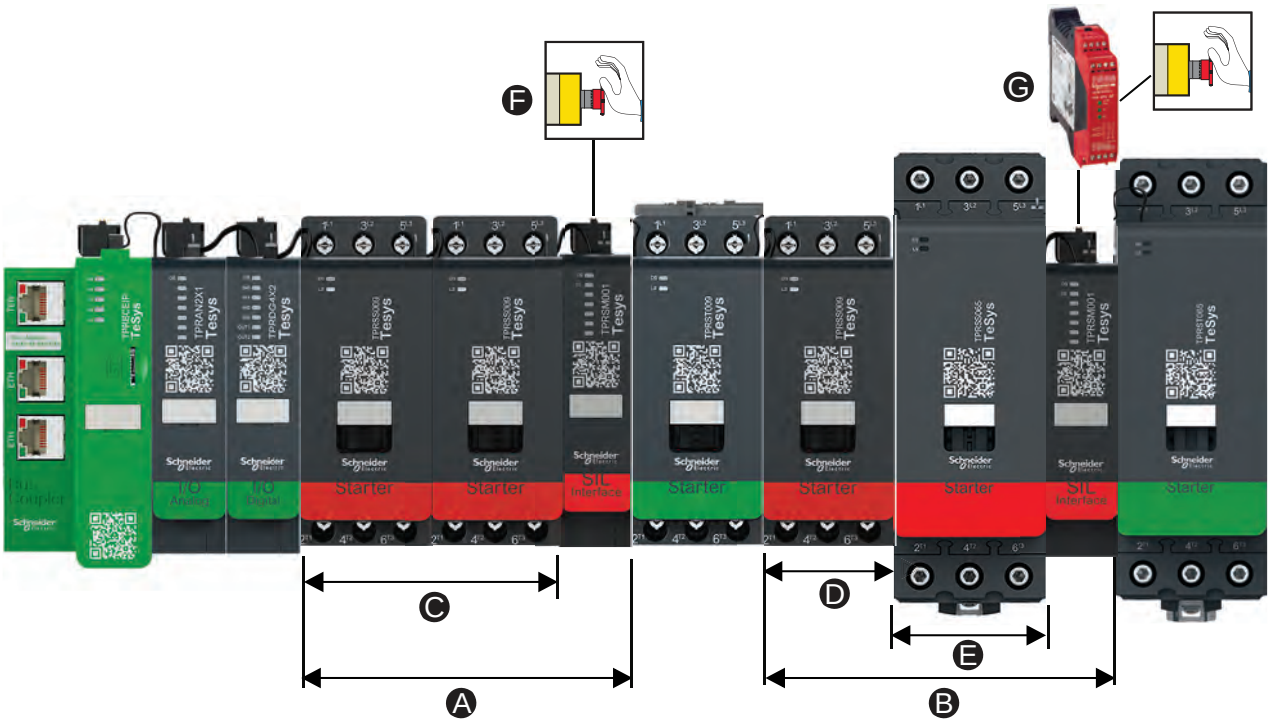
The system integrator/machine manufacturer must perform an acceptance test of the safety function to verify and document the correct functionality of the safety function. The system integrator/machine manufacturer thereby certifies to have tested the effectiveness of the safety functions used. The acceptance test must be performed based on the hazard analysis and risk assessment. All applicable standards and regulations must be followed.

Concepts and Components

Typical TeSys™ island Structure

The illustration below shows an example of a TeSys™ island that consists of two SIL groups. The composition of the island is defined by the TeSys island digital tools according to the functional needs expressed by the user.

Figure 2 - TeSys island with Two SIL Groups



A	SIL Group 1	E	Avatar A4
B	SIL Group 2	F	Wiring Category 1, Stop Category 0
C	Avatar A1	G	Wiring Category 2, Stop Category 1
D	Avatar A3		

SIL Group 1: includes one avatar that includes two SIL starters: for instance, a “Motor Two Directions – Safe Stop, W. Cat 1/2” avatar (Avatar A1). The actual motor is wired to these SIL starters and follows the avatar logic and the operational commands coming from the PLC through the fieldbus. The Safe Stop Command comes from the emergency stop push button wired to the SIL interface module (Wiring Category 1) and causes the SIL starters to de-energize the load and enter the safe state (contactor is opened, and the motor is de-energized).

SIL Group 2: includes two avatars, for instance a “Switch – Safe Stop, W. Cat 1/2" (Avatar A3) and a “Motor One Direction – Safe Stop, W. Cat 1/2" (Avatar A4), each of them consisting of a single SIL starter. Both avatars follow the avatar logic and operational commands coming from the PLC through the fieldbus. The Safe Stop Command comes from the external Preventa™ XPS module (or equivalent) wired to the SIL interface module, and causes the SIL starters to de-energize the load and enter the safe state (Wiring Category 2).

SIL Group

A SIL group is made up of one or more SIL avatars, all assigned to a single SIL interface module. All SIL avatars in the SIL group react to a single Safe Stop Command. The SIL interface module is always installed to the right of the last SIL starter included in the SIL group (far side of the bus coupler).

An island may include several SIL groups.

SIL Avatars

SIL avatars available for Safe Stop functions are:

- Switch - Safe Stop, W. Cat 1/2
- Motor One Direction - Safe Stop, W. Cat 1/2
- Motor Two Directions - Safe Stop, W. Cat 1/2
- Motor Two Speeds - Safe Stop, W. Cat 1/2
- Motor Two Speeds Two Directions - Safe Stop, W. Cat 1/2

SIL avatars consist of specific hardware devices, including SIL starters, standard starters, and the required SIL interface module that manages the SIL group that the SIL avatars are assigned to.

NOTE: SIL avatars are designed for applications with a low frequency of operational commands—below a yearly average of 15 start/stop cycles per hour.

SIL Starter

Standard Starter

SIL Interface Module

SIL Interface Module (SIM)

The TeSys™ island SIL interface module (SIM) is an accessory module required to enable the Functional Safety feature of the island.

The Safe Stop function is achieved by pure electromechanical means without any digital communication or bus coupler involvement.

The SIM:

- interfaces with an external Preventa™ XPS module (or equivalent)
- commands the stop function of its SIL group
- exchanges operational data with the bus coupler
- reports operational information through front face LEDs

SIM LED Status Indicators

Table 3 - Device Status LED

Indicator State	Summary	Description
Single Flash Green/Red	LED Diagnostic	Visual indication that LEDs are operational
Steady Off	Off	Module not energized
Steady Red	Device Major Event	Internal detected error of the device
Flashing Red	Not Ready	Discovery, addressing, firmware update, Device Minor Detected Error, etc.
Steady Green	Ready	Ready

Table 4 - SIM – SIL Status (SS) LED

Indicator State	Summary	Description
Single Flash Green/Red	LED Diagnostic	Visual indication that LEDs are operational
Steady Off	Off/Not Ready	Module not energized or Device Not Ready
Steady Green	Normal	No Safe Stop Command
Flashing Green	Safe Stop Command	Successful Safe Stop Command, not yet in Safe State
Flashing Red	Safe State with wiring issue detected	Successful Safe Stop Command but indicative of wiring issue, Safe State achieved
Steady Red	Safe Stop Command, Safe State	Successful Safe Stop Command and Safe State achieved

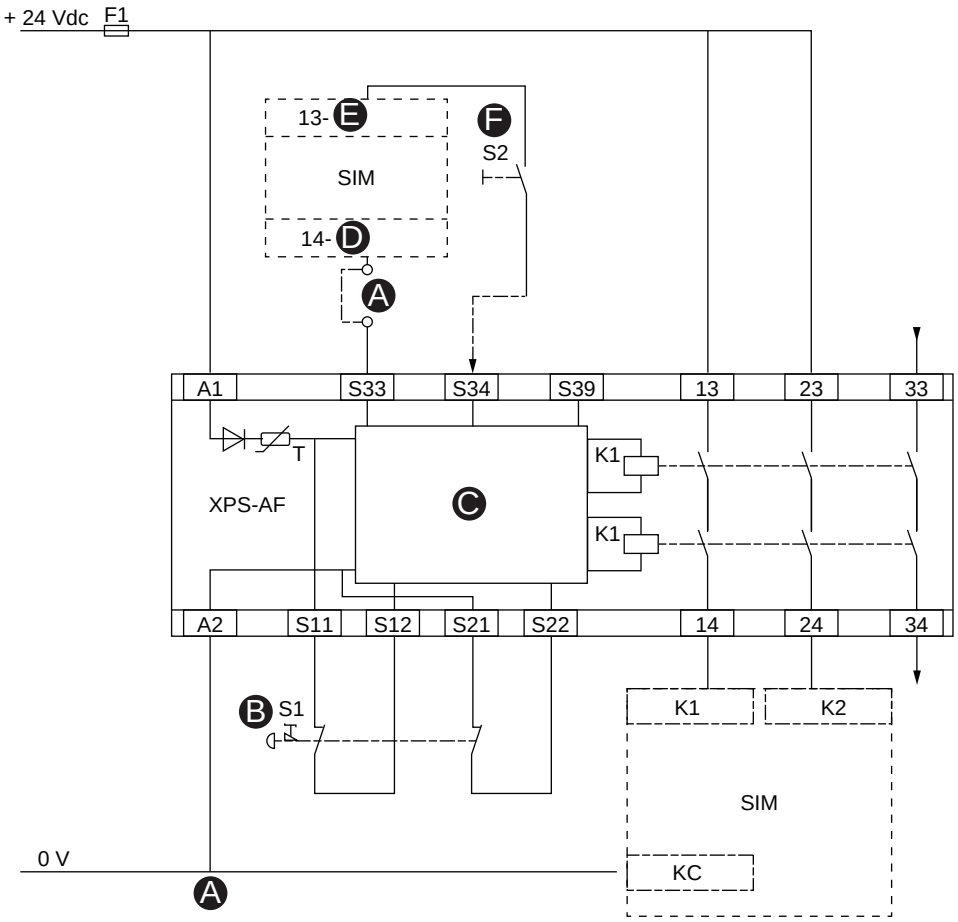
SIL Starters Contact Status

The status of the SIL starters belonging to a SIL group is reported via the SIM Mirror In/Out connections. This allows the implementation Wiring Category 2 architectures where the mirror contacts are connected to the Preventa XPS module (or equivalent). These configurations provide direct monitoring capabilities of electromechanical devices by a mechanically linked contact element, which gives diagnostic coverage up to 99%. Refer to EN ISO 13849-1, Table E.1 – Estimates for diagnostic coverage (DC).

Table 5 - SIL Starter Contact Status

SIL Group Status	Mirror In/Out Status
All SIL Starters are open	Mirror In/Out contact is closed
At least one SIL Starter is closed	Mirror In/Out contact is open
TeSys island unpowered, or fault detected by the safety function	Mirror In/Out contact is open

Figure 3 - SIM to Preventa Module XPS-AF Wiring



A	External start conditions (ESC)	D	SIM mirror out
B	Emergency stop push button (S1)	E	SIM mirror in
C	Preventa XPS-AF Module	F	Start button (S2)

Safety-Related Sensor Element

The SIM module is connected upstream:

- to the 24 Vdc source
- to the safety-related sensor element or a Preventa XPS module (or equivalent).

The SIM module is designed with two input channels to accommodate dual channel safety-related sensor elements. For a higher level of fault tolerance, the two-input channel architecture is recommended.

For the wiring diagrams below, refer to *Legend for SIM Channel Wiring Diagrams, page 21*.

Figure 4 - SIM — One Channel Wiring

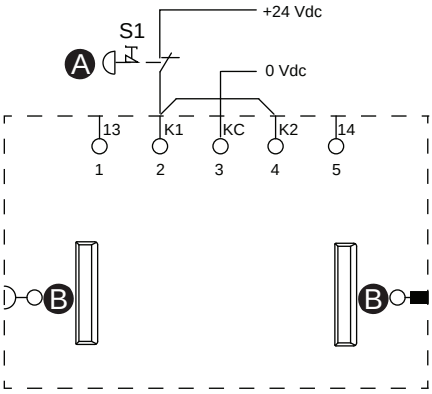


Figure 5 - SIM — Two Channel Wiring

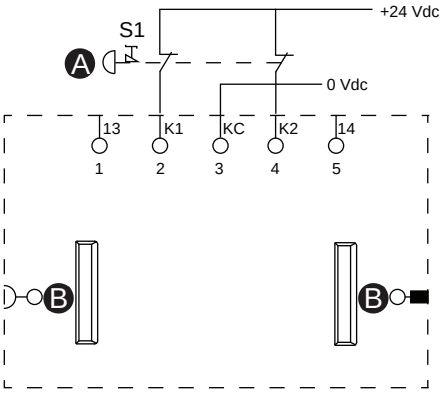


Table 6 - Legend for SIM Channel Wiring Diagrams

A	Emergency stop push button (S1)
B	Flat cable connector

SIL Starters

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

For complete instructions about functional safety, refer to the *TeSys™ island Functional Safety Guide*, 8536IB1904.

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

SIL[2] starters provide similar functions to standard starters but are associated with a SIL interface module.

The main functions of the SIL starters are as follows:

- Provide Stop Category 0 and Stop Category 1 functionality[3]
- Provide operational control for loads
- Measure electrical data related to the load

2. Safety Integrity Level according to standard IEC 61508
3. Stop categories as defined in EN/IEC 60204-1.

- Provide energy monitoring data when a voltage interface module is installed in the island

Multiple SIL starters might be needed for a single TeSys Avatar function. For example, the Avatar *Motor Two Directions - Safe Stop, W. Cat 1/2*[4] includes two SIL starters. In addition, Avatars using SIL starters always include a SIL interface module.

The SIL starters are connected:

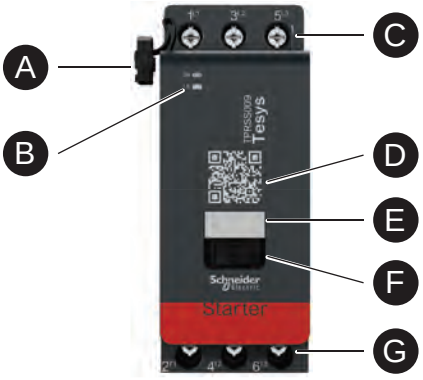
- Upstream to a circuit breaker
- Downstream to the load

The SIL starters communicate with the bus coupler, sending operational data and receiving commands.

Table 7 - SIL Starter Ratings

Power Ratings		Amperage	Reference
kW	hp		
4	5	0.18–9	TPRSS009
11	15	0.5–25	TPRSS025
18.5	20	0.76–38	TPRSS038
30	40	3.25–65	TPRSS065
37	40	4–80	TPRSS080

Figure 6 - SIL Starter Features



A	Flat cable (for connection with the module to the left)	E	Name tag
B	LED status indicators	F	Mobile bridge
C	Upstream power connections	G	Downstream power connections
D	QR code		

4. Safe Stop according to EN 61800-5-2.

External Safety-Related Element

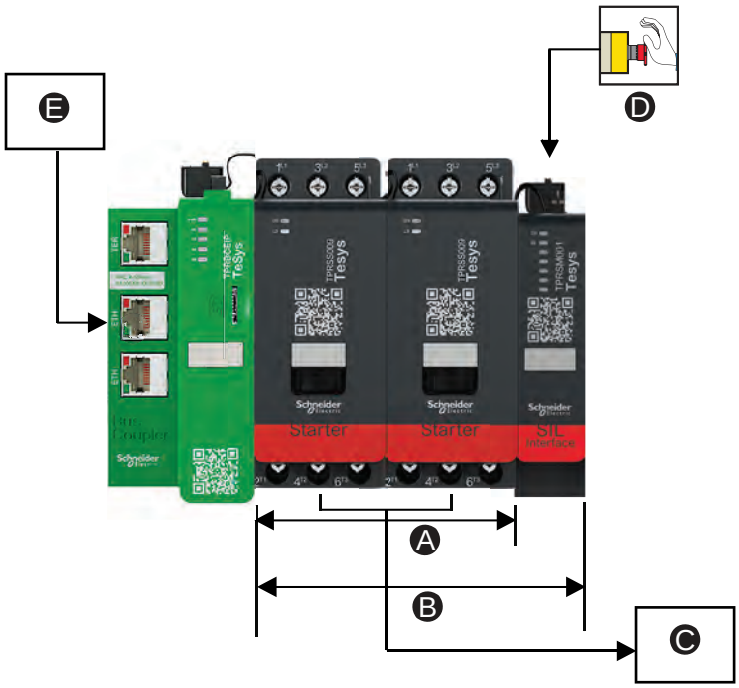
TeSys™ island must be integrated with other safety-related elements in a broader safety-related system to help ensure the functional safety of a machine or a system/process.

The following configurations illustrate typical devices.

Safe Stop, Stop Category 0, Wiring Category 1 Configuration

The Safe Stop of the motor is directly controlled by the opening of the contact of the emergency stop push button.

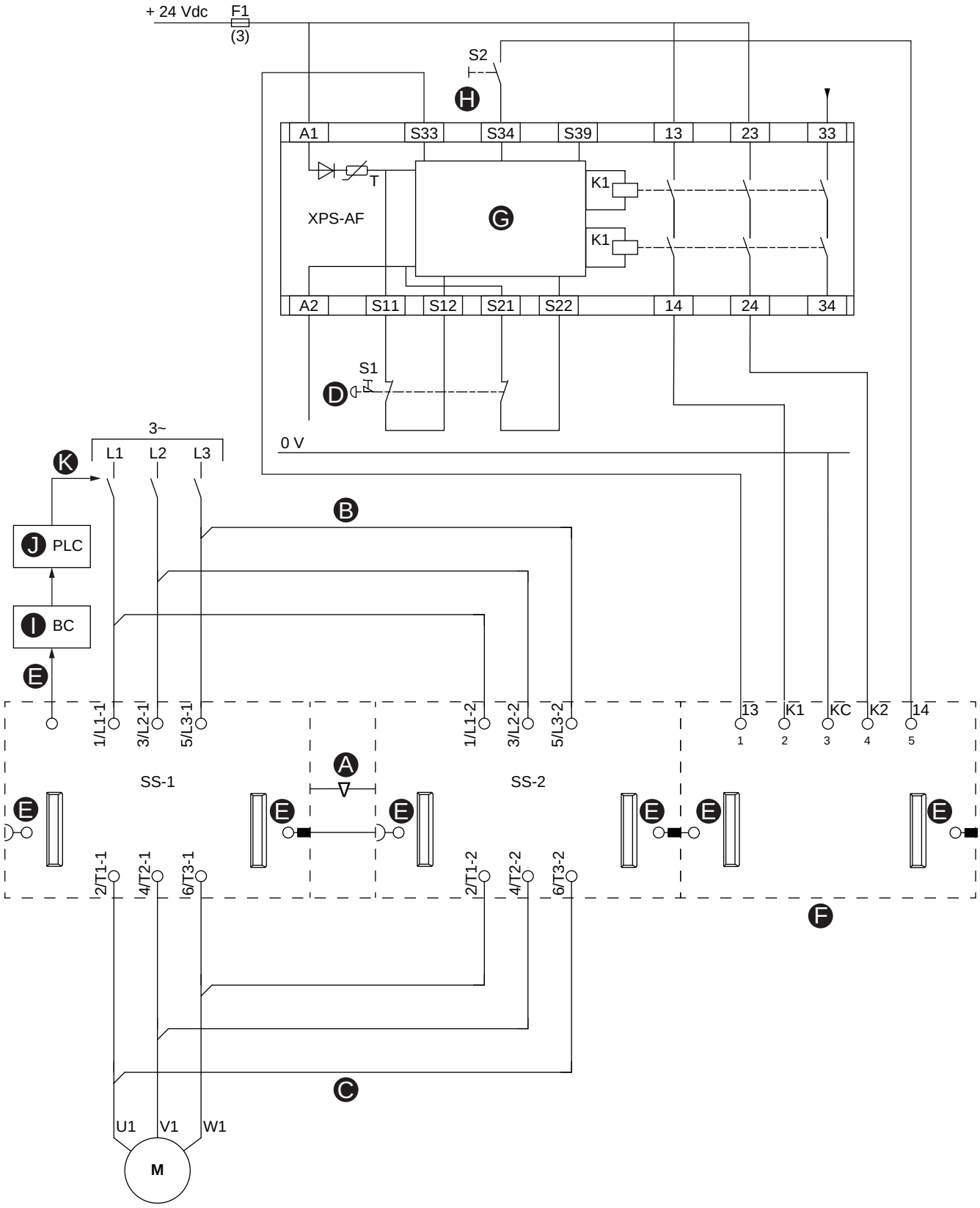
Figure 7 - Safe Stop



A	Avatar A1	D	Wiring Category 1, Stop Category 0
B	SIL Group 1	E	PLC
C	Motor		

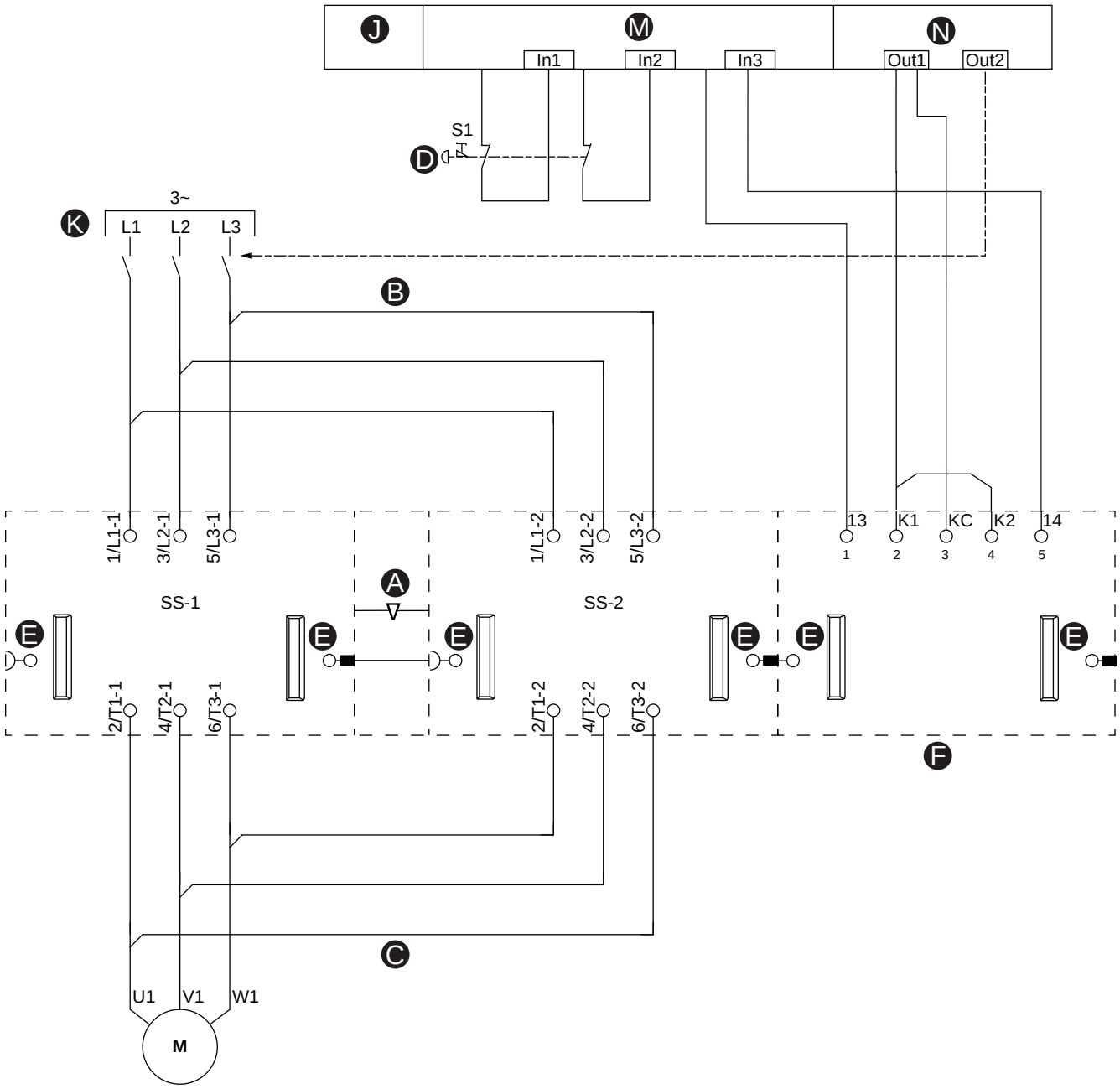
Safe Stop, Stop Category 0, Wiring Category 2 Configuration

Figure 8 - Example: Motor Two Directions — Safe Stop, W. Cat 1/2 — Stop Category 0, Wiring Category 2 Configuration (Indirect Monitoring)



A	Mechanical interlock	G	Preventa XPS-AF Module
B	Parallel link	H	Start button (S2)
C	Reversing link	I	Bus coupler
D	Emergency stop push button (S1)	J	PLC
E	Flat cable connector	K	Upstream circuit breaker
F	SIL interface module (SIM)		

Figure 9 - Example: Motor Two Directions — Safe Stop, W. Cat 1/2 — Stop Category 0, Wiring Category 2 Configuration (Direct Monitoring)



A	Mechanical interlock	G	Preventa XPS-AF Module
B	Parallel link	H	Start button (S2)
C	Reversing link	J	Safety Function PLC
D	Emergency stop push button (S1)	K	Upstream circuit breaker
E	Flat cable connector	M	Digital input
F	SIL interface module (SIM)	N	Digital output

Safe Stop, Stop Category 1, Wiring Category 2 Configuration

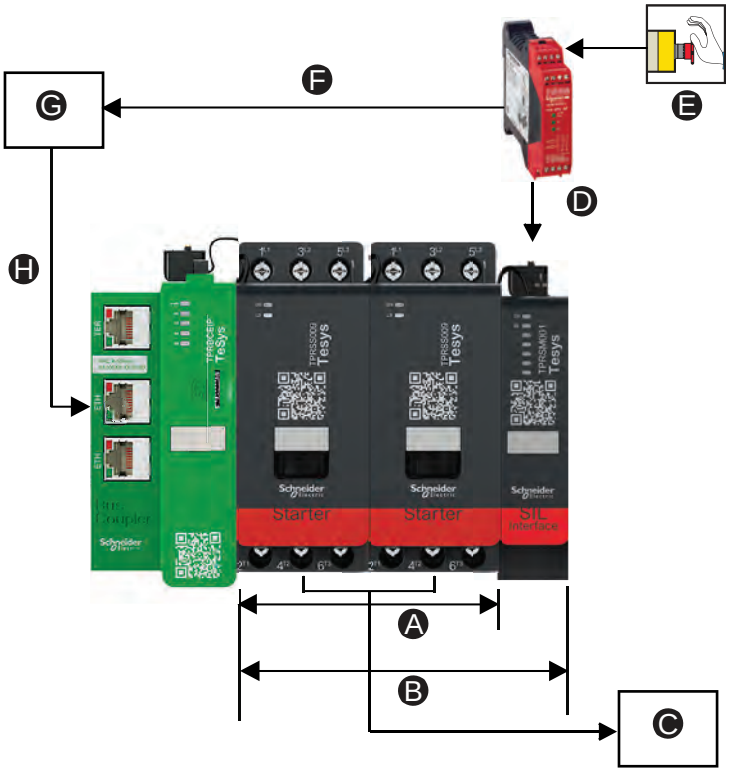
Stop Category 1 is defined as “a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved.”

When the emergency stop is triggered, the stop command is first sent to an external device (for example, a PLC or a drive). In this way, the process is stopped in a controlled manner rather than by immediate power removal. After a pre-defined time, the Safe Stop Command is then sent to the SIM to de-energize loads on the SIL avatars in the associated SIL group.

The recommended setup is to use a PLC to help ensure that the process is correctly stopped before the Safe Stop occurs.

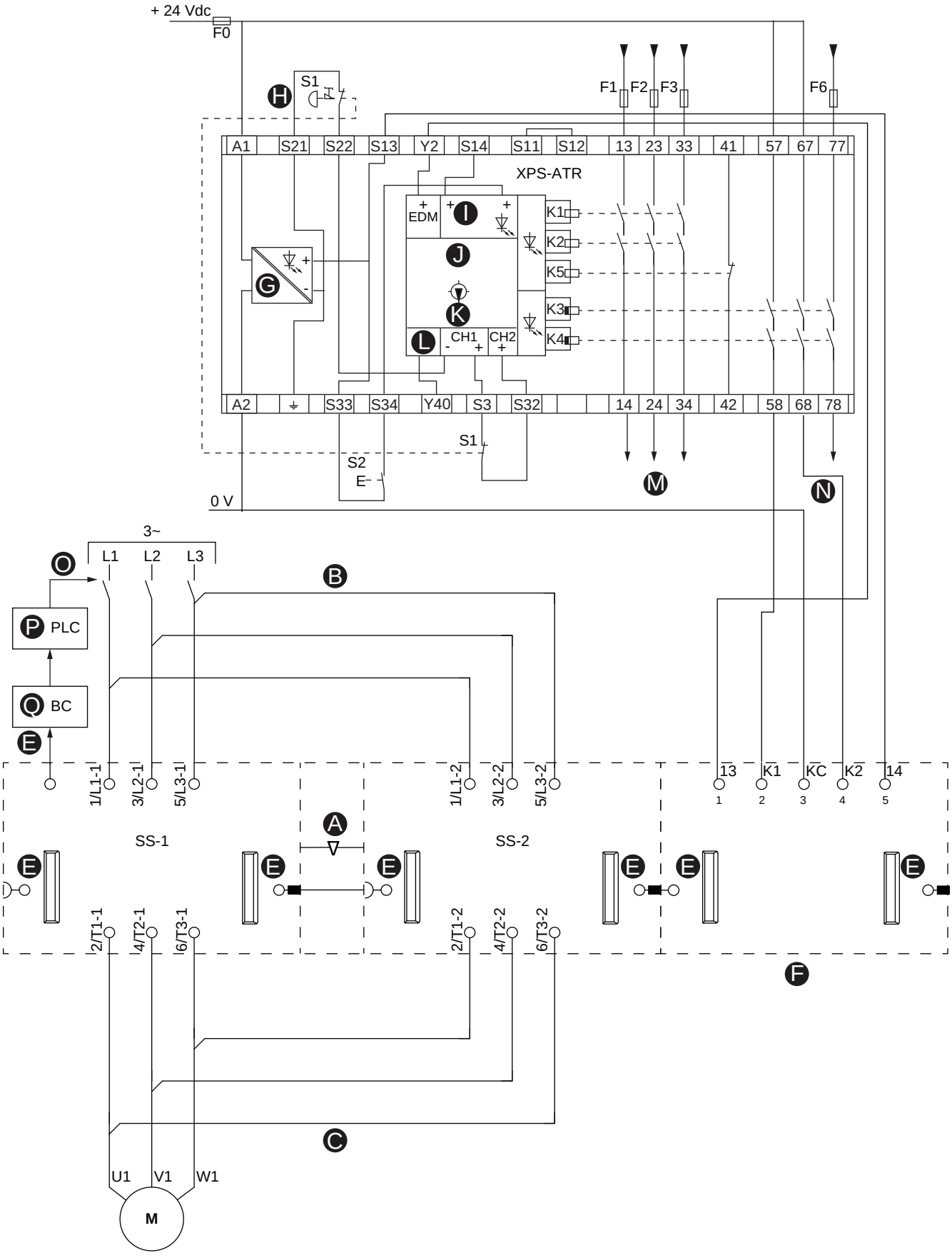
The stop command can be routed directly to a digital input of the PLC, or to a TeSys™ island Digital I/O Module avatar, using one of its digital inputs read by the PLC. Upon receiving a stop command input, the PLC initiates a controlled stop by issuing an operational stop command to the targeted TeSys island avatar.

Figure 10 - Stop Command



A	Avatar A1	E	Wiring Category 2, Stop Category 1
B	SIL Group 1	F	Controlled Stop Category 1 command
C	Motor	G	PLC
D	Uncontrolled stop	H	Operational stop command

Figure 11 - Example: Motor Two Directions — Safe Stop, W. Cat 1/2 — Stop Category 1, Wiring Category 2 Configuration



A	Mechanical interlock	J	Control logic
B	Parallel link	K	Time (s)
C	Reversing link	L	Time clear
E	Flat cable connector	M	Controlled stop
F	SIL interface module (SIM)	N	Stop Category 1
G	Supply	O	Upstream circuit breaker
H	Emergency stop push button	P	PLC
I	Reset	Q	Bus coupler

Protected Cable Insulation

⚠ DANGER

UNINTENDED EQUIPMENT OPERATION

Make sure to install the cables of the safety-related system according to ISO 13849-2.

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

If short circuits and cross circuits can occur with the cables of the safety-related system and if they are not detected by upstream devices, protected cable installation according to ISO 13849-2 is required.

In the case of an unprotected cable installation, the two signals (both channels) of a safety function in short circuit state may be connected to external voltage if a cable is damaged. In this case, the safety function is no longer operative.

Low/High Frequency Switching Architecture

The following can be used to determine whether you are operating in a low or high frequency architecture.

The electromechanical part of the SIL starter is characterized with a B10d.

To calculate the $MTTF_d$ (according ISO 13849-1) or λd (according to IEC 62061), the following formula applies:

$$MTTF_d = B10d/(0,1*Nop)$$

with $\lambda d = 1/MTTF_d$

Nop: Mean number of annual operations

According to ISO 13849, the operation time of an electromechanical component is limited to T10d (the mean time until 10% of the components fail dangerously[5]).

5. Fail dangerously according to ISO 13849

Therefore, the operation time of a SIL starter is limited to:

$$T10d = B10d / Nop$$

The B10d of the SIL starter is B10d = 1,369,863 and assuming a T10d of 10 years, the number of cycles for a TeSys island SIL starter is limited to Nop = B10d/T10 = 131,400/year (or a yearly average of 15 cycles/h).

If the application requires a Nop lower than that value, it falls under the low switching frequency category (where SIL Avatars can be used as is). Otherwise, it falls under the high switching frequency category (where the safety function must be implemented with a devoted SIL avatar as described below).

Low Switching Frequency (< 15 cycles per hour)

In low switching frequency, the Safe Stop and the operational on/off control functions can be achieved together with a SIL avatar.

Figure 12 - Example Avatar with SIL Starter

SIL avatars can be used for low frequency use.

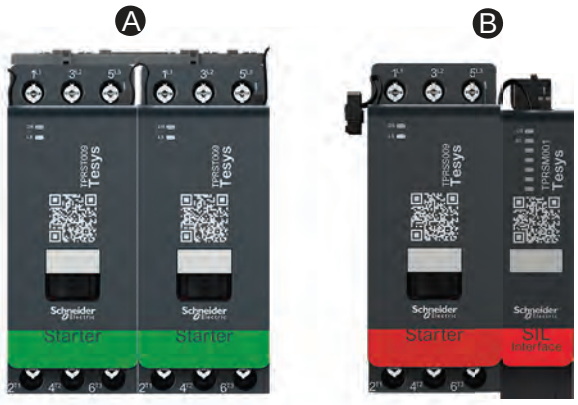
Table 8 - Low Switching Frequency — Operational and Safety Functions

SIL Avatar	Module 1	Module 2	Module 3	Module 4	Module 5
Switch - Safe Stop, W. Cat 1/2	SIL Starter	SIM			
Motor One Direction - Safe Stop, W. Cat 1/2	SIL Starter	SIM			
Motor Two Directions - Safe Stop, W. Cat 1/2	SIL Starter	SIL Starter	SIM		
Motor Two Speeds - Safe Stop, W. Cat 1/2	SIL Starter	SIL Starter	SIM		
Motor Two Speeds Two Directions - Safe Stop, W. Cat 1/2	Standard Starter	Standard Starter	SIL Starter	SIL Starter	SIM

High Switching Frequency (≥ 15 cycles per hour)

For high frequency use, the safety function must be isolated from the operational function by using a SIL avatar for the safety function and a standard avatar for the operational function. The standard starters are then wired in series downstream the SIL starter. *High Switching Frequency – Operational and Safety Functions, page 31* shows examples of standard avatars used downstream the SIL starter.

Figure 13 - Standard Avatar for Operational Function + SIL Avatar Used for Safety Function



A	Standard Avatar
B	SIL Avatar

Table 9 - High Switching Frequency — Operational and Safety Functions

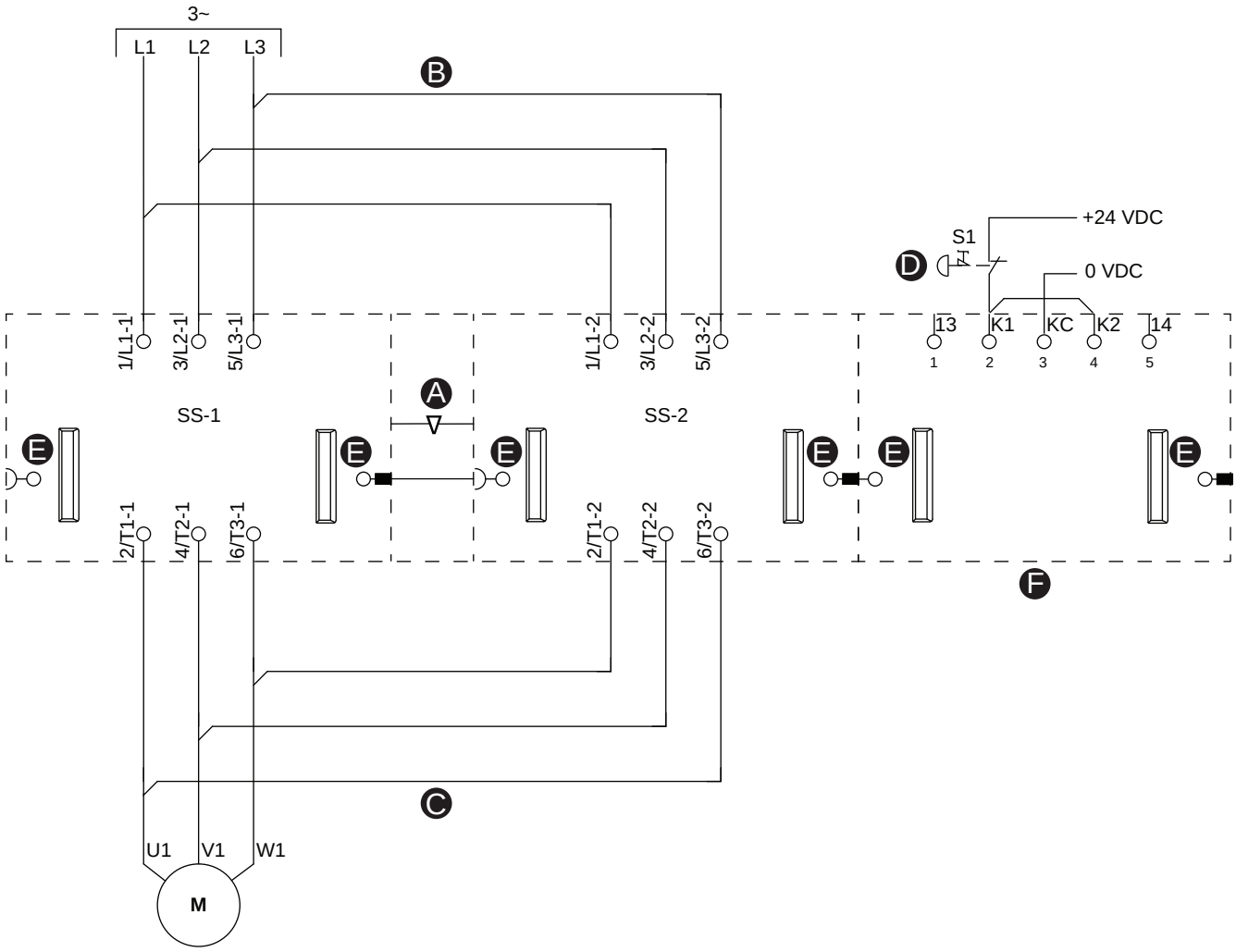
Standard Avatar	SIL Avatar	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6
Switch	Switch - Safe Stop, W. Cat 1/2	Standard Starter	SIL Starter	SIM			
Motor One Direction	Switch - Safe Stop, W. Cat 1/2	Standard Starter	SIL Starter	SIM			
Motor Two Directions	Switch - Safe Stop, W. Cat 1/2	Standard Starter	Standard Starter	SIL Starter	SIM		
Motor Two Speeds	Switch - Safe Stop, W. Cat 1/2	Standard Starter	Standard Starter	SIL Starter	SIM		
Motor Two Speeds Two Directions	Switch - Safe Stop, W. Cat 1/2	Standard Starter	Standard Starter	Standard Starter	Standard Starter	SIL Starter	SIM

Sample Architectures

The following architectures are available for TeSys™ island functional safety:

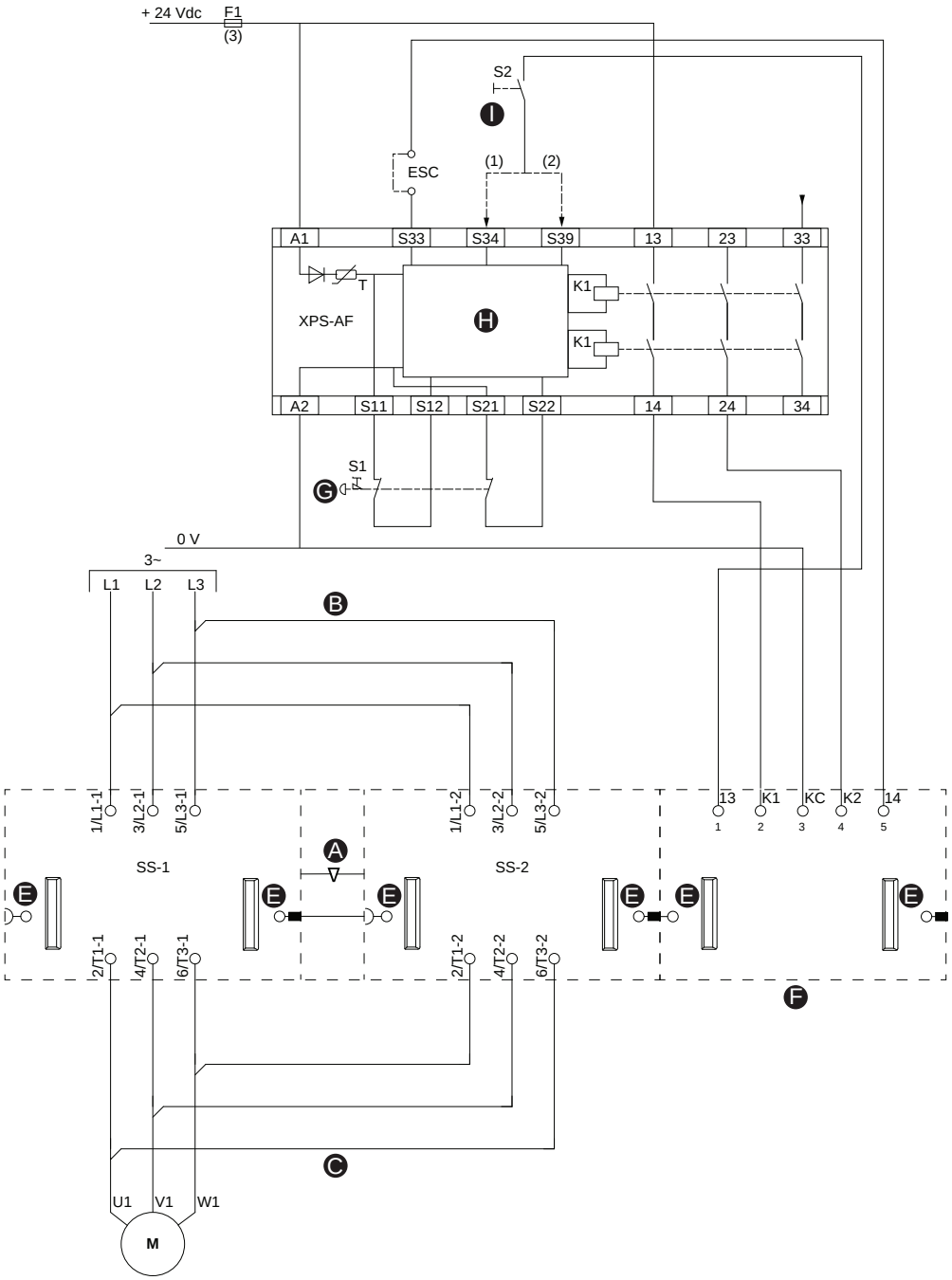
- Safe Stop, Stop Category 0, Wiring Category 1
- Safe Stop, Stop Category 0, Wiring Category 2
- Safe Stop, Stop Category 1, Wiring Category 2

Safe Stop, Stop Category 0, Wiring Category 1



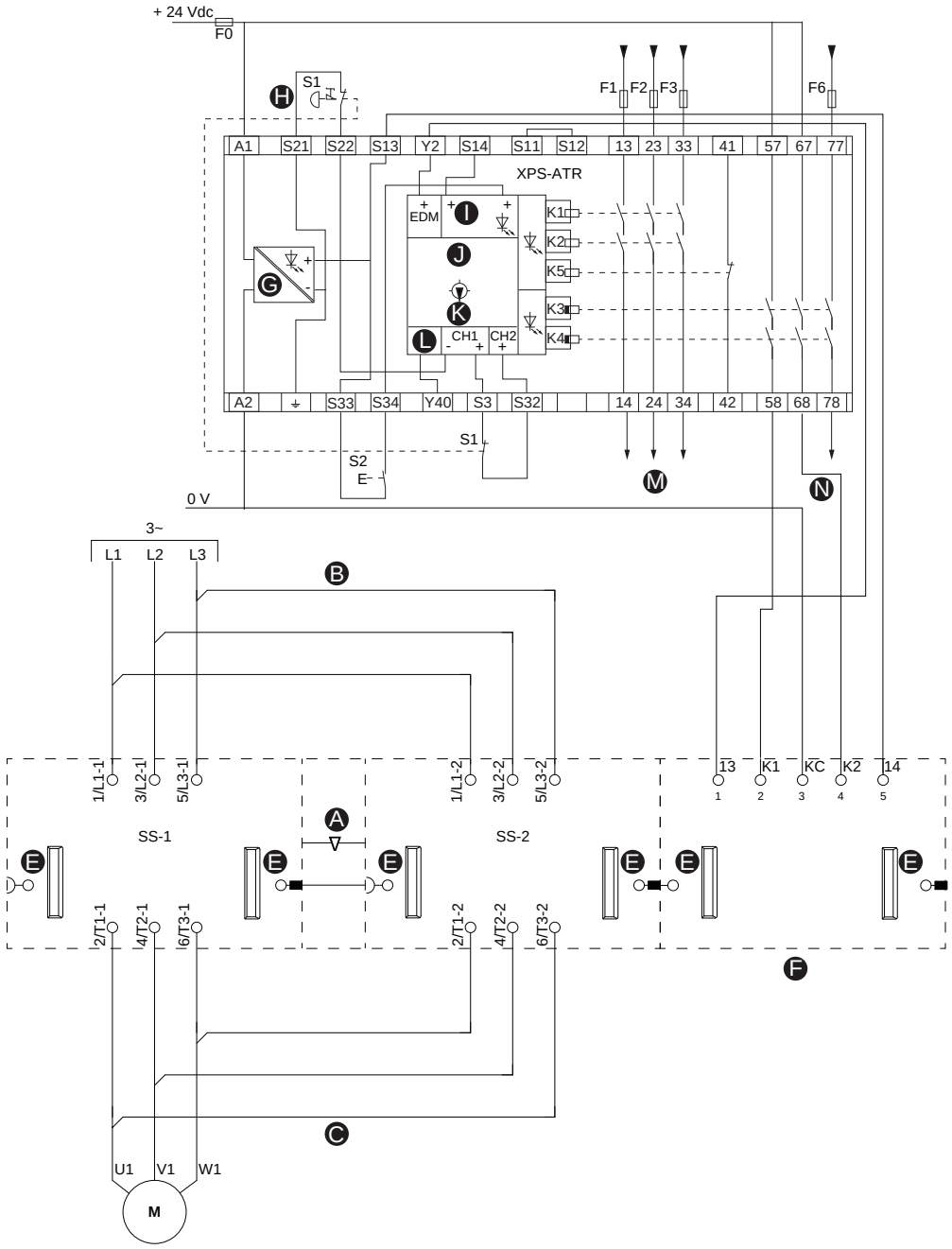
A	Mechanical interlock	D	Emergency stop push button (S1)
B	Parallel link	E	Flat cable connector
C	Reversing link	F	SIL interface module (SIM)

Safe Stop, Stop Category 0, Wiring Category 2



A	Mechanical interlock	F	SIL interface module (SIM)
B	Parallel link	G	Emergency stop push button (S1)
C	Reversing link	H	Preventa XPS-AF Module
E	Flat cable connector	I	Start button (S2)

Safe Stop, Stop Category 1, Wiring Category 2



A	Mechanical interlock	G	Supply	L	Time clear
B	Parallel link	H	Emergency stop push button (S1)	M	Controlled stop
C	Reversing link	I	Reset	N	Stop Category 1
E	Flat cable connector	J	Control logic		
F	SIL interface module (SIM)	K	Time (s)		

Technical Data

SIL Interface Module (SIM)

The calculated values of the SIL interface module (SIM) are provided in the following table:

Architecture	SIM					
	PFH	PFD	SFF	HFT	$MTTF_d$ (years)	DC
Category 1	2.10^{-10}	2.10^{-5}	>90%	1	17,459	Not relevant
Category 2			>99%			99%

NOTE: PFD and PFH values are calculated with the following:

- TI=20 years
- MTTR=MRT= 24 hours

Architectural requirements defined in IEC 61508-2 Table 3 and EN 62061 Table 5 are met for levels up to SIL 3.

SIL Starter

The following data help define the level of performance for SIL starters.

B10: **1,000,000**

% of dangerous failures[6]: **73%**

$B10_d$: **1,369,863**

Assuming a nop = 131,400 cycles/year (average of 15 cycles/hour)

The calculated values of the SIL starter in single-channel architecture are provided in the following table:

Table 10 - SIL Starter in Single Channel

Wiring Category	SFF	HFT	$MTTF_d$ (years)	DC
Category 1	27%	0	100 years	Not relevant
Category 2 – Direct monitoring	90%	0	100 years	≥ 90%

The relation between PFHd and PFD of the SIL starters, depending on the architecture and the test interval, is given in the following table:

Table 11 - SIL Starters — PFHd and PFD

Wiring Category	PFH (IEC 61508)	PFD (IEC 61508) Ti 10 years	PFD (IEC 61508) Ti=5 years
Category 1	1.10E-06	4.80E-02	4.82E-03
Category 2 – Direct monitoring	1.10E-06	4.82E-03	5.06E-04

Architectural requirements defined in IEC 61508-2 Table 3 and EN 62061 Table 5 are met for levels up to SIL 2.

A Category 2 architecture is needed to meet SIL 2 architectural constraints (accomplished using direct monitoring Mirror In/Mirror Out).

6. Dangerous failure as defined in IEC 61508-4

NOTE: The fault detection and specified fault reaction must be performed before the hazardous situation addressed by the safety-related control function can occur.

Reliability Data

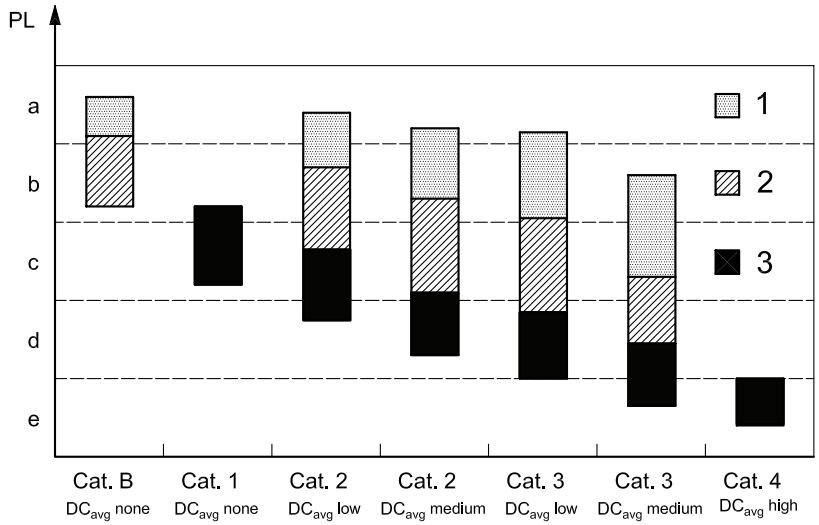
Safety Function Standard Reference

The Safe Stop function has priority over a stop triggered for operational reasons (EN ISO 13849-1, 5.2.1).

The performance level depends on the wiring category, the $MTTF_d$, and the DC_{avg}.

The following diagram shows the positioning of TeSys™ island according to the category requirement.

Figure 14 - TeSys island Positioning by Category Requirement



Key

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Table 12 - Simplified Procedure for Evaluating PL Achieved by SRP/CS

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**none**	**none**	**low**	**medium**	**low**	**medium**	**high**
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	v	d	d	d	e

According to TeSys island architecture and wiring category, the key indicators (DC_{avg}, $MTTF_d$, PL) for TeSys island comply with the values shown in the table below.

TeSys island system architecture	**Category**	**Single fault tolerance**[7]	**DC_{avg}**	**$MTTF_d$ of each channel**	**Targeted PL**
Single channel	1	No	None	High (≥ 30 years)	c

7. Single fault tolerance means that a single fault (including common-mode events) must not lead to the loss of the safety function.

TeSys island system architecture	Category	Single fault tolerance[8]	DC_{avg}	$MTTF_d$ of each channel	Targeted PL
	2	No	Low (≥ 60%) to medium (≥ 90%)	Low (≥ 3 years) to high (≥ 30 years)	c, d

SIL Avatar Wiring

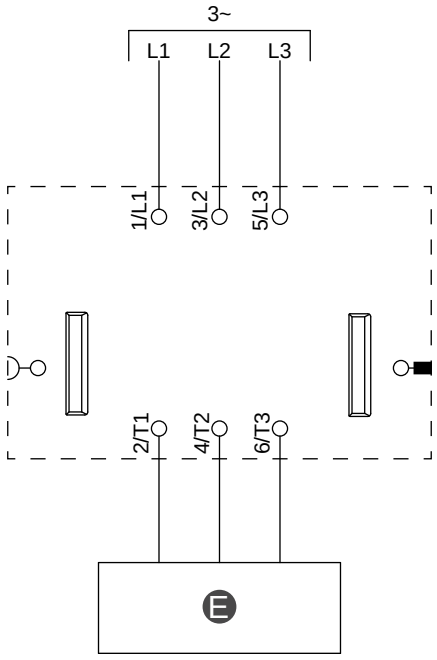
The following wiring diagrams are for the SIL avatars.

Table 13 - Legend for Wiring Diagrams

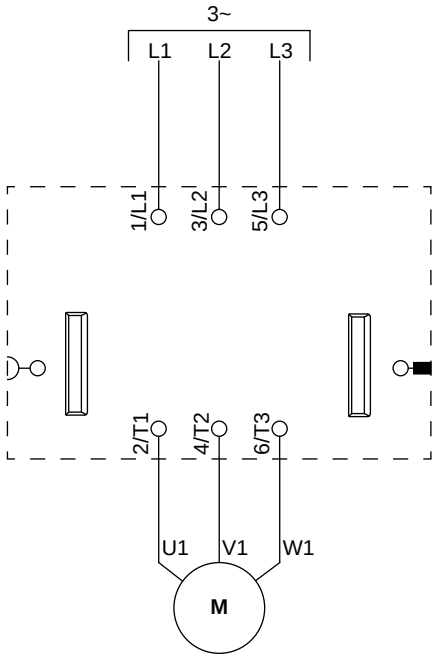
A	Mechanical interlock
B	Parallel link
C	Reversing link
E	Electrical circuit

Table 14 - SIL Avatar Wiring Diagrams

NOTE: See *Table 13, page 37*.



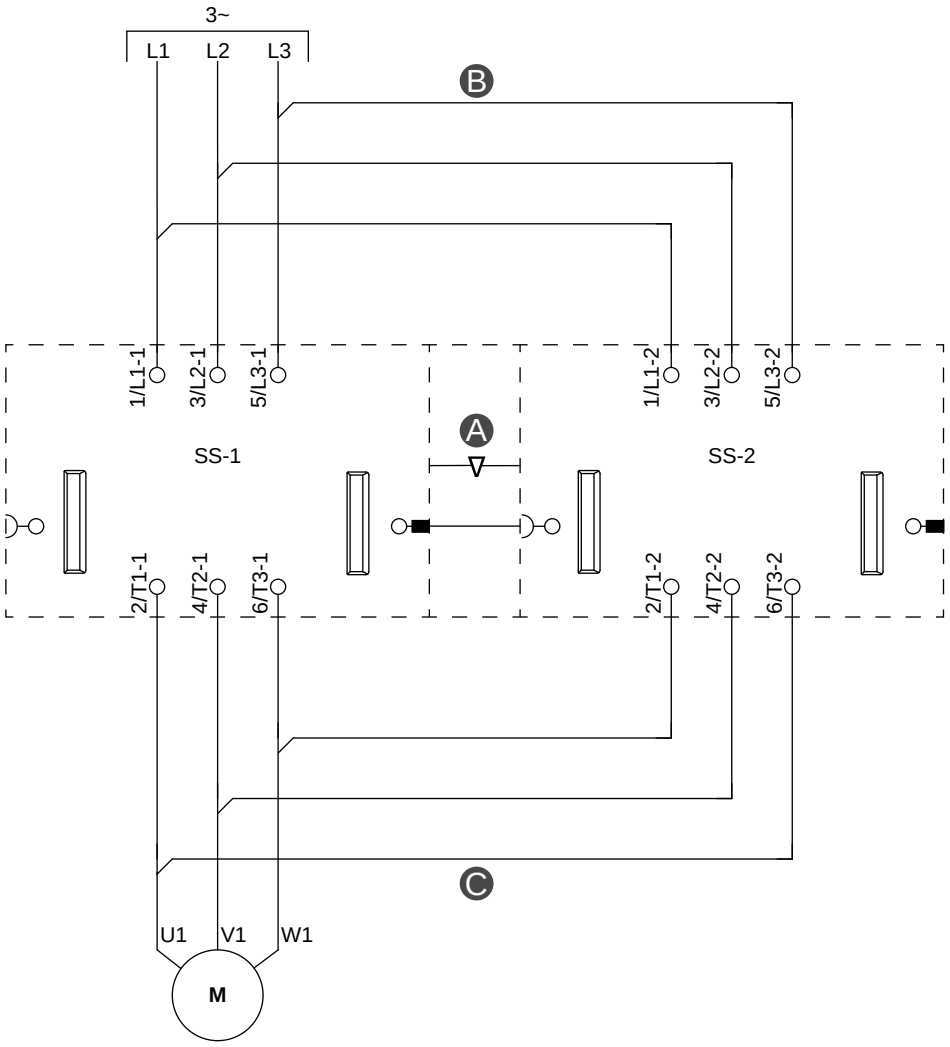
Switch - Safe Stop, W. Cat 1/2



Motor One Direction - Safe Stop, W. Cat 1/2

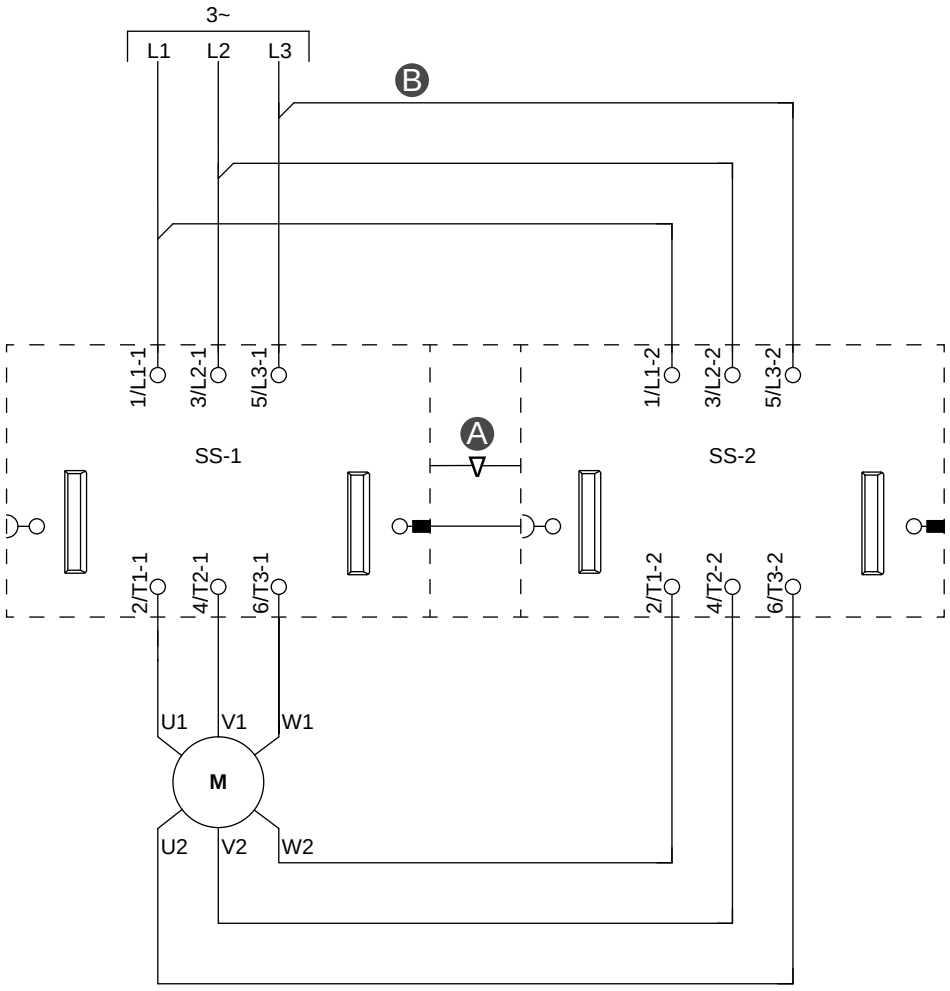
8. Single fault tolerance means that a single fault (including common-mode events) must not lead to the loss of the safety function.

Table 14 - SIL Avatar Wiring Diagrams (Continued)

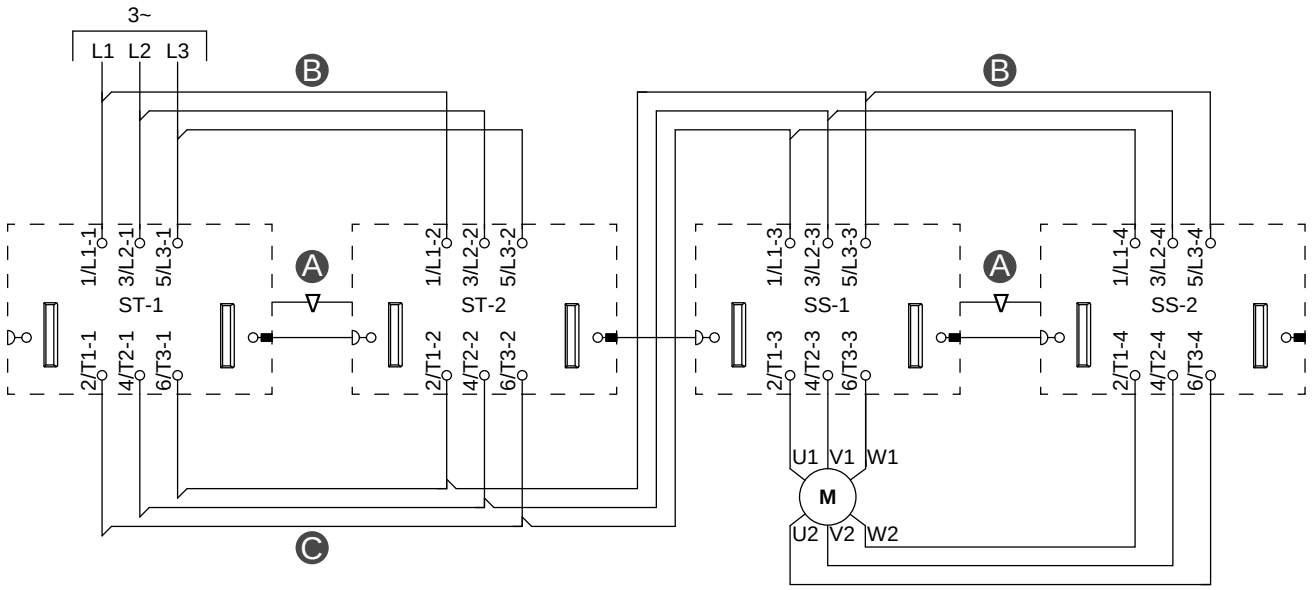


Motor Two Directions - Safe Stop, W. Cat 1/2

Table 14 - SIL Avatar Wiring Diagrams (Continued)



Motor Two Speeds - Safe Stop, W. Cat 1/2



Motor Two Speeds Two Directions - Safe Stop, W. Cat 1/2

Commissioning the Safety Function

Use this procedure to commission the safety function. The procedure comprises two steps:

- Installation tests
- Safety function proof tests[8]

Installation Tests

Perform the steps in the following table to test the installation of the safety function.

Table 15 - Installation Test

1	Using the **DIAGNOSTICS** panel in the TeSys™ island DTM, verify that the physical topology matches the logical topology.
2	Using the **MY AVATAR** panel in the TeSys island DTM, verify in **AVATAR PARAMETERS** that the SIL Avatars are associated with the proper SIL group.

Safety Function Proof Test

The safety function proof test is performed for each SIL group on the island. A SIL group may comprise multiple SIL Avatars managed by one SIL Interface Module (SIM).

The safety function proof test is successful if upon activation of the emergency stop device associated with a SIL group, all SIL starters belonging to that SIL group enter the safe state (the load is de-energized).

NOTE: For Stop Category 0 (uncontrolled stop), the stop should be immediate. For Stop Category 1 (controlled stop) the stop is effective after a delay.

Perform the steps in the following table for each SIL group on the island to perform the safety function proof test.

Table 16 - Safety Function Proof Test

1	Activate the emergency stop device associated with the SIL group, and check that all SIL starters belonging to the group enter the safe state (the load is de-energized). **NOTE:** The Device Status (DS) LED will flash red on the SIL starters, indicating a Device Minor Event state. If the test fails: • The emergency stop device may be connected to the wrong SIM. Check these connections. • The emergency stop device may not be correctly wired to the SIM. Check these connections. • Some SIL Avatars may not be attached to the expected SIL Group. Check the configuration.
2	In the TeSys™ island DTM or OMT **AVATARS** panel, in the **DIAGNOSTICS** section, check the **STATUS** and **EVENT LOGS** to verify that **SIL Group Status** is equal to "**Safe Stop Command**." In the Event Log it will read “ss0 cmd, Safe State achieved.” If the test fails: • Some SIL Avatars may not be attached to the expected SIL Group. Check the configuration.
3	In the **DEVICES** section of the **DIAGNOSTICS** panel, verify that the **SIL Interface Module (SIM) Status** is equal to "**Safe Stop Command**.” In the Event Log it will read “ss0 cmd, Safe State achieved.”

8. Proof test as defined in IEC 62061

Table 16 - Safety Function Proof Test (Continued)

	If the test fails: • The emergency stop device may be connected to the wrong SIM. Check these connections. • The emergency stop device may not be correctly wired to the SIM. Check these connections.
4	Apply a start command to a SIL Avatar belonging to the SIL group and verify that the start is unsuccessful: the starters should remain open and the start command should be disregarded until the emergency stop device is reset. If the test fails: • Some SIL Avatars may not be attached to the expected SIL Group. Check the configuration. If any of these tests continue to fail despite corrective actions, do not continue to operate the island. Replace the devices that failed the tests.
5	After the safety function proof test is complete, reset the emergency stop device and verify that all SIL starters and SIL interface modules are in Ready state (the DS LED is steady green).

Safety Function Maintenance Requirements

This section describes the routine maintenance required for maintaining functional safety on your TeSys™ island.

Maintenance Schedule

Maintenance intervals depend on the frequency mode.

- For Low Frequency mode (the yearly average number of contactor cycles is less than 15 cycles/hour), perform maintenance every 12 months.
- For High Frequency mode (the yearly average number of contactor cycles is greater than 15 cycles/hour or 136,986 cycles/year), perform maintenance at intervals that are 1/10th of the device estimated lifetime.

The device estimated lifetime (years) = B10d (=1,369,863) / yearly average number of contactor cycles

Maintenance Checks

Device Usage Checks

Perform the checks described in the following table to verify that the SIL starter contactor cycles are within the acceptable lifetime values.

1	Using the Devices **DIAGNOTSICS** feature of the TeSys™ island DTM or OMT, access the device asset information for each SIL starter.
2	If the **Number of Contactor Cycle** is greater than B10d (=1,369,863), then replace the SIL starter.
3	If not, use the **Number of Contactor Cycle** value to schedule the next maintenance. See *Maintenance Schedule, page 42*.

Safety Function Proof Test

Perform the Safety Function Proof Test on each SIL Group. See *Safety Function Proof Test, page 40*.

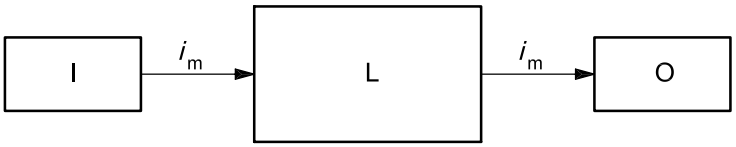
Appendix: Single-Channel Architecture

This single-channel architecture encompasses Wiring Categories 1 and 2.

Architectural Requirements for Wiring Category 1

Designated architecture for **Category 1** is defined in EN ISO 13849-1, 6.2.4.

Figure 15 - Designated architecture for Category 1 (EN ISO 13849-1)



I: input device

L: logic

O: output device

i m: interconnecting means

SRP/CS, the safety-related part of the control system, of Wiring Category 1 must be designed and constructed using **well-tried components**.

A “well-tried component” for a safety-related application is a component which has been either:

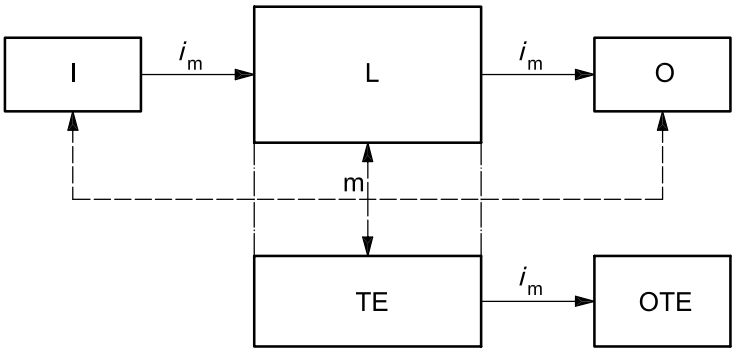
- widely used in the past with successful results in similar applications, or
- made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

There is **no diagnostic coverage** (DC_{avg} = none) within Category 1 systems.

Architectural Requirements for Wiring Category 2

Designated architecture for **Category 2** is defined in EN ISO 13849-1, 6.2.5.

Figure 16 - Designated Architecture for Category 2 (EN ISO 13849-1)



I: input device

L: logic

O: output device

i m: interconnecting means

m: monitoring

TE: test equipment

OTE: output of TE

SRP/CS, the safety-related part of the control system, of Wiring Category 2 must be designed so that their function(s) are checked at suitable intervals by the machine control system.

In single-channel architecture, a SIM is associated with a SIL starter.

Specifically, for Wiring Category 2, the mirror contact is connected to the Preventa™ XPS module (or equivalent). If the state of the mirror contact feedback line does not equal the Preventa XPS module (or equivalent) output state, the Preventa XPS module (or equivalent) blocks a second start.

NOTE: The mirror contact feedback conveys diagnosis information only.

Glossary

E

EN ISO 13849 Standard

This European Standard specifies the validation process, including hazard analysis, risk assessment, and testing, for the safety functions and categories for the safety-related parts of control systems. Descriptions of the safety functions and the requirements for the categories are given in ISO 13849-1, which covers the general principles for design. Some requirements for validation are general and some are specific to the technology used. EN ISO 13849-2 also specifies the conditions under which the validation by testing of the safety-related parts of control systems should be carried out.

EN 60204-1 Standard

Stop Category 0 is defined as a function “stopping by immediate removal of power to the machine actuators (i.e. an uncontrolled stop).”

Stop Category 1 is defined as “a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved.”

F

Fault Avoidance Measures

Systematic errors in the specifications, in the hardware and the software, usage faults and maintenance faults in the safety-related system must be avoided to the maximum degree possible. To meet these requirements, IEC 61508 specifies a number of measures for fault avoidance that must be implemented depending on the required SIL. These measures for fault avoidance must cover the entire life cycle of the safety-related system, i.e. from design to decommissioning of the system.

Functional Safety

Automation and functional safety engineering are two areas that were completely separate in the past but have recently become more integrated.

The engineering and installation of complex automation solutions are simplified by integrated safety functions.

Usually, the functional safety engineering requirements depend on the application.

The level of requirements results from the risk and the hazard potential arising from the specific application.

H

Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF)

Depending on the SIL for the safety-related system, the IEC 61508 standard requires a specific hardware fault tolerance (HFT) in connection with a specific proportion of safe failures, shown as Safe Failure Fraction (SFF).

The HFT is the ability of a system to execute the required safety function in spite of the presence of one or more hardware faults.

The SFF of a system is defined as the ratio of the rate of safe failures to the total failure rate of the system.

According to IEC 61508, the maximum achievable SIL of a system is partly determined by the HFT and the SFF of the system.

These types are specified on the basis of criteria which the standard defines for the safety-related elements.

SFF	HFT Type A Subsystem			HFT Type B Subsystem		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
60% – < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% – < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

I

IEC 61508 Standard

The standard IEC 61508 covers the functional safety of electrical/electronic/programmable electronic safety-related systems.

Instead of a single component, an entire function chain (for example, from a sensor through the logical processing units to the actuator) is considered as a unit.

This function chain must meet the requirements of the specific safety integrity level as a whole.

L

Low/High Demand Mode

IEC 61508 defines the safety function demand mode of operation:

- high demand or continuous mode (PFH)
- low demand mode (PFDavg, PTI)

M

Mean Time to Dangerous Failure ($MTTF_d$)

The $MTTF_d$ for each channel must be calculated or estimated as part of the verification that the required performance level has been met. The standard summarizes $MTTF_d$ into three levels: low, medium, and high, with a maximum value for a channel of 100 years. The $MTTF_d$ of individual components may be much higher than 100 years.

P

Performance Level (PL)

The standard IEC 13849-1 defines five performance levels (PL) for safety functions.

Level a is the lowest level and e is the highest.

Five levels (a, b, c, d, and e) correspond to different values of average probability of dangerous failure per hour.

Performance Level	Probability of a Dangerous Failure per Hour
e	≥ 10^{-8} to < 10^{-7}
d	≥ 10^{-7} to < 10^{-6}
c	≥ 10^{-6} to < 3 x 10^{-6}
b	≥ 3 x 10^{-6} to < 10^{-5}
a	≥ 10^{-5} to < 10^{-4}

Probability of a Dangerous Hardware Failure Per Hour (PFH)

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected errors, depending on the required SIL.

All components of a safety function must be subjected to a probability assessment to evaluate the effectiveness of the measures implemented for controlling detected faults.

This assessment determined the PFH (Probability of a dangerous Failure per Hour) for a safety-related system. This is the probability per hour that a safety-related system fails in a hazardous manner and the safety function cannot be correctly executed.

Depending on the SIL, the PFH must not exceed certain values for the entire safety-related system.

The individual PFH values of a function chain are added. The result must not exceed the maximum value specified in the standard.

Safety Integrity Level	Probability of a Dangerous Failure per Hour (PFH) at High Demand or Continuous Demand
4	10^{-9} ≤ — < 10^{-8}
3	10^{-8} ≤ — < 10^{-7}
2	10^{-7} ≤ — < 10^{-6}
1	10^{-6} ≤ — < 10^{-5}

S

Safety Integrity Level (SIL)

The standard IEC 61508 defines four safety integrity levels (SIL) for safety functions.

SIL 1 is the lowest integrity level and SIL 4 is the highest.

A hazard analysis and risk assessment serves as a basis for determining the required safety integrity level.

This is used to decide whether the relevant function chain is to be considered as a safety function, and which hazard potential it must cover.

Schneider Electric
800 Federal Street
01810 Andover, MA
USA

https://www.schneider-electric.com/en/work/support/

www.schneider-electric.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

8536IB1904EN