M580 Safety

Safety Related Application Conditions Verification Plan

Original instructions

EIO0000004540.02
06/2024

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

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.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

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

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

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

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

Document Scope

This document is a generic verification plan of the Safety Related Application Conditions (SRAC) to demonstrate compliance with the **Specific Requirements** section of the Modicon M580 Safety EC Type Examination Certificate.

The Modicon M580 Functional Safety Controller System EC Type Examination certificate ref REG.-NO.: 01/205/5610/01/19 [3], page 9 expresses this specific requirement: The instruction of the associated Installation and Safety Manual shall be considered.

EC Type-Examination Certificate

Product Safety
Functional
Safety

TÜVRheinland
CERTIFIED

www.tuv.com
ID 0600000000

Reg.-No.: 01/205/5610/01/19

Product tested	Safety-related Programmable Electronic System	**Certificate holder**	SCHNEIDER ELECTRIC 8 eme rue - ZI Carros 06516 Carros France
Type designation	M580 Functional Safety Controller System, details see "Revision List"		
Codes and standards	EN ISO 13849-1:2015 EN ISO 13849-2:2012 IEC 62061:2015		IEC 61508 Parts 1-7:2010 IEC 61131-2:2017 IEC 61131-6:2012
Intended application	The M580 Functional Safety Controller System complies with the requirements of Cat.4/PL e acc. to EN ISO 13849-1 and SIL3 acc. to IEC 61508 and IEC 62061. Hence it is suitable for the use in applications up to PL e according to EN ISO 13849-1 and SIL 3 according to IEC 62061 / IEC 61508. The product was also reviewed in reference to (Further the products comply with) the applicable requirements of IEC 61511:2017, EN 50156-1:2015, NFPA 85:2015, NFPA 86:2015, NFPA 72:2016, EN 298:2015, EN 54-2:2006 and can therefore be used in Process Control, Burner Management System (BMS), Fire and Gas, Emergency Shutdown System, where the safe state is the de-energized state and in applications up to SIL 3, where the demand state is the de-energized or energized state.		
Specific requirements	The instructions of the associated Installation and Safety Manuals shall be considered.		

Valid until 2024-12-09

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1476.05/19 dated 2019-12-09.
This certificate is valid only for products which are identical with the product tested.

Köln, 2019-12-09

Notified Body for Machinery, NB 0035

Dipl.-Ing. Eberhard Frejno

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

This verification plan of the Safety Related Application Conditions is aimed at :

- identifying all “instruction of the associated Installation and Safety Manual” (also called requirements or SRAC)
- providing a generic frame to justify that these *instructions of the associated Installation and Safety Manual* are fulfilled

Validity Note

This document is valid for EcoStruxure™ Control Expert 16.0 + HF001 or later.

For product compliance and environmental information (RoHS, REACH, PEP, EOLI, etc.), go to www.se.com/ww/en/work/support/green-premium/.

Related Documents

Ref	Title of documentation	Reference number	Rev — Date
[1]	Modicon M580, Safety Manual	QGH46982	06–10/2020 or later
[2]	Modicon M580, Safety System Planning Guide	QGH60283	06–09/2020 or later
[3]	M580 Functional Safety Controller EC Type Examination	01/205/5610/01/19	-
[4]	EcoStruxure Control Expert, Safety Block Library	QGH60275	06–10/2020 or later
[5]	Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726	02–10/2018 or later

To find documents online, visit the Schneider Electric download center (www.se.com/ww/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.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the unit.
- 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.

⚠⚠DANGER

POTENTIAL FOR EXPLOSION

- Only use this equipment in non-hazardous locations, or in locations that comply with Class I, Division 2, Groups A, B, C and D.
- Do not substitute components which would impair compliance to Class I Division 2.
- Do not connect or disconnect equipment unless power has been removed or the location is known to be non-hazardous.

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

⚠WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it 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

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.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Acronyms

Acronym	Definition
CIP	Common Industrial Protocol
CPU	Central Processing Unit
DDDT	Device Derived Data Type
DTM	Device Type Manager

Acronym	Definition
EMC	Electromagnetic compatibility
E/E/PE	Electrical/Electronic/Programmable Electronic
DDT	Derived Data Type
IO (or I/O)	Input / Output
FS	Functional Safety
MTTR	Mean Time To Restoration
NTP	Network Time Protocol
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller
PELV	Protective extra low voltage
PL	Performance level
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SAid	Safety Application identifier
SRAC	Safety Related Application Condition
SRT	System Reaction Time
UID	Unique IDentifier
VS	Voltage Supply

SIL2 and SIL3

NOTE:

- Each time in the document that SIL2 or SIL3 is mentioned without a standard reference, this is regarding IEC 61508 / IEC 61511.
- Each time SIL2 is mentioned, it is also SIL3 regarding EN 50126 / EN 50128 / EN 50129.
- Each time SIL3 is mentioned, it is also SIL4 regarding EN 50126 / EN 50128 / EN 50129.

Verification Process

Requirements

Five subsets of requirements have been extracted from the following documents:

- requirements related to the Application Life Cycle as described in the Modicon M580, Safety Manual
- requirements related to the Safety Information Messages of the Modicon M580, Safety Manual
- requirements related to the Safety Information Messages of the Modicon M580, Safety System Planning Guide
- requirements related to the Safety Information Messages of the EcoStruxure Control Expert, Safety Block Library
- requirements related to the Safety Information Messages of the Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications

Therefore, five separate checklists are constructed in the next chapter, corresponding to each subset of requirements.

The verification process consists of checking that all the identified requirements have been correctly taken into account in the specific project application submitted to verification.

NOTE:

- Each time SIL2 or SIL3 is mentioned in the document without a standard reference, it relates to IEC 61508 / IEC 61511.
- Each time SIL2 is mentioned, it also relates to SIL3 regarding EN 50126 / EN 50128 / EN 50129.
- Each time SIL3 is mentioned, it also relates to SIL4 regarding EN 50126 / EN 50128 / EN 50129.

You can find the most recent information on the certified product versions on the TÜV Rheinland Group website:
www.certipedia.com or www.fs-products.com

Pre-condition

The people in charge of the SRAC's verification justify the following conditions:

- level of independency (i.e. independency vs. the design team)
- level of competence in Functional Safety (i.e. 3rd part FS training certificate)
- level of competence in Modicon M580 Safety and Control Expert (i.e. Schneider Electric M580 safety training certificate)

Exclusions

This document is valid only with the referenced documents and revisions, as listed in the Related Documents, page 9 topic.

Safety Related Application Requirements

Application Life Cycle Requirements

The following table is a checklist of requirements related to the Application Life Cycle. For more information on the related requirement, refer to the Modicon M580, Safety Manual.

Id	Application Life Cycle Requirement	Done	Justification
Application Life Cycle **> Step 9: E/E/PE System safety requirements specification**			
LC #1	This step occurs when the risk analysis is completed and has provided, among other things, the following information: • definition of the safety integrated functions • their required performances (time, risk reduction, SIL…) • their failure modes	□ □ □	
LC #2	Produces the safety requirement specifications which include, at least, the following information necessary to design a safe application using any type of Safety controller. • safe state of the safety integrated functions • SIS operating mode analysis (including the behavior in run, stop, power on sequence, maintenance, repair…) • test interval of the SIF • MTTR of the SIS • choice of energized or de-energized SIF • performance of the logic solver (reaction time, precision …) • performance requirements • fault tolerance • integrity • maximum spurious trip rate • maximum dangerous fault rate • environmental specification (EMC, mechanical, chemical, climate…)	□ □ □ □ □ □ □ □ □ □ □ □ □	

Id	Application Life Cycle Requirement	Done	Justification
	> Step 10: E/E/PE Safety related systems realization		

LC #3	The goal of the first sub-steps (10.1) is to convert the SIS safety requirements into a specification of the hardware design, hardware tests, software design, software tests, and integration tests. It should provide at least the following information necessary to design a safe application using safety M580:
	• hardware architecture that defines:
	  • the respect of M580 rules about mixing non-Safety and Safety modules (All Safety modules — Safety I/O modules and Safety processors/co-processors — are installed on backplanes where the main backplane and its extension backplane are powered by Safety power supply modules and contain only Safety modules or non-interfering type 1 modules.)
	  • electric consumption per rack
	  • derating rules
	• power supply architecture:
	  • only PELV power supply
	• software architecture:
	  • including the usage of M580 global variables (A global variable should not prevent a safety action to be triggered unless a *safe application protocol* is used.)
	• hardware integration (cabling, cabinet, and so forth):
	  • fuse protection
	  • accessories for wire diagnostic
	• human machine interfaces:
	  • including the usage of M580 global variables (A global variable should not prevent a safety action to be triggered unless a *safe application protocol* is used.)
	• electric/numerical interfaces:
	  • safe state
	  • sensor and actuator
	• algorithm
	• performances (including task period, watchdog, and timeout definition) and prediction of good behavior using this formula:
	$\Sigma_{all\ tasks} \frac{Exe_{task}}{Period_{task}} < 80\%$
	• behavior in case of:
	  • unlocked configuration
	  • maintenance mode
	  • maintenance input
	  • invalid channel
	  • wiring failure
	  • channel health
	  • module health
	• management of the UID of the Safety I/O modules (define when a UID should be changed).
	• NTP server:
	  • choice of controller as NTP server or external NTP server (depending on the usage of I/O time stamping in the process application)
	  • server redundancy
	  • server loss
		□
		□
		□
		
		□
		
		□
		
		□
		
		□
		
		□
		□
		
		□
		□
		□
		□
		□
		□
		□
		
		□
		□
		□	

Id	Application Life Cycle Requirement	Done	Justification
	> Step 12: Overall installation and commissioning		
LC #4	The goal of this step is to define the requirements for installation, task planning, tooling, commissioning procedure and then build the system and verify its correctness. • For Hot Standby applications, verify that the fallback timeout of the Safety output modules fits the conditions defined for swap and switchover operations, and verify the CRA hold-up time. • Verify that fallback safety timeout (S_TO) for the safety output modules is, at least, greater than the greater of 40 ms or (2.5 * TSAFE), where TSAFE equals the configured SAFE task period. • Clear any pre-existing application inside the PLC, or use an application configured with no CIP safety devices before installing the safety device onto an Ethernet safety network (with CIP safety devices).	□ □ □	

LC #5	In an M580 safety system, the commissioning procedure should include the following points:
	• Verify Control Expert integrity, verify Control Expert version.
	• Correctness of the processor and coprocessor firmware versions by supervising the system words %SW14 (firmware version of the processor) and %SW142 (firmware version of the coprocessor).
	• Correctness of each module addresses (position in rack, CRA switches)
	• Correctness of the cabling:
	  • point– to– point verification: from internal variable to I/O module and to actuator/sensor
	  • fuses
	  • equipment for wiring diagnostic
	• At the end of the procedure, all Safety modules are in *lock* mode (The safe application should check this condition).
	• Correctness of each module configuration (including the timeouts):
	  • Read the configuration using the Control Expert screen and compare to specification.
	• All the safety applications have been rebuilt using the **Rebuild All Project** option, then downloaded to each controller, and their SAId saved as well as the application archive.
	• The task period and task watchdog are correct.
	• Module references and version
	• Use PELV only.
	• If CIP Safety devices are used in the safety application:
	  • The Safety Configuration ID signature (SCID) can be verified (option enabled in Control Expert CIP Safety DTM) and target configuration can be locked after user testing.
	  • To confirm that the originator configuration created by the user with the Control Expert software tool was correctly sent to and saved in the M580 CIP Safety originator, visually compare all CIP Safety target configuration parameter values displayed in the target DDDTs (in connected mode with the controller, using an animation table) with the parameter values displayed and configured in the target DTM Configuration verification tab. All values need to be identical.
	  • Test all safety connection configurations after they are applied in the M580 CIP Safety originator to confirm that each target connection is operating as intended.
	  • Before installing the CIP Safety devices on the safety network, commission all safety devices with MacId and Baud Rate as necessary.
	• User testing is the means by which all application downloads are validated.
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□
		□	

Id	Application Life Cycle Requirement	Done	Justification
	> Step 13: Overall safety validation		
LC #6	The goal of this step is to prove that the safety-integrated system fulfills its requirements. It executes all the tests and produce the reports define in step 7 of the *safety lifecycle* and should: • Verify that there is no overrun condition during any of the system state (verification of the system bit %S19 in the MAST, FAST, AUX0 tasks), and that the max and current SAFE task execution time (%SW42 and %SW43) are below the SAFE task period. • Verify the CPU load formula: $\Sigma_{all\ tasks} \frac{Exe_{task}}{Period_{task}} < 80\%$ **NOTE:** You can use the system words %SW110 to %SW115 to perform a real-time evaluation of the average load for CPU tasks (if all tasks are periodic, % SW116 should be less than 80). • Verify the special operating modes (module unlock, maintenance input, invalid channel, wiring defect). • For Hot Standby applications, verify that all tasks are correctly synchronized through the Hot Standby link by checking and using the MAST_SYNCHRONIZED, FAST_ SYNCHRONIZED, and SAFE-SYNCHRONIZED bits in the T_M_ECPU_HSBY DDT. Refer to the *Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures* for a description of the T_M_ECPU_HSBY DDT.	□ □ □ □	
	> Step 14: Overall operation, maintenance and repair		
LC #7	• Execute the proof tests at the right period. • Monitor the SAId. (See below note). **NOTE:** As long as the SAId has not changed, the safety portion of the application has not been changed. Refer to the S_SYST_STAT_MX function block for details on SAId behavior. • Monitor the configuration lock status of each safety module. • Record the repair operations. • If a module is replaced, properly configure the replacement module and verify its operation. Execute (at minimum) the commissioning operations related to this module. • Record the deviations.	□ □ □ □ □	
	> Step 15: Overall modification and retrofit		
LC #8	• Treat all modifications as new designs. An impact analysis may help define the part of the former safety system that can be kept and the part that must be designed again. **NOTE:** If an application modification does not concern the SAFE application, you can use the SourceSafeSignature to verify that no unwanted modification has been introduced to the SAFE code. The SourceSafeSignature is an a priori verification that the application is unchanged. • SourceSafeSignature does not replace the SAId, which is the only measure that reliably confirms a controller is executing the same SAFE application that was validated.	□ □	

Safety Information — M580 Safety Manual

Checklist of requirements related to the Safety Information Messages of the Safety Manual. For more information on the related requirement, refer to the Modicon M580, Safety Manual .

Id	Safety Information Message Requirement	Done	Justification
Safety Information			
	> Before You Begin		
SM #1	UNGUARDED EQUIPMENT Do not use this software and related automation equipment that does not have point-of-operation protection. Do not reach into machinery during operation.	□ □	
	> Start and Test		
SM #2	EQUIPMENT OPERATION HAZARD • Verify that all installation and set-up procedures have been completed. • Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices. • Remove tools, meters, and debris from equipment.	□ □ □	
M580 Safety Function			
	> Safety Loop		
SM #3	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS • Use only safety modules to perform safety functions. • Do not use inputs or outputs of non-interfering modules for safety-related functions. • Do not use variables from the global area for safety-related functions.	□ □ □	
M580 Safety System Supported Modules			
	> Safety Loop		
SM #4	INCORRECT USE OF SAFETY-RELATED DATA Confirm that neither input data nor output data from non-interfering modules are used for controlling safety-related outputs. Non-safety modules can process only non-safety data.	□	
M580 Safety I/O Modules **> M580 Safety I/O Module Shared Features**			
	> External Power Supply Used with Digital Safety I/O		
SM #5	PELV OVER-VOLTAGE CATEGORY II POWER SUPPLY REQUIRED Use only an PELV-type over-voltage category II power supply with a maximum output of 60 Vdc to supply power to sensors and actuators.	□	
M580 Safety I/O Modules **> BMXSAI0410 Analog Input Module**			
	> BMXSAI0410 Input Application Wiring Examples		
SM #6	RISK OF UNINTENDED OPERATION The maximum safety integrity level (SIL) is determined by the quality of sensor and the length of the proof-test interval to IEC 61508. If you are using sensors that do not meet the quality of the intended SIL standard, wire these sensors redundantly to two channels.	□	
> SIL3 Cat2/PLd			
SM #7	RISK OF UNINTENDED OPERATION	□	

Id	Safety Information Message Requirement	Done	Justification
	To achieve SIL3 according to IEC 61508 and Category 2/Performance Level d according to ISO13849 using this wiring design, use a suitable, qualified sensor.		
	> SIL3 Cat/PLd with High Availability		
SM #8	RISK OF UNINTENDED OPERATION To achieve SIL3 according to IEC 61508 and Category 2/Performance Level d according to ISO13849 using this wiring design, use a suitable, qualified sensor.	□	
	SIL3 Cat4/PLe		
SM #9	RISK OF UNINTENDED OPERATION To achieve SIL3 according to IEC 61508 and Category 4/Performance Level e according to ISO13849 using this wiring design, use a suitable, qualified sensor.	□	
	> SIL3 Cat4/PLe with High Availability		
SM #10	RISK OF UNINTENDED OPERATION To achieve SIL3 according to IEC 61508 and Category 4/Performance Level e according to ISO13849 using this wiring design, use a suitable, qualified sensor.	□	
M580 Safety I/O Modules **> BMXSDI1602 Digital Input Module > BMXSDI1602 Input Application Wiring Examples**			
SM #11	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS Use only an PELV-type process power supply module with a maximum output of 60 V.	□	
SM #12	IMPROPER FUSE SELECTION Use fast-acting fuses to help protect the electronic components of the digital input module from an over-current condition. Improper fuse selection can result in damage to the input module.	□	
SM #13	RISK OF UNINTENDED OPERATION The maximum safety integrity level (SIL) is determined by the quality of sensor and the length of the proof-test interval to IEC 61508. If you use sensors that do not meet the quality of the intended SIL standard, wire these sensors redundantly to two channels.	□	
SM #14	RISK OF UNINTENDED OPERATION Enable the available diagnostics provided in Control Expert to detect or exclude the conditions previously listed. If a diagnostic test is not enabled or is not available in Control Expert, apply another safety measure to detect or exclude these conditions.	□	
	> SIL3 Cat2/PLd		
SM #15	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group. Apply another safety measure to detect or exclude this condition.	□	
SM #16	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels (in the case of a single sensor connected with one input, powered by external power, depicted above).. Apply another safety measure to detect or exclude this condition.	□	
SM #17	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of a single sensor connected with one input, powered by external power, depicted above).. Apply another safety measure to detect or exclude this condition.	□	
	> SIL3 Cat2/PLd with High Availability		
SM #18	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS	□	

Id	Safety Information Message Requirement	Done	Justification
	The module cannot detect crossed circuits between two channels (in the case of a single sensor connected to two inputs, powered by external power, depicted above).. Apply another safety measure to detect or exclude this condition.		
SM #19	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of a single sensor connected on two inputs, powered by external power, depicted above).. Apply another safety measure to detect or exclude this condition.	□	
SM #20	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group. Apply another safety measure to detect or exclude this condition.	□	
SM #21	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels (in the case of two redundant sensors connected on a single input of two modules, using external power).. Apply another safety measure to detect or exclude this condition.	□	
SM #22	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of two redundant sensors connected on a single input of two modules using external power). Apply another safety measure to detect or exclude this condition.	□	
	> Cat4/PLe		
SM #23	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group. Apply another safety measure to detect or exclude this condition.	□	
SM #24	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels (in the case of a single sensor connected on two inputs of the same module using external power).. Apply another safety measure to detect or exclude this condition.	□	
SM #25	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of a single sensor connected on two inputs of the same module using external power). Apply another safety measure to detect or exclude this condition.	□	
SM #26	RISK OF UNINTENDED OPERATION To achieve SIL3 according to IEC 61508 and Category 4/Performance Level e according to ISO13849 using this wiring design, use suitable, qualified sensors.	□	
SM #27	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group (in the case of the acquisition of the same process variable using two separated sensors using VS supplied power). Apply another safety measure to detect or exclude this condition.	□	
SM #28	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of the acquisition of the same process variable using two separated sensors using VS supplied power). Apply another safety measure to detect or exclude this condition.	□	
SM #29	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels (in the case of the acquisition of the same process variable using two separated sensors using external power). Apply another safety measure to detect or exclude this condition.	□	

Id	Safety Information Message Requirement	Done	Justification
SM #30	RISK OF UNINTENDED OPERATION To achieve SIL3/Cat4/PLe using this wiring design, use suitable, qualified sensors.	□	
	> Cat4/PLe with High Availability		
SM #31	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group. Apply another safety measure to detect or exclude this condition.	□	
SM #32	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels (in the case of a single channel connection of two redundant single-channel sensors using external power). Apply another safety measure to detect or exclude this condition.	□	
SM #33	RISK OF SHORT CIRCUIT TO THE 24 VDC The module cannot detect a short circuit to the 24 Vdc condition (in the case of a single channel connection of two redundant single-channel sensors using external power). Apply another safety measure to detect or exclude this condition.	□	
SM #34	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS IN THE SAME GROUP The module cannot detect crossed circuits between two channels in the same channel VS group. Apply another safety measure to detect or exclude this condition.	□	
SM #35	RISK OF CROSSED CIRCUITS BETWEEN CHANNELS The module cannot detect crossed circuits between two channels. Apply another safety measure to detect or exclude this condition.	□	
SM #36	RISK OF UNINTENDED OPERATION To achieve SIL3 according to IEC 61508 and Category 4/Performance Level e according to ISO13849 using this wiring design, use suitable, qualified sensors.	□	
M580 Safety I/O Modules **> BMXSDO0802 Safety Digital Output Module**			
SM #37	IMPROPER FUSE SELECTION Use fast-acting fuses to help protect the electronic components of the digital output module from an over-current condition. Improper fuse selection can result in damage to the module.	□	
	> BMXSDO0802 Output Application Wiring Examples		
SM #38	RISK OF UNINTENDED OPERATION The maximum safety integrity level (SIL) is determined by the quality of the actuator and the length of the proof-test interval to IEC 61508. If you use actuators that do not meet the quality of the intended SIL standard, wire these actuators redundantly to two channels.	□	
SM #39	RISK OF UNINTENDED OPERATION When the equipment is used in a fire and gas application or when the demand state of the output is energized: • Verify that your proof-test procedure includes a test that the cut wire detection is effective by removing the terminal block and verifying that the corresponding error bits are set. □ • Verify that short circuit to ground detection effectiveness either by enabling the pulse test to energized diagnostic function in the module's **Configuration** tab or by implementing another procedure (for example, by setting the output to 1 and checking the diagnostics, and so forth. □ • Avoid using lamp-like actuators because their impedance is very low when they are switched on, which can result in a risk of detecting a false short circuit overload condition. □		
	> Configurable Wiring Diagnostics in Control Expert		

Id	Safety Information Message Requirement	Done	Justification
SM #40	RISK OF UNINTENDED OPERATION Enable the available diagnostics provided in Control Expert to detect and respond to the conditions listed above. If a diagnostic test is not enabled or is not available in Control Expert, apply another safety measure to detect or exclude these conditions.	□	
	> Output Wiring Diagnostic Summary		
SM #41	RISK OF SHORT CIRCUIT TO 0 VDC GROUND For the short circuit to the 0 V ground condition with the output state de-energized, enable the short circuit to 24 V dection option in the module's **Configuration** tab. Alternatively, apply another safety measure to detect or exclude this condition.	□	
SM #42	RISK OF SHORT CIRCUIT TO THE 24 VDC For the short circuit to the 24 Vdc condition with the output state energized or de-energized, enable the short circuit to 24 V detection option in the module's **Configuration** tab. Alternatively, apply another safety measure to detect or exclude this condition.	□	
SM #43	RISK OF CROSSED CIRCUITS The module cannot detect the crossed circuits between two channels condition with the output state de-energized and the other channel de-energized. If it occurs when the output state changes to energized, apply another safety measure to detect or exclude this condition.	□	
SM #44	RISK OF CROSSED CIRCUITS For the crossed circuits between two channels condition with the output state de-energized and the other channel energized, enable the short circuit to 24 V detection option in the module's **Configuration** tab. Alternatively, apply another safety measure to detect or exclude this condition when the output state changes to energized.	□	
SM #45	RISK OF CROSSED CIRCUITS The module cannot detect the crossed circuits between two channels condition with the output state energized and the other channel de-energized. Apply another safety measure to detect or exclude this condition.	□	
SM #46	RISK OF CROSSED CIRCUITS For the crossed circuits between two channels condition with the output state energized and the other channel de-energized, enable the short circuit to 24 V detection option in the module's **Configuration** tab. Alternatively, apply another safety measure to detect or exclude this condition when the output state changes to energized.	□	
M580 Safety I/O Modules **> BMXSRA0405 Safety Digital Relay Output Module**			
	> BMXSRA0405 Wiring Connector		
SM #47	RISK OF UNINTENDED OPERATION implement appropriate wiring diagnostics to detect and help prevent the occurrence of dangerous faults on the external wiring.	□	
	> Application_1: 4 Outputs, SIL2 / Cat2 / PLc, De-energized State, No Automatic Signal Test		
SM #48	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS To achieve SIL2 according to IEC61508 and Category 2 / Performance Level c according to ISO 13849 using this wiring design, you need to perform a daily signal transition from the energized state to the de-energized state.	□	
	> Application_3: 4 Outputs, SIL2 / Cat2 / PLc, De-energized State, No Automatic Signal Test		
SM #49	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS To achieve SIL2 according to IEC61508 and Category 2 / Performance Level c according to ISO 13849 using this wiring design, perform a daily signal transition from the energized state to the de-energized state.	□	

Id	Safety Information Message Requirement	Done	Justification
	> Application_5: 2 Outputs, SIL3 / Cat4 / PLe, De-energized State, No Automatic Signal Test		
SM #50	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS To achieve SIL3 according to IEC61508 and Category 4 / Performance Level e according to ISO 13849 using this wiring design, perform a daily signal transition from the energized state to the de-energized state.	□	
	> Application_7: 2 Outputs, SIL3 / Cat4 / PLe, De-energized State, No Automatic Signal Test		
SM #51	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS To achieve SIL3 according to IEC61508 and Category 4 / Performance Level e according to ISO 13849 using this wiring design, perform a daily signal transition from the energized state to the de-energized state.	□	
M580 Safety Power Supplies			
SM #52	LOSS OF THE ABILITY TO PERFORM SAFETY FUNCTIONS Use only a BMXCPS4002S, BMXCPS4022S, or BMXCPS3522S power supply module in any backplane that includes an M580 safety module. Check both your physical installation and your project in Control Expert to confirm that only M580 safety power supply modules are used.	□	
Validating an M580 Safety System **> M580 Safety System Performance and Timing Calculations**			
SM #53	RISK OF UNINTENDED EQUIPMENT OPERATION Set the fallback safety timeout (S_TO) for a safety output module to a value greater than the greater of 40 ms or (2.5* TSAFE) where TSAFE equals the configured SAFE task period.	□	
SM #54	RISK OF EXCEEDING THE PROCESS SAFETY TIME Set the maximum CPU SAFE task period by considering your process safety time. Verify that your CPU SAFE task period is less than your project process safety time.	□	
Safety Library **> Certified Safety Functions and Function Blocks**			
SM #55	UNINTENDED APPLICATION BEHAVIOR • Do not use V1.00 of the S_GUARD_LOCKING derived function block in your application. • In Control Expert 13.0 XLS or later, update the S_GUARD_ LOCKING function block in your application with V1.01 or later, and rebuild the application.	□ □	
M580 Safety System Communications **> NTP Service**			
	> Configuring the NTP Service		
SM #56	RISK OF UNINTENDED OPERATION If you install safety I/O modules in an RIO drop, configure the current time for the controller with firmware 3.10 or earlier. Enable the NTP service for your M580 system and configure the safety controller as an NTP server or an NTP client.	□	
	> Changing the NTP Time Setting During Operations		
SM #57	RISK OF SAFETY SYSTEM SHUTDOWN • Use Control Expert 13.0 or 13.1 with controller firmware 2.70 or earlier. Do not change the time setting in the NTP server or the controller. •	□ □	
	>Procedure for Synchronizing the NTP Time Settings		
SM #58	RISK OF INOPERABLE EQUIPMENT When using the Update Controller time (optional feature) on a BMENOP0300 module, a BMENOC0301 module, or a BMENOC0311 module to update the controller time, synchronize the SAFE time with the	□	

Id	Safety Information Message Requirement	Done	Justification
	external NTP server by using %SW128 after the NTP server becomes operational (when %SW152 changes from 0 to 1). Perform the steps in the following procedure for synchronizing the NTP time set.		
SM #59	RISK OF SYSTEM SAFETY SHUTDOWN • If you use Control Expert 14.0 or later and firmware 2.80 or later to perform a controller time modification, perform the synchronized procedure previously described. • If you do not perform a synchronization procedure, the safety I/O modules can enter their SAFE or fallback state after the clock drifts for about a communication delay timeout.	□ □	
	> Configuring the S_WR_ETH_MX DFB		
SM #60	LOSS OF ABILITY TO PERFORM SAFETY FUNCTIONS Verify that the ID parameter value is unique and fixed in the network for a sender/receiver pair.	□	
	> Configuring the S_RD_ETH_MX DFB		
SM #61	LOSS OF ABILITY TO PERFORM SAFETY FUNCTIONS • Call the S_RD_ETH_MX DFB function block at each cycle in the receiver controller program logic. Execute the function block before the data in the cycle is used. • Verify that the ID parameter value is unique and fixed in the network for a sender/receiver pair. • Test the HEALTH bit value of the S_RD_ETH_MX DFB at each cycle before using any safe data to manage the safety function.	□ □ □	
	> Configuring the S_WR_ETH_MX2 DFB		
SM #62	LOSS OF ABILITY TO PERFORM SAFETY FUNCTIONS Verify that the ID parameter value is unique and fixed in the network for a sender/receiver pair.	□	
	> Configuring the S_RD_ETH_MX2 DFB		
SM #63	LOSS OF ABILITY TO PERFORM SAFETY FUNCTIONS • Call the S_RD_ETH_MX2 DFB function block at each cycle in the receiver controller program logic, and execute it before the data in the cycle is used. • Verify that the ID parameter is unique and fixed in the network for a sender/receiver pair. • Test the HEALTH bit value of the S_RD_ETH_MX2 DFB at each cycle before using any SAFE data to manage the safety function.	□ □ □	
	> M580 Black Channel Communications		
SM #64	RISK OF UNINTENDED OPERATION If you install safety I/O modules in an RIO drop, configure the current time for the controller with firmware 3.10 or earlier. Enable the NTP service for your M580 system and configure the safety controller as an NTP server or an NTP client.	□	
SM #65	UNINTENDED OUTPUT STATE CHANGE UPON RE-ESTABLISHING COMMUNICATION Monitor the health status of the output channels with program logic, and activate the safety function accordingly by setting the output commands to the SAFE state.	□	
Diagnosing an M580 Safety System **> M580 Safety Controller and Coprocessor Diagnostics**			
	> M580 Safety Controller LED Diagnostics		
SM #66	RISK OF INACCURATE SYSTEM DIAGNOSTICS Do not use LEDs as operational indicators.	□	
Operating an M580 Safety System **> Operating Modes, Operating States, and Tasks**			
	> Maintenance Mode Functionality		

Id	Safety Information Message Requirement	Done	Justification
SM #67	LOSS OF THE SAFETY INTEGRITY LEVEL While the safety controller is in maintenance mode, take appropriate measures to help ensure the SAFE state of the system.	□	
	> Start-up Sequence		
SM #68	UNINTENDED EQUIPMENT OPERATION Confirm that selecting automatic start in RUN is compliant with the correct behavior of your system; otherwise, de-activate this feature.	□	
	> Locking M580 Safety I/O Module Configurations		
SM #69	LOSS OF SAFETY INTEGRITY LEVEL Lock each safety I/O module after it is configured and before beginning operations.	□	
SM #70	UNINTENDED VARIABLE VALUE • Verify that your application has the current project settings. • Verify that the syntax to access the variables in the different namespaces.	□	
CIP Safety **> CIP Safety Operations**			
	> Configuring the CIP Safety Device Using a Vendor-provided Tool		
SM #71	RISK OF UNINTENDED EQUIPMENT OPERATION If you configure an M580 controller as a CIP Safety originator, test and verify that the CIP Safety functional behavior of the system before using CIP Safety communication to control the related safety function. After testing and verification are successfully completed, enable the CIP Safety target configuration signature (if one exists) in the Control Expert Safety DTMs.	□	
	> Interactions Between Safety Controller Operations and the Target Connection		
SM #72	RISK OF UNINTENDED EQUIPMENT OPERATION Do not use the CTRL_IN or CTRL_OUT bits as a safety measure to set the target data into a SAFE state.	□	

Safety Information — M580 Safety System Planning Guide

The following table is a checklist of all safety information related to the Safety Information Messages of the *M580 Safety System Planning Guide*. For more information on the related requirement, refer to the Modicon M580, Safety System Planning Guide.

Id	Safety Information Message Requirement	Done	Justification
Safety Information			
	> Before You Begin		
PG #1	UNGUARDED EQUIPMENT • Do not use this software and related automation equipment on equipment that does not have point-of-operation protection. • Do not reach into machinery during operation.	□ □	
PG #2	**> Start Up and Test**		
	EQUIPMENT OPERATION HAZARD • Verify that all installation and set-up procedures have been completed. • Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices. • Remove tools, meters, and debris from equipment.	□ □ □	
M580 Safety System Supported Modules			
	> Non-Interfering Modules		
PG #3	INCORRECT USE OF SAFETY-RELATED DATA Confirm that neither input data nor output data from non-interfering modules are used for controlling safety-related outputs. Non-safety modules can process only non-safety data.	□	
M580 Safety Processor and Coprocessor			
	> M580 Safety Processor and Coprocessor Physical Features		
PG #4	HAZARD OF ELECTRIC SHOCK If you cannot prove that the end of a shielded cable is connected to the local ground, consider the cable dangerous and wear personal protective equipment (PPE).	□	
Installing the M580 Safety Controller			
	> Installing M580 Backplanes and Extender Modules		
PG #5	UNINTENDED EQUIPMENT OPERATION Install the backplanes lengthwise and horizontally to facilitate ventilation.	□	
PG #6	OVERHEATING AND UNINTENDED EQUIPMENT OPERATION Maintain proper thermal clearances when installing the backplanes.	□	
	> Installing M580 Processors, Coprocessors, Power Supply, and I/O Modules		
PG #7	HAZARD OF ELECTRIC SHOCK Remove all power sources before installing the controller.	□	
PG #9	HAZARD OF ELECTRIC SHOCK If you cannot prove that the end of a shielded cable is connected to the local ground, consider the cable dangerous and wear personal protective equipment (PPE).	□	
PG #10	LOSS OF THE ABILITY TO PERFORM THE SAFETY FUNCTION Use only the BMXCPS4002S, BMXCPS4022S, or BMXCPS3522S safety power supply on any backplane that also includes at least one safety module.	□	
PG #11	RISK OF UNINTENDED SYSTEM BEHAVIOR Confirm that power is turned off when either removing an M580 safety power supply module from a backplane, or inserting it into a backplane.	□	

Id	Safety Information Message Requirement	Done	Justification
PG #12	RISK OF UNINTENDED SYSTEM BEHAVIOR Confirm that power is turned off – i.e. the upstream breaker must be OFF – before plugging in, or unplugging the main input removable terminal block of the M580 safety power supply module.	□	
PG #13	RISK OF UNINTENDED SYSTEM BEHAVIOR Confirm that the M580 safety power supply module is de-energized before plugging in, or unplugging the module's alarm relay removable terminal block.	□	
PG #14	HAZARD OF ELECTRIC SHOCK If you cannot prove that the end of a shielded cable is connected to the local ground, the cable must be considered as dangerous and personal protective equipment (PPE) must be worn.	□	
PG #15	HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH While mounting or removing safety I/O modules: • Verify that each terminal block remains connected to the BMXXSP•••• grounding bar. • Disconnect the voltage that supplies the sensors and actuators.	□ □	
Operating an M580 Safety System **> Operating Modes, Operating States, and Tasks**			
PG #16	LOSS OF THE SAFETY INTEGRITY LEVEL While the safety controller is in maintenance mode, take appropriate measures to help ensure the safe state of the system.	□	
PG #17	UNINTENDED EQUIPMENT OPERATION Confirm that selecting automatic start in RUN mode is compliant with the correct behavior of your system; otherwise, de-activate this feature.	□	
	> Locking M580 Safety I/O Module Configurations		
PG #18	RISK OF UNINTENDED DEGRADATION TO PROJECT SAFETY INTEGRITY LEVEL Lock each safety I/O module after it is configured and before beginning operations.	□	
	> Working with Animation Tables in Control Expert		
PG #19	UNINTENDED VARIABLE VALUE • Verify that your application has the correct project settings. • Verify the syntax to access the variables in the different namespaces.	□ □	

Safety Information — EcoStruxure™ Control Expert Safety Block Library

Checklist of requirements related to the Safety Information Messages of the Safety Block Library. For more information on the related requirements, refer to *EcoStruxure™ Control Expert, Safety Block Library*[4], page 9 .

Id	Safety Information Message Requirement	Done	Justification
About the Book			
	> Product Related Information		
LIB #1	UNINTENDED EQUIPMENT OPERATION Use only Schneider Electric approved software.	□	
LIB #2	UNINTENDED EQUIPMENT OPERATION • Refer to IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety related systems". • Completely understand the applications and environment defined by Safety Integrity Level (SIL) 3 within IEC 61508 Parts 1-7, edition 2.0. • Do Not exceed SIL3 ratings in the application of this product.	□ □ □	
S_EDM: Actuator Error Detection Monitoring			
	> Description		
LIB #3	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_ENABLE_SWITCH: Three Position Enable Switch			
	> Description		
LIB #4	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_ESPE: Electro-Sensitive Protective Equipment			
	> Description		
LIB #5	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_GUARD_LOCKING: Guard Lock Control			
	> Description		
LIB #6	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_GUARD_MONITORING: Guard Lock Monitoring			
	> Description		
LIB #7	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_OUTCONTROL: Output Driver			
	> Description		
LIB #8	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	

Id	Safety Information Message Requirement	Done	Justification
S_AI_COMP: Analog Input Compare			
	> Description		
LIB #9	LOSS OF THE SAFETY INTEGRITY LEVEL Code that includes the S_AI_COMP function block must be certified in accordance with IEC61508 before it is used in operation.	□	
S_EMERGENCYSTOP: Emergency Stop Monitor			
	> Description		
LIB #10	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_MUTING_PAR: Parallel Muting			
	> Description		
LIB #11	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_MUTING_SEQ: Sequential Muting			
	> Description		
LIB #12	RISK OF UNINTENDED OPERATION Activate the S_StartReset and S_AutoReset inputs only after you verify that no hazardous situation can occur if the system is started.	□	
S_AIHA: High Availability for Mx80 Safety Analog Inputs			
	> Description		
LIB #13	LOSS OF THE SAFETY INTEGRITY LEVEL Code that includes the S_AIHA function block must be certified in accordance with IEC61508 before it is used in operation.	□	
S_DIHA: High Availability for Mx80 Safety Digital Inputs			
	> Description		
LIB #14	LOSS OF THE SAFETY INTEGRITY LEVEL Code that includes the S_DIHA function block must be certified in accordance with IEC61508 before it is used in operation.	□	

Safety Information — Standards and Certifications

Checklist of requirements related to the Safety Information Messages of the Standards and Certifications. For more information on the related requirement, refer to Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications.

Id	Safety Information Message Requirement	Done	Justification
About the Book **> Product Related Information**			
CERT #1	UNINTENDED EQUIPMENT OPERATION • The application of this product requires expertise in the design and programming of safety control systems. Only persons with such expertise are allowed to program, install, alter, and apply this product. • Follow all local and national safety codes and standards.	□ □	
Installation General Rules			
CERT #2	Check and verify that **Installations General Rules** comply with the ones defined in document Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications.	□	
Operating and Storage Conditions			
CERT #3	Check and verify that **Operating and Storage Conditions** comply with the ones defined in document Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications.	□	

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

EIO0000004540.02