Modicon M580

Safety System Planning Guide

Original instructions

09/2019

QGH60283.05

www.schneider-electric.com

Schneider Electric

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

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

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

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

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

Table of Contents

Safety Information

Important Information

NOTICE

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

PLEASE NOTE

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

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

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 be 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 (English version prevails):

- 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 actually 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

At a Glance

Document Scope

This Safety System Planning Guide describes the modules of the M580 Safety system with special regard to how they meet the Safety requirements of the IEC 61508. It provides detailed information on how to install, run, and maintain the system correctly in order to help protect human beings as well as to help prevent damage to environment, equipment, and production.

This documentation is intended for qualified personnel familiar with Functional Safety and Control Expert XL Safety. Commissioning and operating the M580 Safety System may only be performed by persons who are authorized to commission and operate systems in accordance with established Functional Safety standards.

Validity Note

This document is valid for EcoStruxure™ Control Expert 14.1 or later.

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

The technical characteristics of the devices described in the present document also appear online. To access the information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the reference or product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the datasheet.
6	To save or print a datasheet as a .pdf file, click **Download XXX product datasheet**.

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

Related Documents

Title of documentation	Reference number
M580 Safety Manual	QGH46982 (English), QGH46983 (French), QGH46984 (German), QGH46985 (Italian), QGH46986 (Spanish), QGH46987 (Chinese)
EcoStruxure™ Control Expert Safety Block Library	QGH60275 (English), QGH60278 (French), QGH60279 (German), QGH60280 (Italian), QGH60281 (Spanish), QGH60282 (Chinese)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (English), EIO0000002001 (French), EIO0000002000 (German), EIO0000002002 (Italian), EIO0000002003 (Spanish), EIO0000002004 (Chinese)
Modicon M580, Hardware, Reference Manual	EIO0000001578 (English), EIO0000001579 (French), EIO0000001580 (German), EIO0000001582 (Italian), EIO0000001581 (Spanish), EIO0000001583 (Chinese)
Modicon M580 Standalone System Planning Guide for Frequently Used Architectures	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Modicon M580 System Planning Guide for Complex Topologies	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chinese)
Unity Loader, User Manual	33003805 (English), 33003806 (French), 33003807 (German), 33003809 (Italian), 33003808 (Spanish), 33003810 (Chinese)
EcoStruxure™ Control Expert, Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003104 (Spanish), 33003696 (Italian), 33003697 (Chinese)
EcoStruxure™ Control Expert, System Bits and Words, Reference Manual	EIO0000002135 (English), EIO0000002136 (French), EIO0000002137 (German), EIO0000002138 (Italian), EIO0000002139 (Spanish), EIO0000002140 (Chinese)

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

Chapter 1
M580 Safety System Supported Modules

Introduction

An M580 safety project can include both safety modules and non-safety modules. You can use:

- Safety modules in the SAFE task.
- Non-safety modules only for the non-safe tasks (MAST, FAST, AUX0, and AUX1).
  NOTE: Only non-safety modules that do not interfere with the safety function can be added to a safety project.

Use only the Control Expert programming software of Schneider Electric for programming, commissioning, and operating your M580 safety application.

- Control Expert L Safety provides all the functionality of Control Expert L and can be used with BMEP582040S and BMEH582040S safety CPUs.
- Control Expert XL Safety provides all the functionality of Control Expert XL and can be used for the entire range of BMEP58•040S and BMEH58•040S safety CPUs.

This chapter lists the safety and non-safety modules supported by the M580 safety system.

What Is in This Chapter?

This chapter contains the following topics:

M580 Safety System Certified Modules

Certified Modules

The M580 safety PAC is a safety-related system certified by TÜV Rheinland Group, according to:

- SIL3/IEC 61508/IEC 61511
- SIL CL3/IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

It is based on the M580 family of programmable automation controllers (PACs). The following Schneider Electric M580 safety modules are certified:

- BMEP584040S standalone CPU
- BMEP582040S standalone CPU
- BMEH582040S Hot Standby CPU
- BMEH584040S Hot Standby CPU
- BMEH586040S Hot Standby CPU
- BMEP58CPROS3 co-processor
- BMXSAI0410 analog input module
- BMXSDI1602 digital input module
- BMXSDO0802 digital output module
- BMXSRA0405 digital relay output module
- BMXCPS4002S power supply
- BMXCPS4022S power supply
- BMXCPS3522S power supply

NOTE: In addition to the safety modules listed above, you can also include non-interfering, non-safety modules *(see page 16)* in your safety project.

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.

Replacing a CPU

It is possible to replace a BME•58•040S CPU with another BME•58•040S. However, the replacement does not work if the following limitations are exceeded :

- number of I/O
- number of I/O drops
- number of variables
- application memory size

Refer to the topics:

- *Configuration Compatibility (see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)* in the *Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures* for a description of Control Expert applications that are compatible with safety and Hot Standby CPUs.
- *M580 CPU & Copro Performance Characteristic*s *(see page 48)* in the *Modicon M580 Safety System Planning Guide* for a description of CPU limitations.

Non-Interfering Modules

Introduction

An M580 safety project can include both safety modules and non-safety modules. You can use non-safety modules only for non-safe tasks. Only non-safety modules that do not interfere with the safety function can be added to a safety project.

Definition of a Non-Interfering Module

⚠ CAUTION

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.

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

A non-interfering module is a module which cannot interfere with the safety function. For in-rack M580 modules (BMEx, BMXx, PMXx, and PMEx), there are two types of non-interfering modules:

- **Type 1**: A type 1 module can be installed in the same rack as safety modules (wherever the safety module is placed, in the main or extension rack).
- **Type 2**: A type 2 non-interfering module cannot be installed in the same main rack as safety modules (wherever the safety module is placed, in the main or extension rack).

NOTE: Type 1 and Type 2 modules are listed on TÜV Rheinland website at https://fs-products.tuvasi.com.
For not in-rack Mx80 modules, all Ethernet equipment (DIO or DRS) can be considered as non-interfering, and therefore can be used as part of an M580 safety system.

Type 1 Non-Interfering Modules for SIL3 Applications

The following non-safety modules can qualify as type-1 non-interfering modules in an M580 safety system.

NOTE: The list of type-1 non-interfering non-safety modules may change from time to time. For the current list, visit the TÜV Rheinland website at https://fs-products.tuvasi.com.

Module type	Module Reference
Backplane 4 slots	BMEXBP0400
Backplane 8 slots	BMEXBP0800
Backplane 12 slots	BMEXBP1200
Backplane 4 slots	BMXXBP0400
Backplane 6 slots	BMXXBP0600

Module type	Module Reference
Backplane 8 slots	BMXXBP0800
Backplane 12 slots	BMXXBP1200
Backplane 6 slots with dual slots for redundant power supplies	BMEXBP0602
Backplane 10 slots with dual slots for redundant power supplies	BMEXBP1002
Communication: Performance X80 Ethernet Drop Adapter 1 CH	BMXCRA31210
Communication: Performance X80 Ethernet Drop Adapter 1 CH	BMECRA31210
Communication: Ethernet module with standard web services	BMENOC0301
Communication: Ethernet module with IP Forwarding	BMENOC0321
Communication: Ethernet module with FactoryCast web services	BMENOC0311
Communication: Rack extender module	BMXXBE1000
Communication: AS-Interface	BMXEIA0100
Communication: Global Data	BMXNGD0100
Communication: Fiber Converter MM/LC 2CH 100Mb	BMXNRP0200
Communication: Fiber Converter SM/LC 2CH 100Mb	BMXNRP0201
Communication: M580 IEC 61850 Communication module	BMENOP0300
Counting: SSI module 3 CH	BMXEAE0300
Counting: High speed counter 2 CH	BMXEHC0200
Counting: High speed counter 8 CH	BMXEHC0800
Motion: Pulse Train Output 2 independent CH	BMXMSP0200
Analog: Ana 8 In Current Isolated HART	BMEAHI0812
Analog: Ana 4 Out Current Isolated HART	BMEAH00412
Analog: Ana 4 U/I In Isolated High Speed	BMXAMI0410
Analog: Ana 4 U/I In Non Isolated High Speed	BMXAMI0800
Analog: Ana 8 U/I In Isolated High Speed	BMXAMI0810
Analog: Ana 4 In U/I 4 Out U/I	BMXAMM0600
Analog: Ana 2 U/I Out Isolated	BMXAMO0210
Analog: Ana 4 U/I Out Isolated	BMXAMO0410
Analog: Ana 8 Out Current No Isolated	BMXAMO0802
Analog: Ana 4 TC/RTD Isolated In	BMXART0414.2
Analog: Ana 8 TC/RTD Isolated In	BMXART0814.2
Discrete: Dig 8 In 220 Vac	BMXDAI0805
Discrete: Dig 8 In 100 to 120 Vac Isolated	BMXDAI0814
Discrete: Dig 16 In 24Vac/24Vdc Source	BMXDAI1602
Discrete: Dig 16 In 48Vac	BMXDAI1603

Module type	Module Reference
Discrete: Dig 16 In 100 to 120 Vac 20 pin	BMXDAI1604
Discrete: Dig 16 Supervised inputs channels 100 to 120 Vac 40 pin	BMXDAI1614
Discrete: Dig 16 Supervised inputs channels 200 to 240 Vac 40 pin	BMXDAI1615
Discrete: Dig 16 Outputs Triacs 100 to 240 Vac 20 pin	BMXDAO1605
Discrete: Dig 16 Outputs Triacs 24 to 240 Vac 40 pin	BMXDAO1615
Discrete: Dig 16 In 24Vdc Sink	BMXDDI1602
Discrete: Dig 16 In 48Vdc Sink	BMXDDI1603
Discrete: Dig 16 In 125Vdc Sink	BMXDDI1604
Discrete: Dig 32 In 24Vdc Sink	BMXDDI3202K
Discrete: Dig 64 In 24Vdc Sink	BMXDDI6402K
Discrete: Dig 8 In 24Vdc 8Q Source Tr	BMXDDM16022
Discrete: Dig 8 In 24Vdc 8Q Relays	BMXDDM16025
Discrete: Dig 16 In 24Vdc 16Q Source Tr	BMXDDM3202K
Discrete: Dig 16Q Trans Source 0.5A	BMXDDO1602
Discrete: Dig 16 O Trans Sink	BMXDDO1612
Discrete: Dig 32Q Trans Source 0.1A	BMXDDO3202K
Discrete: Dig 64Q Trans Source 0.1A	BMXDDO6402K
Discrete: Dig 8Q 125Vdc	BMXDRA0804T
Discrete: Dig 8Q 24 Vdc or 24 to 240 Vac Isolated Relays	BMXDRA0805
Discrete: Dig 16 non-isolated relay output channels 5 to 125 Vdc or 25 to 240 Vac	BMXDRA0815
Discrete: Dig 16Q Relays	BMXDRA1605
Discrete: Dig NC Output 5 to 125 Vdc or 24 to 240 Vac Relays	BMXDRC0805
Discrete: Dig 16In 24/125Vdc TSTAMP	BMXERT1604
Mx80 Network Option Switch	BMENOS0300
Turbomachinery Frequency Input 2 CH	BMXETM0200

Type 2 Non-Interfering Modules for SIL2/3 Applications

The following in-rack non-safety modules can be considered to be type-2 non-interfering modules in an M580 safety system.

NOTE: The list of type-2 non-interfering non-safety modules may change from time to time. For the current list, visit the TÜV Rheinland website at https://fs-products.tuvasi.com.

Module type	Module Reference
Communication: Standard X80 Ethernet Drop Adapter 1 CH	BMXCRA31200
Standard AC power supply	BMXCPS2000
Standard Isolated DC power supply	BMXCPS2010
High Power Isolated 24 to 48 VDC power supply	BMXCPS3020
Standard Redundant 125VDC power supply	BMXCPS3522
Standard Redundant 24048VDC power supply	BMXCPS4022
Standard Redundant AC power supply	BMXCPS4002
High Power AC power supply	BMXCPS3500
High Power DC power supply	BMXCPS3540T
Communication: Bus module 2 RS485/232 Port	BMXNOM0200
CANopen X80 Master	BMECXM0100
Weight module	PMESWT0100
Profibus DP/DPV1 Master module support	PMEPXM0100
Partner diagnostic module	PMXCDA0400

NOTE: All authorized equipment of an M580 system that are linked to safety modules via Ethernet are considered as non-interfering. As a consequence, all modules from Quantum and STB Advantys ranges (not pluggable in the same rack as M580 safety modules) are Type 2 non-interfering modules.

Chapter 2
Selecting an M580 Safety System Topology

Introduction

This chapter describes the topologies supported by an M580 safety system.

What Is in This Chapter?

This chapter contains the following topics:

Designing an M580 Safety System Topology

Support for Standalone PACs

An M580 safety system supports only SIL3 applications for standalone PACs. A standalone PAC includes a single CPU with coprocessor.

NOTE: For a description of available racks and their permitted usage refer to the topic *Rack Usage (see page 83)*.

Placing Safety Modules in the RIO Main Ring

Install M580 safety modules only in the RIO main ring, which includes:

- The local main rack. Standalone safety PACs can also include up to seven optional local extended racks.
  - The local main rack must include a safety power supply, a safety CPU, and a safety coprocessor.
  - For a standalone safety PAC, the local main rack and the local extended racks may also include safety I/O. An M580 Hot Standby PAC does not support I/O on the local main rack, or local extended racks.

  NOTE: The maximum distance between the main rack and the last extended rack is 30 m.
- Up to 31 RIO drops for the BMEH586040S Hot Standby CPU (16 RIO drops for the BME•584040S CPU; 8 RIO drops for the BME•582040S CPU), each consisting of a remote main rack and an optional remote extended rack.

Any rack with safety modules also requires a safety power supply.

NOTE: A rack that includes safety modules may also include type 1 non-interfering modules *(see page 16)*. However, type 2 non-interfering modules *(see page 19)* may not be placed on the same rack as safety modules. Type 2 non-interfering modules may be placed on racks without safety modules–for example, in racks of distributed equipment. Other non-safe modules may not be included in an M580 safety system.

Extending a Main Rack

Use BMXXBE1000 rack extender modules to daisy chain together main and extended racks. Connect each pair of extender modules using BMXXBC•••K connector cables, and terminate each end of the chain with TSXELYEX line terminators.

Local Rack Communications with an RIO Drop

To support RIO drops in an M580 safety system, configure the M580 safety CPU as an NTP server, or as an NTP client (with another device configured as an NTP server). Without a properly set up clock (NTP), safety I/O communication may not operate correctly.

Use a BM•CRA312•0 remote adapter module (a BM•CRA31200 for a remote rack hosting Non Interfering only modules, and a BM•CRA31210 adapter for remote rack hosting both non-interfering and/or safety I/O modules to connect the RIO drop to the RIO main ring. Connect each end of the RIO main ring to the two dual ports on the BME•58•040S safety CPU.

If the connection is made via Cat5e copper cable, the maximum distance between drops is 100 m.

NOTE: Alternatively, you can connect the local main rack to the BM•CRA312•0 remote adapter in the RIO drop by placing a BMXNRP020• fiber optic repeater module into each rack. Refer to the topic *Using Fiber Converter Modules (see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures)* in the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures* for additional information.

Connecting Two M580 Safety PACs

A M580 safety system also supports peer-to-peer black channel communication between two safety PACs. Typically, this connection is made via a BMENOC0321 in each safety system. Refer to the peer-to-peer communications *(see Modicon M580, Safety Manual)* topic in the *Modicon M580 Safety Manual* for more information.

NOTE: To support black channel communications between two PACs, enable the NTP service in both PACs. You can configure one PAC as the NTP server, and the other as the NTP client. Alternatively, you can configure each PAC as an NTP client, with another device configured as NTP server.

Adding Distributed Equipment to an M580 Safety System

You can include distributed equipment in your M580 safety system. Typically, distributed equipment is connected as either non-looping daisy chain, or a daisy chain loop.

You can connect a distributed equipment daisy chain loop to the two network ports of one of the following modules on the RIO main ring:

- a BMENOC0301/11 Ethernet communications module.
- a BMENOS0300 Ethernet network option switch.
- a ConneXium dual ring switch.

You can also use the service port of a BMENOC0301/11 Ethernet communications module, a BMENOS0300 Ethernet network option switch or the BME•58•040S safety CPU to connect distributed equipment in the shape of a non-looping daisy chain.

NOTE: Place only type 1 and type 2 non-interfering modules in a distributed equipment network. Place safety modules only in the local rack (main or extended) and the RIO network. Exclude non-safe modules that are not type 1 or type 2 non-interfering modules from your safety project.

Refer to the topic *Selecting the Correct Topology (see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures)* in the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures* for additional information on connecting distributed equipment to an M580 CPU.

Adding CIP Safety Equipment to the M580 Safety System

You can include CIP Safety I/O (CSIO) devices in your M580 safety system as CSIO distributed equipment.

You can connect CSIO distributed equipment to the RIO main ring through:

- the service port of a CPU or a BM•CRA31210 X80 EIO adapter module.
- a BMENOS0300 Ethernet network option switch.
- a ConneXium Dual Ring Switch (DRS).

Each type of I/O (CSIO, RIO, DIO) has its own limitation. To maintain an acceptable level of performance, it is recommended not to use the maximum of all I/O types in the same architecture.

It is recommended that a typical M580 CIP Safety architecture is based on a remote or distributed topology. Recommended limitations are listed in table below:

	BMEP582040S			BMEP584040S		
	CSIO Devices	DIO Devices	RIO Drops	CSIO Devices	DIO Devices	RIO Drops
Recommended Remote Max Topology	10	10	8	32	10	16
Recommended Distributed Max Topology	16	61	2	64	61	2

The CSIO time contribution to the SAFE task is roughly 100 µs/equipment with a BMEP584040S CPU and 400 µs/equipment with a BMEP582040S CPU.

M580 Safety Topologies

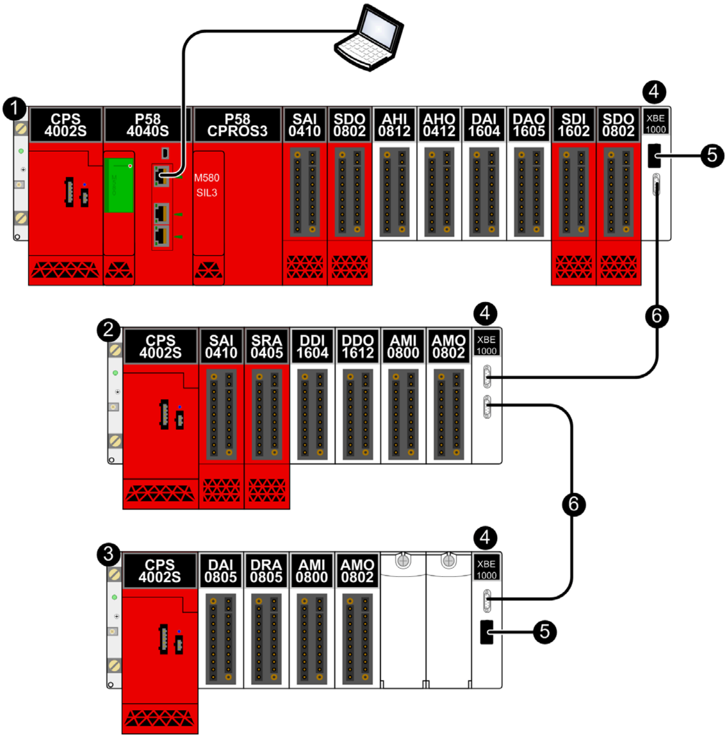
Introduction

The following diagrams present examples of M580 safety topologies. This collection of sample topologies does not include every potential topology supported by an M580 safety system.

Refer to the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures* and the *Modicon M580 System Planning Guide for Complex Topologies* for additional information on how to set up an M580 topology.

Extending the Local Main Rack

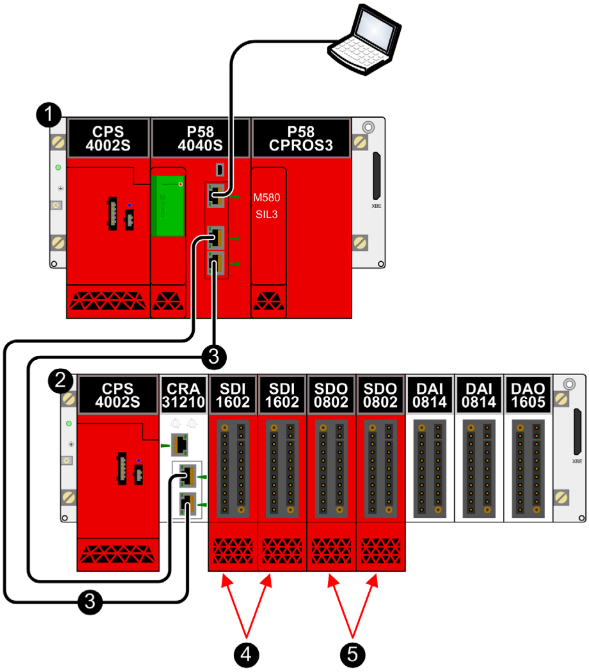
The following diagram presents a local main rack, with two extended racks. Note that the M580 safety system supports a single local main rack plus up to seven extended racks over a maximum length of 30 m:



1 Local main rack with safety and type 1 non-interfering modules
2 Local extended rack with safety and type 1 non-interfering modules
3 Local extended rack with type 1 and type 2 non-interfering modules
4 BMXXBE1000 rack extender modules
5 TSXELYEX line terminators
6 BMXXBC•••K connector cables

High Availability I/O Topologies

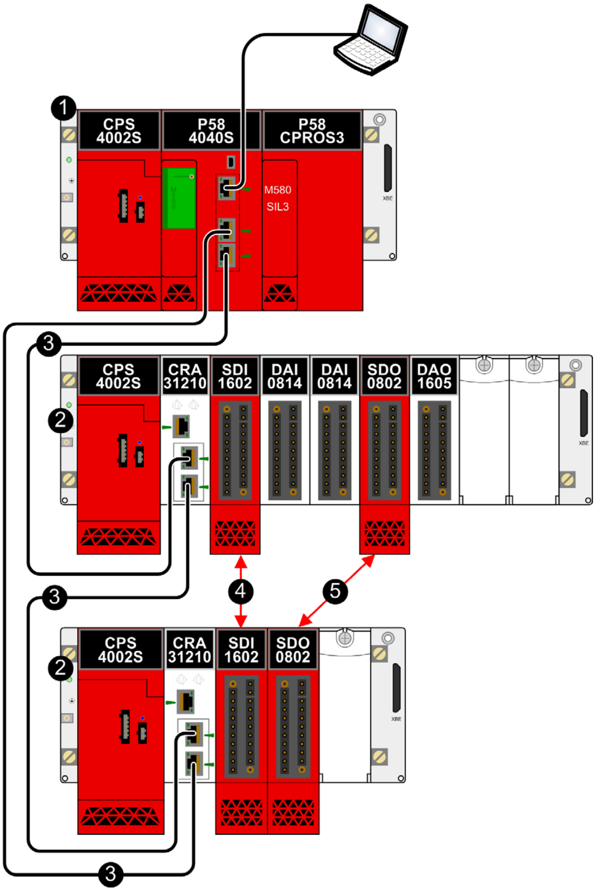
The following diagram presents an example of redundant I/O placed in the same RIO drop:



1 Local main rack
2 RIO drop
3 RIO main ring
4 Two redundant input modules in the same RIO drop
5 Two redundant output modules in the same RIO drop

NOTE: Enable the NTP service for the M580 safety PAC to support black channel communication between the local main rack and RIO drops on the RIO main ring, and configure the time inside the PAC if the PAC is to be the NTP server. The safety PAC can be either the NTP server, or the NTP client (with another device configured as the NTP server).

The following diagram presents an example of placing redundant I/O in two separate RIO drops:



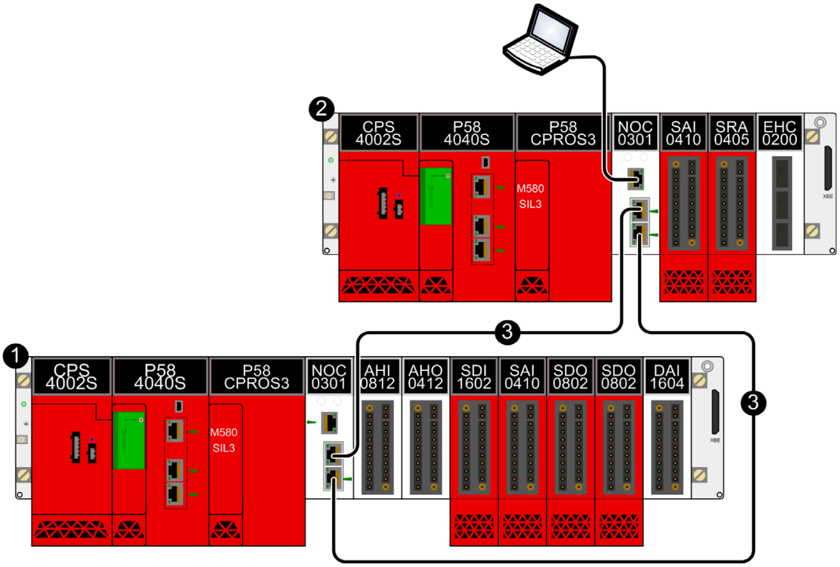
1 Local main rack
2 RIO drop
3 RIO main ring
4 Two redundant input modules in separate RIO drops
5 Two redundant output modules in separate RIO drops

NOTE:

- Schneider Electric recommends placing redundant safety I/O modules in separate RIO drops.
- Enable the NTP service for the M580 safety PAC to support black channel communication between the local main rack and RIO drops on the RIO main ring. The safety PAC can be either the NTP server, or the NTP client (with another device configured as the NTP server).

Peer-to-Peer Topology for Two Standalone Safety PACs

The following diagram presents an example of how to connect two separate M580 safety PACs. In this example, a sensor linked to a safety input module in PAC 1 can be configured to cause a response by an actuator linked to a safety output module in PAC 2:



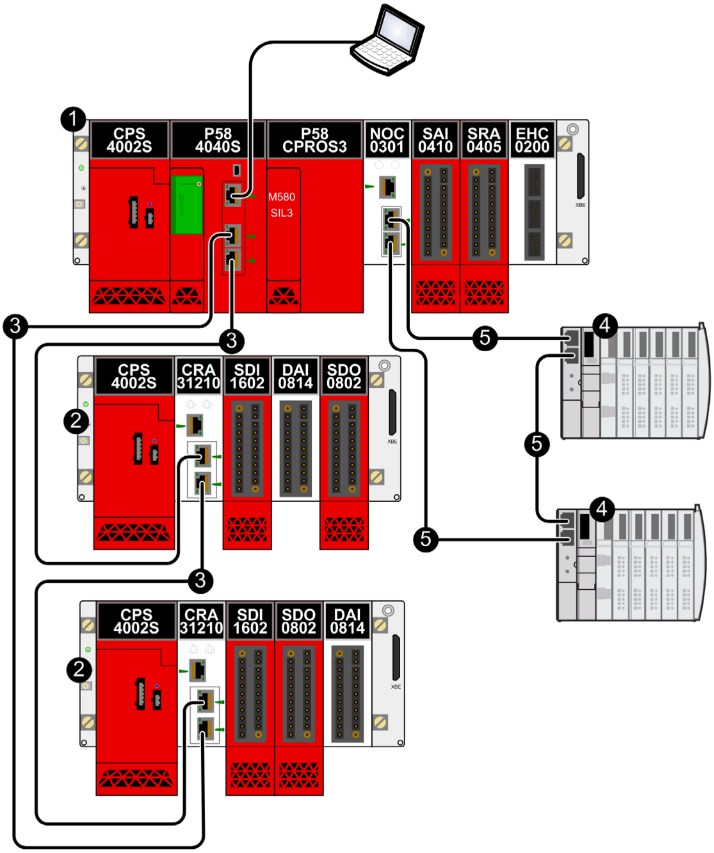
1 Standalone M580 safety PAC 1
2 M580 safety PAC 2
3 Black channel communication between PACs

NOTE: To support black channel communications between the two PACs, enable the NTP service in both PACs. You can configure one PAC as the NTP server, and the other as the NTP client. Alternatively, you can configure each PAC as an NTP client, with another device configured as NTP server.

Adding Distributed Equipment to the M580 Safety PAC

You can add type 1 and type 2 non-interfering modules to your M580 safety project as distributed equipment, in either a non-looping daisy chain or a daisy chain loop design.

The following diagram depicts an example of distributed equipment added as a non-looping daisy chain. In this example, the distributed equipment daisy chain connects to the PAC via the ETH2 and ETH3 EIO ports of a BMENOC0301/11 Ethernet communications module:



1 Local main rack with Ethernet backplane
2 RIO drop with safety modules and type 1 non-interfering modules
3 RIO main ring
4 Distributed equipment
5 Ring of distributed equipment

Chapter 3
M580 Safety CPU and Coprocessor

Introduction

This chapter describes the BME•58•040S CPUs and the BMEP58CPROS3 Coprocessor (Copro).

What Is in This Chapter?

This chapter contains the following sections:

Section 3.1
M580 Safety CPU & Coprocessor Physical Features

Introduction

This section describes the physical common features of the BME•58•040S CPUs and the BMEP58CPROS3 coprocessor (Copro).

What Is in This Section?

This section contains the following topics:

Physical Description of the M580 Safety CPU & Coprocessor

Position on the Local Rack

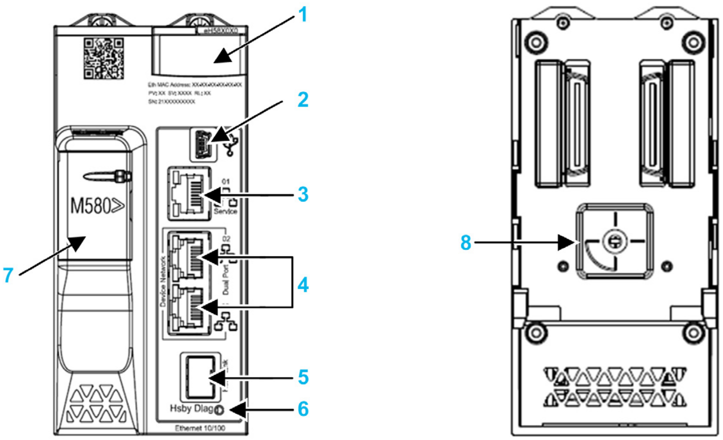
Every M580 standalone SIL3 safety system requires one BME•58•040S CPU and one BMEP58CPROS3 coprocessor (Copro). The CPU requires two module slots and is placed in slots 0 and 1 immediately to the right of the power supply in the main local rack. The Copro also requires two module slots and is placed in slots 2 and 3 immediately to the right of the CPU. Both the CPU nor the Copro cannot be placed into any other slot locations or on any other rack. If there are extended racks in the local rack configuration, assign address 00 to the rack with the CPU and Copro.

NOTE: Both the safety CPU and the Copro can be installed only on a BMEXBP•••• Ethernet rack. For a description of available M580 racks refer to the topic *Local and Remote Racks* in the *Modicon M580 Hardware Reference Manual*.

CPU Front Panel

BME•58•040S safety CPU supports both RIO and DIO scanning.

CPU Physical features:



Legend:

Item	Marking	Description
1	–	LED display *(see page 38)* for CPU status and diagnostics.
2		Mini-B USB connector *(see page 43)* to which you can attach a PC running Control Expert or Unity Loader, or an HMI.
3	Service	RJ45 Ethernet connector *(see page 40)* for the service port.

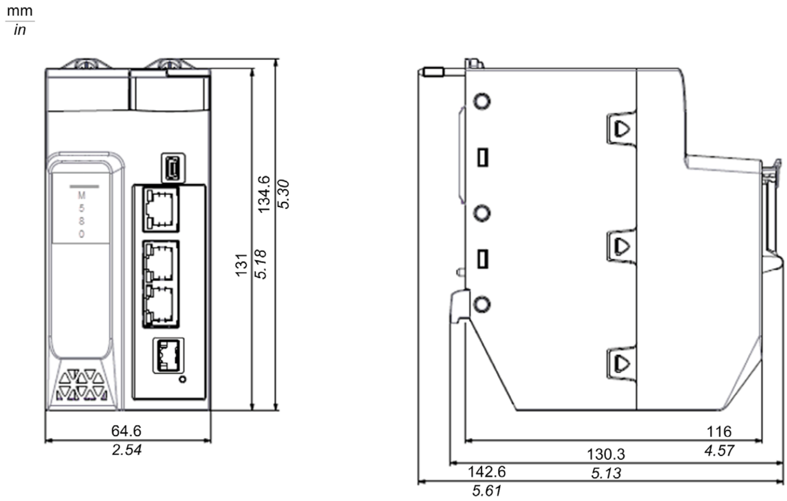
Item	Marking	Description
4	**Dual Port**	Dual RJ45 Ethernet connectors *(see page 40)* that support distributed equipment and RIO drops.
5	**Dual Port**	SFP socket for copper or fiber-optic redundant link connection.
6	—	Redundant link status LED.
7	—	SD memory card *(see page 46)* slot.
8	—	A/B/Clear rotary selector switch, used to designate a Hot Standby PAC as either PAC A or PAC B, or to clear the existing Control Expert application.

Coprocessor Front Panel

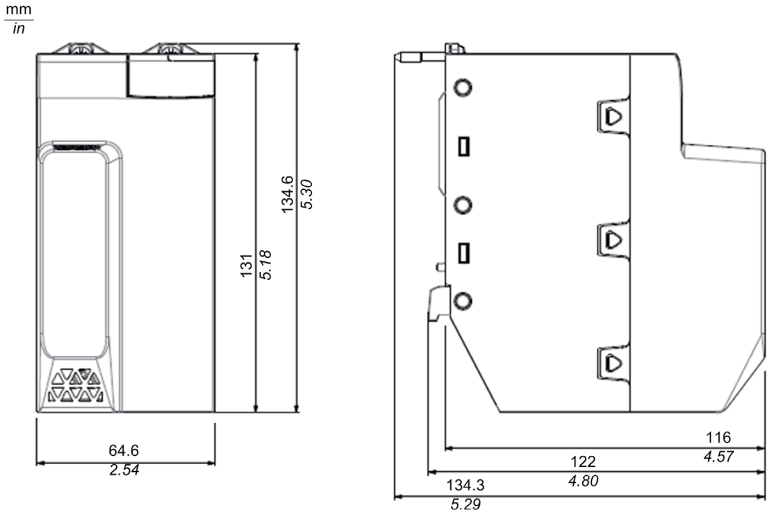
The BMEP58CPROS3 Coprocessor presents only an LED display on its front face.

CPU & Copro Dimensions

The BME•58•040S safety CPUs present the following physical dimensions:



The BMEP58CPROS3 Copro presents the following physical dimensions. Unlike the CPU, the Copro does not present physical connectors or related labels



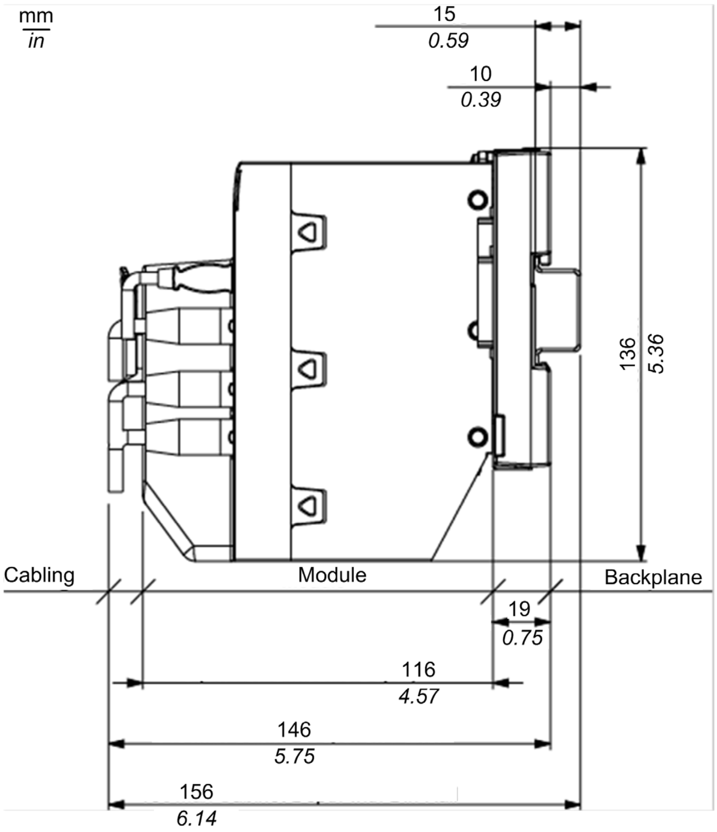
NOTE:

Consider the height of the CPU and Copro when you are planning the installation of the local rack. Both the CPU and Copro extend below the lower edge of the rack by:

- 29.49 mm (1.161 in.) for an Ethernet rack
- 30.9 mm (1.217 in.) for an X Bus rack

CPU Wiring Dimensions

The BME•58•040S safety CPUs present the following dimensions when mounted on a DIN rail with cabling:

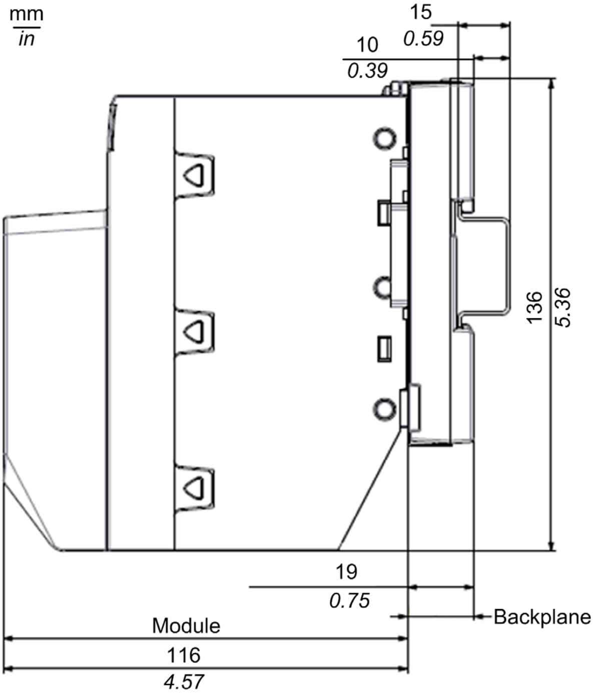


Overall depth for the CPU is:

- 146 mm with cabling
- 156 mm with cabling plus DIN rail

Copro Wiring Dimensions

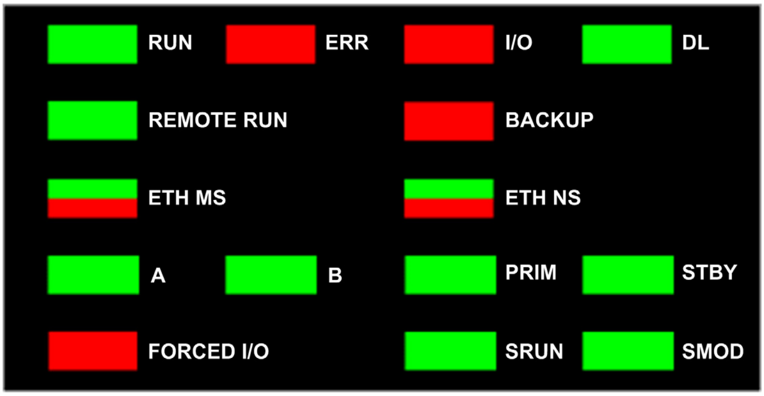
The BMEP58CPROS3 Copro presents the following dimensions when mounted on a DIN rail:



LED Displays for the M580 Safety CPU and Copro

CPU LED Display

A 10-LED display is located on the front panel of the CPU:



NOTE: The Copro LED display is a sub-set of the CPU display, and includes the following LEDs:

- ERR
- DL
- SRUN
- SMOD

LED Descriptions

NOTE: Refer to the topics:

- *M580 Safety CPU LED Diagnostics (see Modicon M580, Safety Manual)* and *M580 Coprocessor LED Diagnostics (see Modicon M580, Safety Manual)* in the *Modicon M580 Safety Manual* for information on how to use the CPU and Copro LEDs to diagnose the state of the safety PAC.
- *LED Diagnostics for M580 Hot Standby CPUs (see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)* in the *Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures* for information on how to use the **A**, **B**, **PRIM**, **STBY**, and **REMOTE RUN** Hot Standby CPU LEDs.

LED Indicator	Applies to...		Description
	CPU	Copro	
RUN	✓	–	**ON**: The CPU is managing its outputs, and at least one task is in the RUN state.
ERR	✓	✓	**ON**: The CPU has detected an internal CPU error (for example, no configuration, detected watchdog error, detected self test error.)
I/O	✓	–	**ON**: The CPU has detected an error, external to the CPU, in one or more I/O modules.
DL (*download*)	✓	+	● **ON**: A firmware upgrade to the CPU, Copro, backplane or other in-rack module is in progress. ● **OFF**: No firmware upgrade in progress.
BACKUP	✓	–	**ON**: ● The memory card or CPU flash memory is missing or inoperable. ● The memory card is not usable (bad format, unrecognized type). ● The memory card or CPU flash memory content is inconsistent with the current application. ● The memory card has been removed and reinserted. ● A **PLC** → **Project Backup...** → **Backup Clear** command has been performed when no memory card is present. The **BACKUP** LED remains **ON** until the project is successfully backed up.
			OFF: The memory card or CPU flash memory content is valid, and the application in the execution memory is identical.
ETH MS	✓	–	MOD STATUS (green/red): Pattern indicates the Ethernet port configuration status. **NOTE:** With the detection of a recoverable error, the **ETH MS** LED can be green or red and on or off.
ETH NS	✓	–	NET STATUS (green/red): Pattern indicates the Ethernet connection status.
FORCED I/O	✓	–	**ON**: At least one input or output on a digital I/O module is forced.
SRUN	✓	✓	**ON**: The PAC is managing its safety outputs, and the SAFE task is in the RUN state.
SMOD	✓	✓	● **ON**: The PAC is operating in safety mode *(see page 112)*. ● **FLASHING**: The PAC is operating in maintenance mode *(see page 113)*.
✓: Applies – : Does not apply.			

Ethernet Ports

Introduction

There are three RJ45 Ethernet ports on the front of the CPU: one service port, and two device network ports. The ports share the characteristics described below.

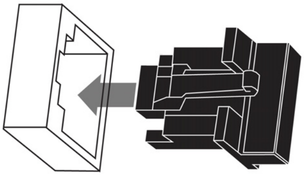
Common Characteristics

All three ports have the same RJ45 connector and all use the same type of Ethernet cables.

NOTE: The three Ethernet ports are connected to chassis ground, and the system requires an equipotential ground.

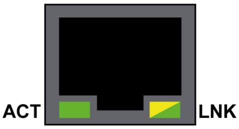
Dust Cover

To keep dust from entering the unused Ethernet ports, cover the unused ports with the stopper:

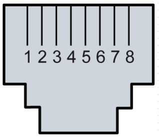


Ethernet Ports

Each RJ45 connector has a pair of LED indicators:



The pin positions, pinouts, and cable connections are the same on all three RJ45 Ethernet ports:

Pin	Description	
1	TD+	Pinout: 
2	TD-	
3	RD+	
4	not connected	
5	not connected	
6	RD-	
7	not connected	
8	not connected	
—	shell/chassis ground	

NOTE: The TD pins (1 and 2) and the RD pins (3 and 6) are auto-MDIX enabled and automatically reverse their roles depending on the connected media (i.e., straight or crossed cables).

The ports have an auto MDIX capability that automatically detects the direction of the transmission.

Choose from these Ethernet cables to connect to the Ethernet ports:

- TCSECN3M3M••••: Cat 5E Ethernet straight-through shielded cable, rated for industrial use, CE- or UL-compliant
- TCSECE3M3M••••: Cat 5E Ethernet straight-through shielded cable, rated for industrial use, CE-compliant
- TCSECU3M3M••••: Cat 5E Ethernet straight-through shielded cable, rated for industrial use, UL-compliant

The maximum length for a copper cable is 100 m. For distances greater than 100 m, use fiber optic cable. The CPU does not have any fiber ports on it. You may use dual ring switches or BMX NRP •••• fiber converter modules *(see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures)* to handle the copper-fiber conversion.

Ethernet Ports on Standalone CPUs

On standalone CPUs, the **ACTIVE** LED is green. The **LNK** LED is either green or yellow, depending on the status:

LED	LED Status	Description
ACTIVE	OFF	No activity is indicated on the Ethernet connection.
	ON / blinking	Data is being transmitted and received on the Ethernet connection.
LNK	OFF	No link is established at this connection.
	ON green	A 100 Mbps link* is established at this connection.
	ON yellow	A 10 Mbps link* is established at this connection.
* The 10/100 Mbps links support both half-duplex and full-duplex data transfer and autonegotiation.		

Service Port

The service port is the uppermost of the three Ethernet ports on the front panel of the CPU. This port can be used:

- To provide an access point that other devices or systems can use to monitor or communicate with the M580 CPU.
- As a standalone DIO port that can support a star, or daisy chain topology of distributed equipment.
- To mirror the CPU ports for Ethernet diagnostics. The service tool that views activity on the mirrored port may be a PC or an HMI device.

NOTE: Use only the device network dual ports, and not the service port, to connect to the device network. Connecting the service port, either directly or through a switch/hub, to the device network may affect system performance.

NOTE: The service port may not provide full performance and features that the **Device Network** ports on the CPU provide.

Device Network Dual Ports

You may use a **Device Network** port to support a star or daisy chain topology of distributed equipment. You may use both **Device Network** ports to support a ring topology.

For details about distributed equipment architectures, refer to the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures*.

When used as RIO ports, both ports connect the CPU to the main ring in an Ethernet daisy-chain loop or ring.

For more information about RIO architectures, refer to the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures (see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures)*.

Grounding Considerations

Follow all local and national safety codes and standards.

⚠ ⚠ DANGER

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.

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

USB Port

Introduction

The USB port is a high-speed, mini-B USB connector, version 2.0 (480 Mbps) that can be used for a Control Expert program or human-machine interface (HMI) panel. The USB port can connect to another USB port, version 1.1 or later.

NOTE: Install M580 USB drivers before connecting the USB cable between the CPU and the PC.

Transparency

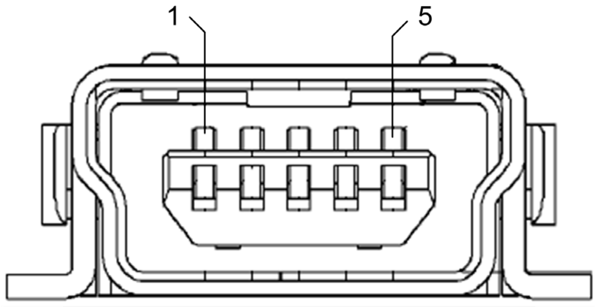
If your system requires transparency between the device connected to the USB port and the M580 device network, add a persistent static route in the device's routing table.

Example of a command to address a device network with IP address `X.X.0.0` (for a Windows PC): `route add X.X.0.0 mask 255.255.0.0 90.0.0.1 -p`

(In this case, `X.X.0.0` is the network address used by the M580 device network, and `255.255.0.0` is the corresponding subnet mask.)

Pin Assignments

The USB port has the following pin positions and pinouts:



Legend:

Pin	Description
1	VBus
2	D-
3	D+
4	not connected
5	ground
shell	chassis ground

Cables

Use a BMX XCA USB H018 (1.8 m/5.91 ft) or BMX XCA USB H045 (4.5 m/14.764 ft) cable to connect the panel to the CPU. (These cables have a type A connector on one side and the mini-B USB on the other side.)

In a fixed assembly with an XBT-type console connected to the CPU, connect the USB cable to a protection bar *(see Modicon X80, Racks and Power Supplies, Hardware Reference Manual)*. Use the exposed part of the shield or the metal lug on the BMX XCA cable to make the connection.

SFP Socket

Redundancy Link Port Connector

Each Hot Standby CPU module includes one SFP socket, to which you can connect either a fiber optic or a copper transceiver:

Refer to the *Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures* for information on installing and removing an SFP socket *(see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)*, and a list of available SFP transceivers *(see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)*.

SD Memory Card

BMXRMS004GPF SD Memory Card

The BMXRMS004GPF memory card is a 4 GB, Class A card rated for industrial use. The SD memory card slot resides behind the door on the front of the CPU.

You can use a BMXRMS004GPF memory card for application and data storage.

You can use a BMXRMS004GPF memory card for storage of:
- The M580 safety project application.
- Data for the non-safe tasks (MAST, FAST, AUX0, AUX1).

NOTE:
- Data cannot be stored on the SD memory card for the SAFE task.
- The SD memory card is not included in the safety loop.

You can insert and extract the card while power is ON and the PAC is in RUN mode. However, to avoid data losses, use system bit %S65 to make a system request to stop data access to the card before extracting it from the CPU.

NOTE:
Other memory cards, including those used in M340 CPUs, are not compatible with M580 CPUs. If you insert an incompatible SD memory card in the CPU:
- The CPU remains in NOCONF state *(see Modicon M580, Hardware, Reference Manual)*.
- The CPU **BACKUP** LED turns ON.
- The memory card access LED remains blinking.

The BMXRMS004GPF memory card is formatted specifically for the M580 CPUs. If you use this card with another CPU or tool, the card may not be recognized.

Memory Card Characteristics

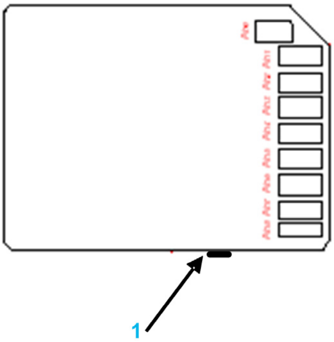
The BMXRMS004GPF memory card presents the following characteristics:

Characteristic	Value
global memory size	4 GB
application backup size	200 MB
data storage size	3.8 GB
write/erase cycles (typical)	100,000
operating temperature range	–40...+85 °C (–40...+185 °F)
file retention time	10 years
memory zone for FTP access	data storage directory only

NOTE: Due to formatting, wear-out, and other internal mechanisms, the actual available capacity of the memory card is slightly lower than its global size.

Read/Write Card Switch

The BMXRMS004GPF memory card has a read/write access switch along its non-beveled side edge, which you can use to help protect the card against non-permitted write access:



1 Read/write access switch

Formatting the Memory Card

The formatting procedure is described in *Formatting the Memory Card* topic in the *EcoStruxure™ Control Expert System Block Library (see EcoStruxure™ Control Expert, System, Block Library)*.

Section 3.2
M580 Safety CPU & Coprocessor Performance Characteristics

M580 CPU & Copro Performance Characteristics

Safety CPU & Copro

The BME•58•040S CPU and the BMEP58CPROS3 Coprocessor (Copro) provide the following performance characteristics in a SIL3 M580 safety solution:

Performance Feature		BME				
		P582040S	P584040S	H582040S	H584040S	H586040S
Local racks		4 (1 main rack + up to 3 extended racks)	8 (1 main rack + up to 7 extended racks)	1	1	1
RIO drops (max of 2 racks/drop: main rack + extended rack)		8 drops (up to 2 racks per drop)	16 drops (up to 2 racks per drop)	8 drops (up to 2 racks per drop)	16 drops (up to 2 racks per drop)	31 drops (up to 2 racks per drop)
I/O Channels	Discrete I/O	2048	4096	0[1]	0[1]	0[1]
	Analog I/O	512	1024	0[1]	0[1]	0[1]
	Expert	72	144	0[1]	0[1]	0[1]
Ethernet Ports	Backplane	1	1	1	1	1
	Service	1	1	1	1	1
	RIO	2	2	2	2	2

1. For M580 safety Hot Standby PACs, no I/O modules are supported in the local rack.
2. This data is included in both the safe and non-safe data areas.
3. Because the SAFE task exchanges data through backplane, there is a negative impact on performance. It takes 1ms to transfer 10KB for BMEH584040S and BMEH586040S and 2ms for BMEH582040S.
4. Application Program (non-safe) + Application Data (non-safe non-retain data only) + Application Program (safe) + Application Data (Safe) is less than 64Mbytes. There is a global memory pool of 64 Mbytes on BMEH586040S CPU for Application Program and Application Data.
5. Maximum of Transfer data (non safe + safe) for redundant data is 4MB.
6. 2 GB without an external memory card.

Performance Feature		BME				
		P582040S	P584040S	H582040S	H584040S	H586040S
Control network	Max # of modules/devices	64	128	64	128	128
	Max input capacity	16 KB	24 KB	16 KB	24 KB	24 KB
	Max output capacity	16 KB	24 KB	16 KB	24 KB	24 KB
	Max FAST input capacity	3 KB	5 KB	3 KB	5 KB	5 KB
	Max FAST output capacity	3 KB	5 KB	3 KB	5 KB	5 KB
Distributed equipment network	Max # of modules/devices	61	61	61	61	61
	Max input capacity	2 KB	8 KB	2 KB	2 KB	2 KB
	Max output capacity	2 KB	8 KB	2 KB	2 KB	2 KB
	Max CIP Safety devices	16	64	–	–	–
	Max CIP Safety connections	32	128	–	–	–
Ethernet comm modules on local rack	Max Eth Comm Modules	2	4	2	4	4
	Max BMENOC0301/0311	2	3	2	3	3
	Max BMENOC0321	2	2	2	2	2

1. For M580 safety Hot Standby PACs, no I/O modules are supported in the local rack.
2. This data is included in both the safe and non-safe data areas.
3. Because the SAFE task exchanges data through backplane, there is a negative impact on performance. It takes 1ms to transfer 10KB for BMEH584040S and BMEH586040S and 2ms for BMEH582040S.
4. Application Program (non-safe) + Application Data (non-safe non-retain data only) + Application Program (safe) + Application Data (Safe) is less than 64Mbytes. There is a global memory pool of 64 Mbytes on BMEH586040S CPU for Application Program and Application Data.
5. Maximum of Transfer data (non safe + safe) for redundant data is 4MB.
6. 2 GB without an external memory card.

Performance Feature			BME				
			P582040S	P584040S	H582040S	H584040S	H586040S
Memory allocation (max)	Non-safe application program		8 MB	16 MB	8 MB	16 MB	64 MB[4]
	Safe application program		2 MB	4 MB	2 MB	4 MB	16 MB[4]
	Non-safe data		768 KB	2048 KB	768 KB	2048 KB	up to 65536 KB[4]
		Max configurable retained data	768 KB	2048 KB	768 KB	2048 KB	4096 KB
		Max configurable redundant transfer data	768 KB	2048 KB	768 KB	2048 KB	4096 KB[5]
	Safe data (non-retained data)		512 KB	1024 KB	512 KB	1024 KB	1024 KB[4]
		Max configurable safe redundant transfer data	512 KB	1024 KB	512 KB	1024 KB	1024 KB[5]
	Shared: Global -> Safe		16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Shared: Safe -> Global		16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Shared: Global -> Process		16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Shared: Process -> Global		16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Total Data Storage		4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]

[1] For M580 safety Hot Standby PACs, no I/O modules are supported in the local rack.

[2] This data is included in both the safe and non-safe data areas.

[3] Because the SAFE task exchanges data through backplane, there is a negative impact on performance. It takes 1ms to transfer 10KB for BMEH584040S and BMEH586040S and 2ms for BMEH582040S.

[4] Application Program (non-safe) + Application Data (non-safe non-retain data only) + Application Program (safe) + Application Data (Safe) is less than 64Mbytes. There is a global memory pool of 64 Mbytes on BMEH586040S CPU for Application Program and Application Data.

[5] Maximum of Transfer data (non safe + safe) for redundant data is 4MB.

[6] 2 GB without an external memory card.

Performance Feature			BME				
			P582040S	P584040S	H582040S	H584040S	H586040S
Instruction execution rate	MAST and FAST tasks:						
		Boolean	10K instructions / ms	40K instructions / ms	10K instructions / ms	40K instructions / ms	60K instructions / ms
		Typed	7.5K instructions / ms	30K instructions / ms	7.5K instructions / ms	30K instructions / ms	40K instructions / ms
	SAFE task:						
		Boolean	10K instructions / ms	40K instructions / ms	10K instructions / ms[3]	40K instructions / ms[3]	40K instructions / ms[3]
		Typed	7.5K instructions / ms	30K instructions / ms	7.5K instructions / ms[3]	30K instructions / ms[3]	30K instructions / ms[3]
Open field bus			–	–	0	0	0
Sensor Bus (AS-i)			–	–	16	16	16

1. For M580 safety Hot Standby PACs, no I/O modules are supported in the local rack.
2. This data is included in both the safe and non-safe data areas.
3. Because the SAFE task exchanges data through backplane, there is a negative impact on performance. It takes 1ms to transfer 10KB for BMEH584040S and BMEH586040S and 2ms for BMEH582040S.
4. Application Program (non-safe) + Application Data (non-safe non-retain data only) + Application Program (safe) + Application Data (Safe) is less than 64Mbytes. There is a global memory pool of 64 Mbytes on BMEH586040S CPU for Application Program and Application Data.
5. Maximum of Transfer data (non safe + safe) for redundant data is 4MB.
6. 2 GB without an external memory card.

Chapter 4
M580 Safety Power Supplies

Introduction

This chapter describes the M580 safety power supplies.

What Is in This Chapter?

This chapter contains the following topics:

Physical Description of the M580 Safety Power Supplies

Use in M580 Safety Loop

Use only a BMXCPS4002S, BMXCPS4022S, or BMXCPS3522S safety power supply in an rack that contains safety modules. You can use the safety power supply in an X Bus or Ethernet rack that is:

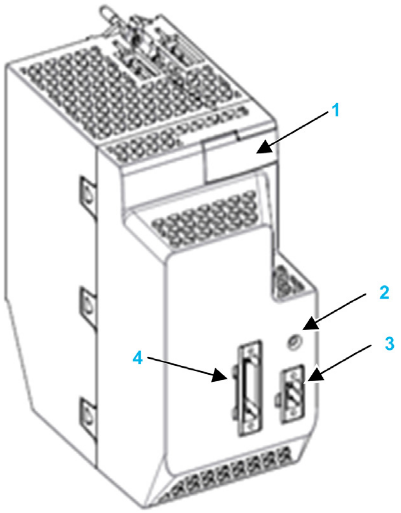
- a main local rack
- an extended local rack
- a main remote rack
- an extended remote rack

You can use two safety power supply modules in Ethernet racks that support redundancy. The safety power supply requires two module slots and is placed in the left-most position in the rack.

NOTE: For a description of available M580 racks refer to the topic *Local and Remote Racks* in the *Modicon M580 Hardware Reference Manual*.

Power Supply Front Panel

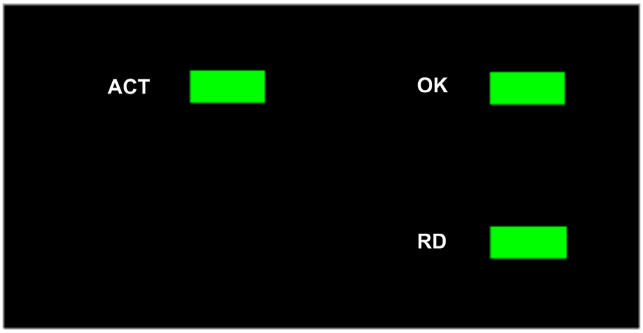
The M580 safety power supplies present the following front panel:



1 LED display panel
2 RESET button
3 Alarm relay contact
4 100...240 Vac main input power supply 5-pin connector

LED Array

The M580 safety power supply modules present the following LED panel:



The LED panel includes the following LED indicators:

- **OK**: Operating Status
- **ACT**: Activity
- **RD**: Redundancy

Each LED has two states: ON (green) and OFF.

Refer to the topic *Power Supply LED Diagnostics (see Modicon M580, Safety Manual)* in the *M580 Safety Manual* for information on how to use these LEDs to diagnose the state of the power supply.

RESET

Pressing the **RESET** button on the power supply causes re-initialization of all modules in same rack as the power supply. If the M580 safety power supply module is in the main local rack, pressing the **RESET** button causes re-initialization of the CPU.

NOTE: In a redundant design, with two M580 safety power supply modules, you can press the RESET button on either, or both, power supply modules to execute the reset function.

Input Power Supply Connections

For each M580 safety power supply, the following pin characteristics apply:

- 5 points
- Removable plug type:
  - on the module: header with threaded flange
  - plug terminal block with screw flange
- Pitch: 5.08 mm
- Minimum wire capability: 0.5 mm^2...2.0 mm^2

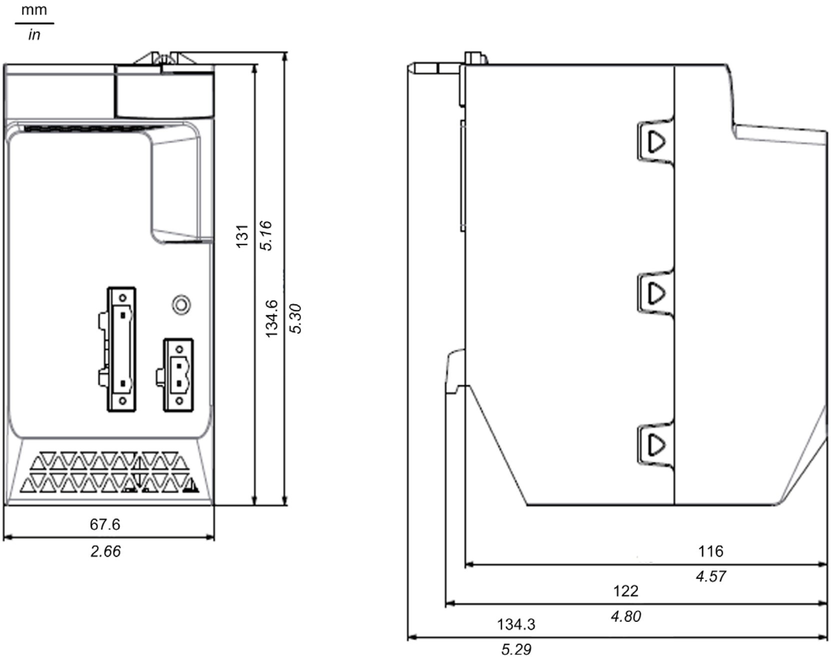
The input power and pin assignments for each M580 safety power supply are as follows:

Description	BMXCPS4002S	BMXCPS4022S	BMXCPS3522S
Main Input Power	100...240 Vac	24...48 Vdc	125 Vdc
Pin 1	NC	DC Line	NC
Pin 2	NC	DC Line	NC
Pin 3	PE	DC Neutral	PE
Pin 4	AC Neutral	DC Neutral	DC Neutral
Pin 5	AC Line	Earth	DC Line

NOTE: A plug terminal block is provided with the module in the shipping materials.

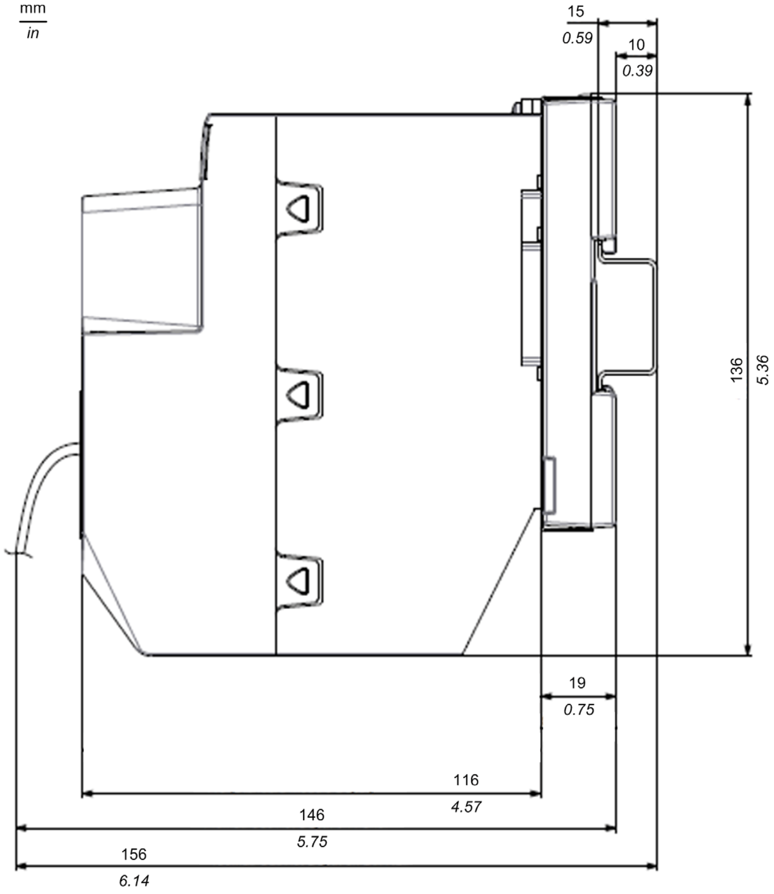
Power Supply Dimensions

The M580 safety power supplies present the following dimensions:



Power Supply Wiring Dimensions

The M580 safety power supplies present the following dimensions when wiring is considered:



M580 Safety Power Supply Performance Characteristics

BMXCPS4002S Safety Power Supply

The BMXCPS4002S safety power supply provides the following performance characteristics:

Input characteristics		
Nominal Voltage		100...240Vrms
Voltage range		85...132Vrms 170...264Vrms
Frequency range		47...63Hz
Masked input power outages		Max 10ms @100Vrms-15% & @200Vrms-15%
Typical Input apparent Power		130VA
Typical input current		1.1Arms @115Vrms 0.55Arms @230Vrms
Inrush Current @25° @ 1st start-up	Peak	30Arms @115Vrms 60Arms @230Vrms
	I^2t (for rating external fuse)	1A2s @115Vrms 4A2s @230Vrms
	It (for rating external breaker)	0.1As @115Vrms 0.15As @230Vrms
Integrated Protection		Internal non-accessible fuse located on L input

Output characteristics		
MAX 3V3_BAC output current		5.5A (18.2W)
MAX 24V_BAC output current		1.67A (40W)
MAX Total output power		40W
Detection	Overload	Yes - Disjunction
	Short-circuit	Yes - Disjunction
	Overvoltage	Yes - Disjunction

Other characteristics		
Dielectric	Primary/All Secondaries	SELV / PELV
Strength	Primary/Ground	SELV / PELV
Insulation Resistance	Primary/All Secondaries	100MΩ
	Primary/Ground	100MΩ

BMXCPS4022S Safety Power Supply

Input characteristics		
Nominal Voltage Type		24...48 Vdc
Input Voltage Range		18...62.4 Vdc
Efficiency		max losses ≤7W (efficiency ≥84.8%) at maximum continuous load, over entire input voltage range, and temperature range
Nominal Input Current		1.9 A @ 24 Vdc
		1.0 A @ 48 Vdc
Inrush current at first start-up @25°C	Peak current	≤60 A @ 24 Vdc
		≤60 A @ 48 Vdc
	I^2t (for rating external fuse)	≤ X A^2s @ 24 Vdc
		≤ X A^2s @ 48 Vdc
	It (for rating external breaker)	≤ X As @ 24 Vdc
		≤ X As @ 48 Vdc
Masked input power outages		Any input power outage lasting at max:
		● 1 ms at full load & minimum line voltage (i.e. 19.2 Vdc)
		● 10 ms at full load & nominal line voltage (i.e. 24 or 48Vdc)
		Must not induce any change in the output characteristics. Period between interruptions 1 sec.
Input Protection		● Protection against risk of fire: by a fuse mounted on the board, not accessible and not changeable by the user and located on DC+ input. Its rating is selected to comply with safety standards. It shall not be damaged during line noise withstand tests, under any circumstances.
		● Protection against reverse input polarity: a built-in circuitry must protect the module. The internal (and eventual external) fuse(s) must not blow up. The power supply must start-up correctly when the right polarity is restored.

Output characteristics:	
Output Nominal Voltage	24.35 V
Output Steady-State Voltage Range	23.3...24.7 V over the entire input voltage range, over the full output load range, and over the full temperature range.
Output Ripple and Noise	240 mV peak to peak (measured with a bandwidth ≥100 MHz, on the module connector pins.
Continuous Output Current Range	● 1.63 A maximum
	● 0 A minimum

Output characteristics:	
Transient Output Current Capability	1.9 A maximum during 500 ms, period minimum 20 sec.
Output impedance versus frequency	180 mΩ
Output Voltage Response to transient load on 24V_BAC	For the following output load transient on 24V_BAC:
	● Load variation I from minimum continuous output current limit to max transient output current limit (and vice versa).
	● Transition time 4 μs – pulse width 500ms – period 20 sec.
	● The transient output voltage on 24V_BAC must stay within the limits 23.0...25.0V, and the response time must be ≤ 50 ms.
	● Whatever the value of the capacitive load on 24V_BAC in the specified limits.
Protection against output overload/short-circuit	● In case of any condition of overload or short-circuit on 24V_BAC (i.e. any case of level, duration, temperature, input voltage), the board must be protected from any damage.
	● The overall maximum value of the overload detection threshold (i.e. including all tolerances, drifts, etc.) must be less than Imax.
	● Imax = 2 A.
Protection against overvoltage	Disjunction of the power supply for a rise of the output reaching 30.0 Vdc ±.8 V.
External Capacitive Load Capability	All the above characteristics must be fulfilled with the following external capacitive load value. This feature must be considered notably for slope-up, regulation loop stability and overload detection/protection.
	11500 μF capacitive value.

BMXCPS3522S Safety Power Supply

Input characteristics:		
Nominal Voltage Type		125 Vdc
Input Voltage Range		100...150 Vdc
Efficiency		max losses ≤7W (efficiency ≥84.8%) @max continuous load, over entire input voltage range & temperature range
Nominal Input Current		0.6 A @ 125 Vdc
Inrush current at first start-up @25°C	Peak current	≤60 A @ 125 Vdc
	I^2t (for rating external fuse)	≤ X A^2s @ 125 Vdc
	It (for rating external breaker)	≤ X As @ 4 Vdc
Masked input power outages		Any input power outage lasting at max :
		● 1 ms at full load & minimum line voltage (i.e. 100 Vdc)
		● 10 ms at full load & nominal line voltage (i.e. 125 Vdc)
		Must not induce any change in the output characteristics. Period between interruptions 1 sec.
Input Protection		● Protection against risk of fire : by a fuse mounted on the board, not accessible and not changeable by the user and located on DC+ input. Its rating is selected to comply with safety standards. It shall not be damaged during line noise withstand tests, under any circumstances.
		● Protection against reverse input polarity: a built-in circuitry must protect the module. The internal (and eventual external) fuse(s) must not blow up. The power supply must start-up correctly when the right polarity is restored.

	BMXCPS3522 /S High Power
Output Nominal Voltage	24.35 V
Output Steady-State Voltage Range	23.3...24.7 V over the entire input voltage range, over the full output load range and over the full temperature range.
Output Ripple and Noise	240 mV peak to peak (measured with a bandwidth ≥100 MHz, on the module connector pins.
Continuous Output Current Range	● 1.63 A maximum
	● 0 A minimum
Transient Output Current Capability	1.9 A maximum during 500ms, period minimum 20 sec.
Output impedance versus frequency	180 mΩ

	BMXCPS3522 /S High Power
Output Voltage Response to transient load on 24V_BAC	For the following output load transient on 24V_BAC:
	● Load variation I from minimum continuous output current limit to max transient output current limit (and vice versa).
	● Transition time 4 µs – pulse width 500ms – period 20 sec.
	● The transient output voltage on 24V_BAC must stay within the limits 23.0...25.0V, and the response time must be ≤ 50 ms.
	● Whatever the value of the capacitive load on 24V_BAC in the specified limits.
Protection against output overload/short-circuit	● In case of any condition of overload or short-circuit on 24V_BAC (i.e. any case of level, duration, temperature, input voltage), the board must be protected from any damage.
	● The overall maximum value of the overload detection threshold (i.e. including all tolerances, drifts, etc.) must be less than Imax.
	● Imax = 2 A.
Protection against overvoltage	Disjunction of the power supply for a rise of the output reaching 30.0 Vdc ±.8 V.
External Capacitive Load Capability	All the above characteristics must be fulfilled with the following external capacitive load value. This feature must be considered notably for slope-up, regulation loop stability and overload detection/protection.
	11500 µF capacitive value.

M580 Safety Power Supply Alarm Relay

Performance Characteristics

The alarm relay terminal block on the M580 safety power supplies present the following performance characteristics:

Characteristics	
Rated switching Voltage / Current	24 Vdc 2A (Restive load)
	240 Vac 2A (cos φ =1) point
Minimum switching load	5 Vdc 1 mA
Maximum switching voltage	62.4 Vdc
	264 Vac
Contact type	Normally open
Contact time	
● OFF → ON	10 ms or Less
● ON → OFF	12 ms or Less
Built-in protection	Against overload / short-circuits: none, a fast-blow fuse must be fitted.
	Against inductive overvoltage in AC: none, an RC circuit or a MOV (ZNO) suppressor (appropriate to the voltage) must be fitted in parallel to the terminals of each pre-actuator.
	Against inductive overvoltage in DC: none, a discharge diode must be fitted to the terminals of each pre-actuator.
Dielectric strength	Contact vs ground: 2000 Vrms 50Hz 1min.(Altitude 0...2000 m)
Insulation resistance	10 MΩ or more under 500 Vdc

Chapter 5
M580 Safety I/O Modules

Introduction

This chapter describes the M580 safety I/O modules.

What Is in This Chapter?

This chapter contains the following sections:

Section 5.1
M580 Safety I/O Modules Physical Description

Physical Description of M580 I/O Modules

Positioning Safety I/O Modules

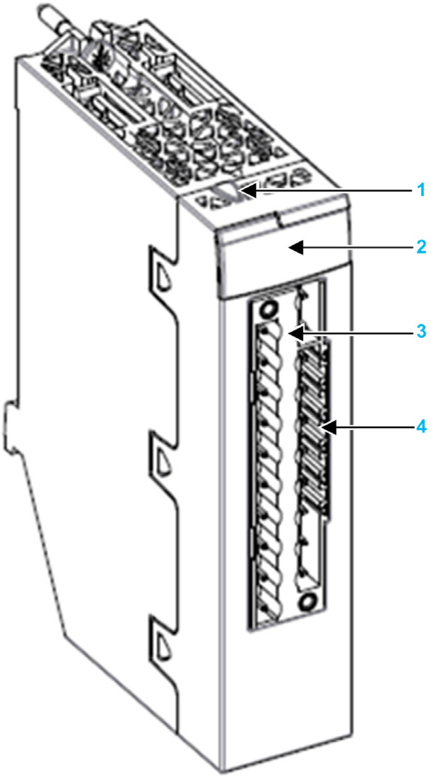
You can install an M580 safety I/O module on:

- the local rack in any slot that is not reserved for the power supply or CPU.
- a remote rack in any slot that is not reserved for the power supply or remote adapter.

NOTE: A safety I/O module can be installed on either a BMXXBP•••• X Bus rack or a BMEXBP•••• Ethernet rack. For a description of available M580 racks refer to the topic *Local and Remote Racks* in the *Modicon M580 Hardware Reference Manual.*

Safety I/O Module Front Panel

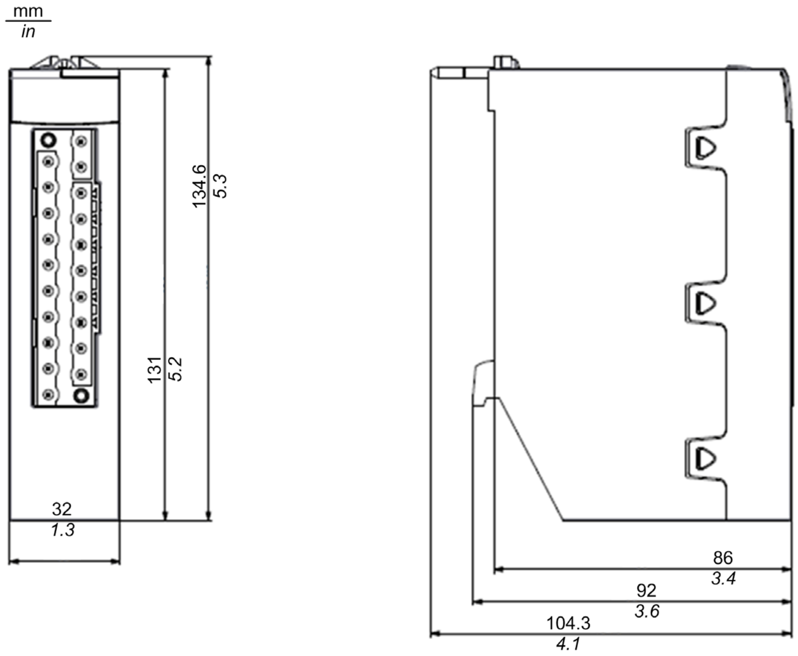
The front panel of each safety I/O module presents the following features:



1 Lock / Unlock configuration button
2 LED panel
3 20-pin connector
4 Keying pin slots

Safety I/O Module Dimensions

Each safety I/O module presents the following physical dimensions:



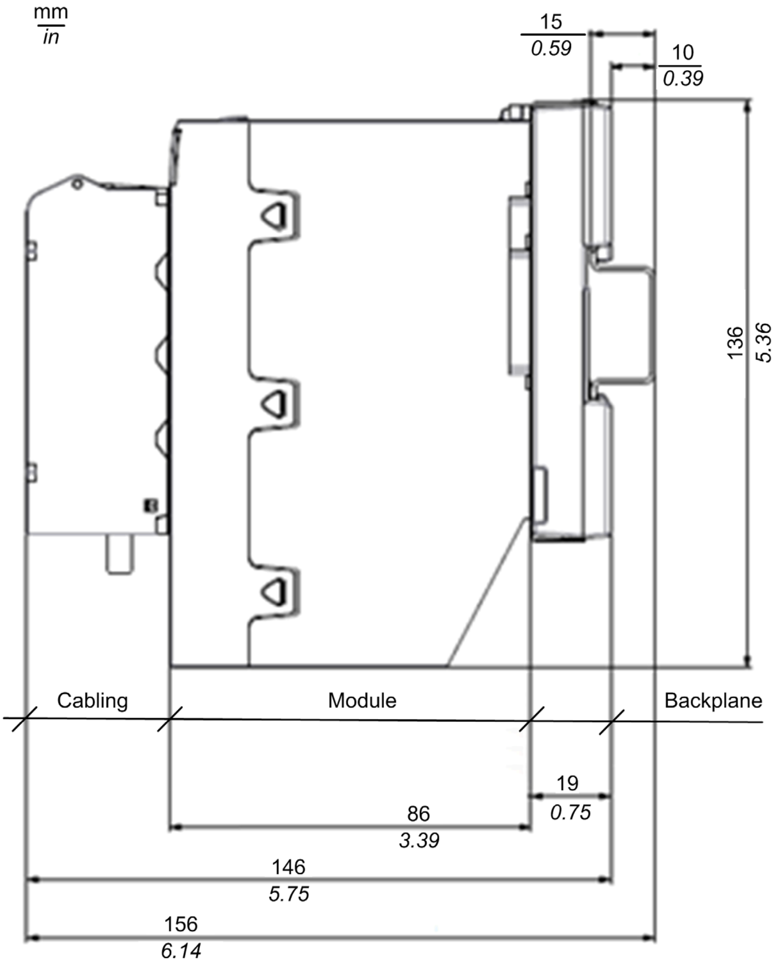
NOTE:

Consider the height of the safety I/O modules when you are planning the installation of a rack. Each safety I/O module extends below the lower edge of the rack by:

- 29.49 mm (1.161 in.) for an Ethernet rack
- 30.9 mm (1.217 in.) for an X Bus rack

Safety I/O Wiring Dimensions

Each safety I/O module presents the following wiring dimensions:



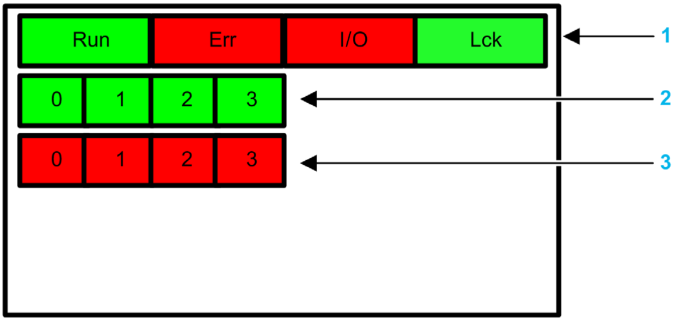
LEDs

Each safety I/O module provides module and channel LED diagnostics on the front face of the module:

- The top four LEDs (**Run**, **Err**, **I/O**, and **Lck**) together describe the state of the module.
- The bottom rows of LEDs combine with the top four LEDs to describe the state and health of each input or output channel.

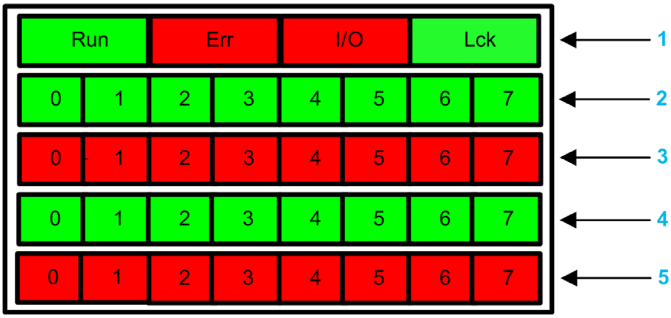
NOTE: For information on how to use the module LEDs to diagnose the condition of M580 safety modules, refer to the *Diagnostics (see Modicon M580, Safety Manual)* chapter of the *M580 Safety Manual*.

BMXSAI0410 safety analog input module, and BMXSRA0405 safety digital relay output module LEDs:



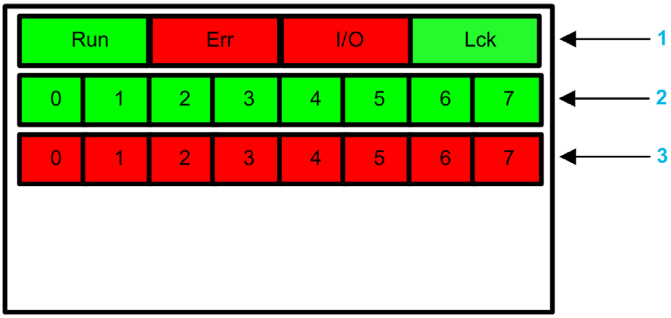
1 Module state LEDs
2 Channel state LEDs
3 Channel detected error LEDs

BMXSDI1602 safety digital input module LEDs:



1 Module state LEDs
2 Channel state LEDs for Rank A
3 Channel detected error LEDs for Rank A
2 Channel state LEDs for Rank B
3 Channel detected error LEDs for Rank B

BMXSDO0802 safety digital output module LEDs:



1 Module state LEDs
2 Channel state LEDs
3 Channel detected error LEDs

Section 5.2
M580 Safety I/O Performance Characteristics

Introduction

This section describes the performance characteristics of the M580 safety I/O modules.

What Is in This Section?

This section contains the following topics:

BMXSAI0410 Safety Analog Input Module Performance Characteristics

Analog Input Module Characteristics

The BMXSAI0410 safety analog input module presents the following performance characteristics:

Static characteristics	Parameter	Unit	Value
Input impedance in signal range	–	Ohm	286
Analog input error	Max full scale error @ 25°C	%	0.30%
Analog input error (=safety tolerance)	Max full scale error full temperature range --25°C to 70°C	%	0.35%
Reliability	MTTF @ 25°C	years	54.2
Linear Measuring Range	–	ct/mA	0...25mA and 12,500 counts (500 ct/mA)
Out of Range Detection	–	mA	<3.75mA and >20.75 mA
Digital resolution	Resolution	bits	16
	Number of channels simultaneously converted	–	4
Data format returned of the application program	–	–	binary
Value of an LSB	–	µA	0.191
Maximum permanent allowed overload	–	mA	25
Digital output reading under overload condition	overload will be signaled to client application	mA	I =25
Type of input	type	mA	4-20mA
	type	–	floating isolated inputs
	maximum Range for input	mA	0-25 mA
Common-mode characteristics	common mode rejection	dB	to be measured

Dynamic characteristics	Parameter	Unit	Value
input filter characteristics	order	–	second
	Frequency cut at -3dB	Hz	10.47

General characteristics	Parameter	Unit	Value
Conversion method	–	–	successive approximation
Type of protection	–	–	protecting diode
Isolation potential under normal operation	Insulation between channel	VAC eff	500 for 1 min.
	Insulation channel to backplane	VAC eff	1500 for 1 min.
External power supply data - if required	–	–	not required
Type & length of cable - installation rules recommended to provide interference immunity	–	–	shielded cable
Calibration or verification to maintain rated accuracy	–	–	No calibration
Typical examples of external connections	–	–	temperature sensor & pressure sensor

Miscellaneous characteristics	Parameter	Unit	Value
Monotonicity with no missing code	–	–	yes
Crosstalk between at d.c. & a.c. 50Hz and a.c. 60Hz	–	–	–
Non-linearity	+/-	LSB	0.006%
Repeatability at fixed temperature after specified stabilization time	–	–	–
3.3V consumption	Typical	mA	223
	Maximum	mA	246
24V consumption	Typical	mA	92
	Maximum	mA	115
Power dissipation	Maximum	W	3.98

BMXSDI1602 Safety Digital Input Module Performance Characteristics

Digital Input Module Characteristics

The BMXSDI1602 safety input module presents the following performance characteristics:

Characteristic		Value
Nominal input	Voltage	24 VDC
Type external sensor Power-supply	SELV/PELV, overvoltage II	(Max 60V)
Typical input current	Current	3.2mA
Input limit values	Voltage at state 1	≥11V
	Voltage at state 0	≤5V
	Current at state 1	> 2 mA for U ≥ 11V
	Current at state 0	< 1.5 mA
	Sensor supply (Ripple included)	From 19 to 30V (Possible up to 33. Limited 1 hour per Day)
Input Impedance	At Unom	7.5 KΩ
Response time	Typical/Maximum	100µs/ 250µs
Reliability	MTTF @ Tamb = 25°C	31.5 years
Reverse polarity		Protected
IEC61131-2 - Edition 3.0 (2007)		Type 3
Compatibility	(2 wires, 3 wires prox. Sensors)	IEC 947-5-2
Dielectric strength	Primaries/secondary	1500VRMS (at 4000m) 50/60 Hz for 1min
Insulation resistance		>10 MΩ (at 500 VDC)
Input type		Current sink
Input paralleling[1]		Yes
Sensor voltage Monitoring threshold	OK	> 18.6 VDC < 32 VDC
	Fault	< 18.6 VDC > 33 VDC
Sensor voltage monitoring response Time	On disappearance	4.4ms < T < 30ms
	On appearance	0.18 ms < T < 0.3 ms
Maximum external capacitance when using VS for short-circuit to 24V detection	Maximum	80nF
1.This characteristic enables several inputs to be wired on the same module, or on different modules if redundant inputs are required.		

Characteristic		Value
3.3V consumption	Typical	200mA
	Maximum	275mA
24V consumption	Typical	63mA
	Maximum	71mA
Max dissipated power		3.57W
1.This characteristic enables several inputs to be wired on the same module, or on different modules if redundant inputs are required.		

BMXSDO0802 Safety Digital Output Module Performance Characteristics

Digital Output Module Characteristics

The BMXSDO0802 safety digital output module presents the following performance characteristics:

Characteristic		Value
Nominal values	Voltage	24 VDC
	Current	0.5A
Limit values	Voltage	19...30V[1]
	Current/Channel	0.625 A
	Current/Module	5A
Type external actuator Power-supply		SELV/PELV (Max 60V), Overvoltage category II
Tungsten filament lamp power	max	6W
Leakage current	At state 0	< 0.5mA
Residual voltage	At state 1	< 1.2V
Protections	Transient voltage	yes
	Overload disjunction current	> 0.625 A
	Short circuit	yes
	Wrong polarity	yes
	Over temperature	yes
Minimum load. Resistance value (For pre-actuator)		48 Ω
Full detection of CUT wire: Maximum cable load capacitance value (including pre-actuator capacitance) between output and pre-actuator		10nF
Response time[2]		1.2 ms
Reliability: MTTF		45.8 years @ 25° C
Switching frequency on inductive load		0.5/LI^{2}Hz with Fmax =2Hz
Output paralleling		Yes (2 maximum)
Compatibility with DC inputs		Yes (Only sink type 3 or sink not IEC)
Built-in protection	Against overvoltage	Yes - by internal TVS
	Against reverse polarity	Yes - by reverse-mounted diode. Provide a fuse to the pre-actuator 24V.
	Against short circuits and overloads	Yes - by current limiter and electronic circuit-breaker 1.5 In < Id < 2 In

1. 33V permissible for 1 hour per 24h.
2. All outputs have fast demagnetization circuits for electromagnets. Electromagnet discharge time < L/R

Characteristic		Value
24V Preactuator voltage Monitoring threshold	OK	> 19.0V and < 31.8V
	Fault	< 18.0 and > 31.8V
Preactuator voltage Monitoring response time	On disappearance	2ms < T < 5.6ms
	On appearance	10 ms < T < 15.6 ms
Consumption 3.3V	Typical	240 mA
	Maximum	264 mA
Consumption 24V backplane	Typical	80 mA
	Maximum	87 mA
Consumption 24V pre-actuator (Without load current)	Typical	5 mA
	Maximum	15 mA
Dissipated power		4.4 W max
Dielectric strength (output/ground or internal logic)		1500 V rms & 50/60 Hz for 1min
Insulation resistance		> 10 MΩ at 500VDC
1. 33V permissible for 1 hour per 24h. 2. All outputs have fast demagnetization circuits for electromagnets. Electromagnet discharge time < L/R		

BMXSRA0405 Safety Digital Relay Output Module

Digital Relay Output Module Characteristics

The BMXSRA0405 safety digital relay output module presents the following performance characteristics:

Characteristic		Value
Rated switching Voltage / Current		24 VDC 5A (Resistive load)
		240 VAC 5A (cos Φ =1)
Current max for contacts on resistive load		5A (DC12 and AC12)
Current max for contacts on inductive load		4A DC13 and 3A AC15
Operating temperature		0 to 60°C
Type external actuator Power-supply		Overvoltage category II
Min switching load		5 VDC 10 mA
Max switching load		264 VAC 30 VDC
Switching time	OFF→ ON (operate)	12 ms typical
	ON →OFF (release)	6 ms typical
Life (Based on Elesta relay SIF3)	Mechanical	10 million cycles or more
	Electrical	DC12 24Vdc / 5A → 300.000 cycles
		DC12 24Vdc / 2A →500.000 cycles
		DC12 24Vdc / 1A→1.000.000 cycles
	L/R=40ms	DC13 24Vdc (0.1Hz) / 4A→30.000 cycles
		DC13 24Vdc (0.1Hz) / 2A→50.000 cycles
		DC13 24Vdc (0.1Hz) / 1A→80.000 cycles
	–	AC12 250Vac / 5A→70.000 cycles
		AC12 250Vac / 2A→30.000 cycles
		AC12 250Vac / 1A→250.000 cycles
	–	AC15 250Vac / 3A→40.000 cycles
		AC15 250Vac / 2A→80.000 cycles
		AC15 250Vac / 1A→80.000 cycles
Built-in Protection	Against overloads and short-circuits	None - a fast blow fuse must be fitted to each channel or group of channels.
	Against inductive overvoltages in ~	None - a RC circuit or MOV peak limiter (ZNO) suitable for the voltage must be fitted in parallel across the terminals of each preactuator.
	Against inductive overvoltages in =	None - a discharge diode must be fitted across the terminals of each preactuator.

Characteristic		Value
Max switching frequency		5 cycles by second
Dielectric maximum voltage between channels		3000 V rms 50/60Hz for 1 min
Dielectric maximum voltage between channels and backplane		3000 V rms 50/60Hz for 1 min
Reinforced insulation standard		3000 Vac insulation between the process side (relay contact) and the backplane
Insulation resistance		>10MW or more by insulation resistance tester
Reliability: MTTF at Tamb = 25°C		36.9 years
Protection degree		IP20
Consumption 3.3V	Typical	215 mA
	Maximum	240 mA
24V relay internal current consumption	Typical	95 mA
	Maximum	130 mA
Dissipated power	4 energized relays	3 W Typical; 3.9 W maximum

Chapter 6
Installing the M580 Safety PAC

Overview

This chapter explains how to install the M580 safety PAC.

NOTE: For additional information on how to install M580 PACs, refer to the topic *Installing a Local Rack (see Modicon M580, Hardware, Reference Manual)* in the *Modicon M580 Hardware Reference Manual*.

What Is in This Chapter?

This chapter contains the following sections:

Section 6.1
Installing M580 Racks and Extender Modules

Introduction

This section describes how to install an M580 rack and extender modules for an M580 safety PAC.

What Is in This Section?

This section contains the following topics:

Planning the Installation of the Local Rack

Introduction

The size and number of racks and the kinds of modules installed on the racks are significant considerations when you are planning an installation. That installation may be either inside or outside an enclosure. The height, width, and depth of the installed system head as well as the spacing between the local and the extender racks need to be well understood.

⚠ WARNING

UNEXPECTED EQUIPMENT OPERATION

Install the racks lengthwise and horizontally to facilitate ventilation.

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

Modules such as the power supply, CPU, coprocessor, and I/O are cooled by natural convection. Install them on a horizontally installed rack as illustrated in this manual to maintain the necessary thermal cooling. Other rack mounting positions may cause overheating and unexpected equipment operation.

Rack Usage

The racks available in Control Expert, and their permitted usage, are described below:

Reference	Slots	Bus	Usage			
			Local Main Rack	Local Extended Rack	Remote Main Rack	Remote Extended Rack
BME racks:						
BME XBP 0400	4	XBus & Ethernet	x	x	x	x
BME XBP 0800	8	XBus & Ethernet	x	x	x	x
BME XBP 1200	12	XBus & Ethernet	x	x	x	x
BME XBP 0602	6	XBus & Ethernet	x	x	x	x
BME XBP 1002	10	XBus & Ethernet	x	x	x	x
BMX racks:						
BMX XBP 0400	4	X Bus	–	x	x	x
BMX XBP 0600	6	X Bus	–	x	x	x
BMX XBP 0800	8	X Bus	–	x	x	x
BMX XBP 1200	12	X Bus	–	x	x	x
X : Permitted – : Not permitted						

Reference	Slots	Bus	Usage			
			Local Main Rack	Local Extended Rack	Remote Main Rack	Remote Extended Rack
Premium racks:						
NOTE: Premium racks are not supported by M580 safety PACs.						
Quantum racks:						
140 XBP 002 00	2	Quantum	–	–	x	x
140 XBP 003 00	3	Quantum	–	–	x	x
140 XBP 004 00	4	Quantum	–	–	x	x
140 XBP 006 00	6	Quantum	–	–	x	x
140 XBP 010 00	10	Quantum	–	–	x	x
140 XBP 016 00	16	Quantum	–	–	x	x
X : Permitted – : Not permitted						

Clearance Around the Racks

Leave a minimum space of 12 mm (0.472 in.) on the right side of each rack for cooling.

When your plan calls for extender racks, leave a minimum space of 35 mm (1.378 in.) in front of the modules. The BMX XBE 1000 rack extender module requires this clearance for the local bus connector and terminator.

Spacing Requirements for an M580 CPU in a Local Main Rack

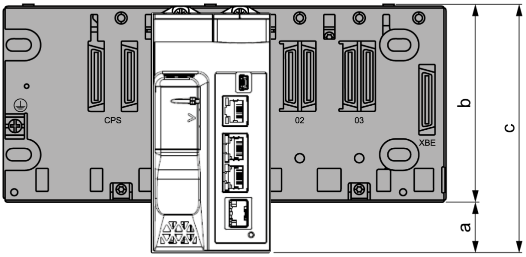
⚠ WARNING

OVERHEATING AND UNEXPECTED EQUIPMENT OPERATION

Maintain proper thermal clearances when installing the racks.

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

In the main local rack, allow additional clearance at the bottom of the rack for the CPU. This illustration shows the mounting dimensions when either an X Bus rack or an Ethernet rack is used. The overall height dimension of the main local rack in both cases is 134.6 mm (5.299 in.).



a Additional space below the rack to accommodate the height of the CPU. For an X Bus rack, the value is 32.0 mm (1.260 in.); for an Ethernet rack, the value is 30.59 mm (1.204 in.).

b The height of the rack. For an X Bus rack, the height is 103.7 mm (4.083 in.); for an Ethernet rack, the height is 105.11 mm (4.138 in.).

c The height of the main local rack, 135.7 mm (5.343 in.).

Thermal Considerations Inside an Enclosure

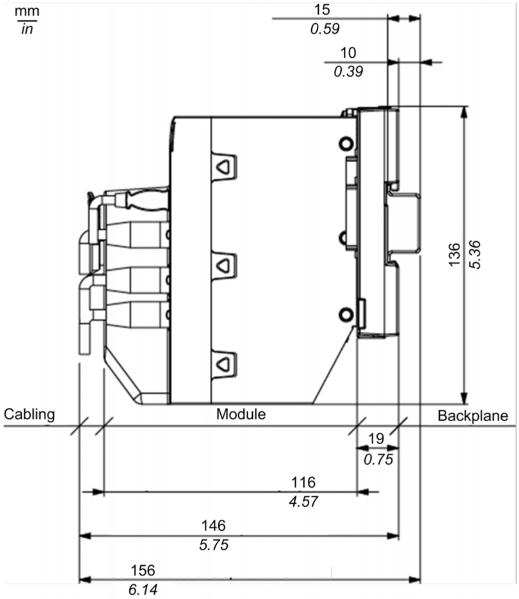
If the racks are installed in an enclosure, you need to facilitate air circulation. Use an enclosure that allows these minimum clearances:

- 80 mm (3.15 in.) above the top of the modules on the rack
- 60 mm (2.36 in.) below the bottom of the modules on the rack
- 60 mm (2.36 in.) between modules and wiring ducts

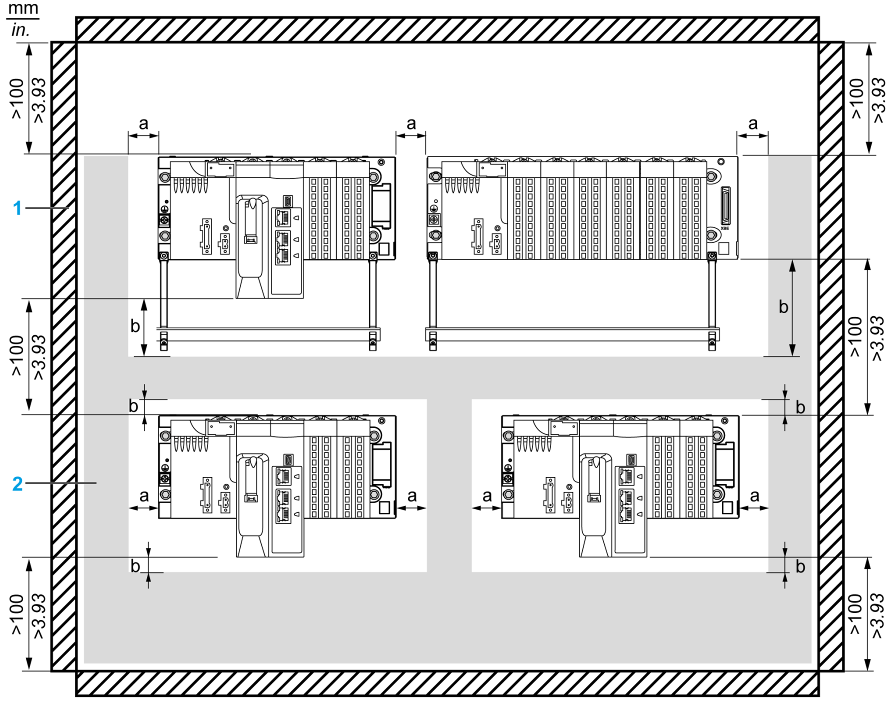
The minimum depth of the enclosure is:

- 150 mm (5.91 in.) if the rack is fastened to a plate
- 160 mm (6.30 in.) if the rack is mounted on a 15 mm (0.59 in.) DIN rail
- If BMX XBE 1000 rack extender modules are connected, the use of BMX XBC •••K cables with connectors angled at 45° is recommended.

Here is a side view of a rack on a DIN rail with modules and cables mounted in an enclosure:



This illustration shows the rules of a typical installation in a cabinet with ducts:



1 installation or casing
2 wiring duct or tray
a side clearance: > 40 mm (1.57 in.)
b top and bottom clearance with surrounding objects: > 20 mm (0.79 in.)

NOTE: In order to rise the density, a lower spacing between racks is acceptable if:
- There is no shielding bar, nor ducts between racks.
- The spacing between racks is not less than 40 mm (1.57 in).
- You apply a 5 °C (9 °F) derating to the maximum ambient temperature allowed. That is 55 °C (131 °F) for standard and coated module versions and 65 °C (149 °F) for hardened modules.

Mounting the Racks

Introduction

Ethernet and X Bus racks may be mounted on:

- DIN rails
- walls
- Telequick mounting grids

NOTE: Mount the racks on a properly grounded metallic surface to allow the PAC to operate correctly in the presence of electromagnetic interference.

NOTE: The mounting screws on the left side of the backplane may be accessible without unplugging the power supply module. Mount the backplane using the far left fastening hole on the panel.

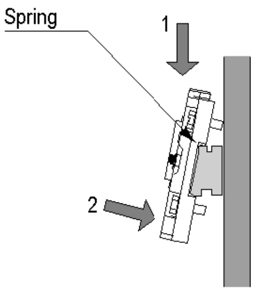
Mounting on a DIN Rail

Most racks can be mounted on DIN rails that are 35 mm (1.38 in.) wide and 15 mm (0.59 in.) deep.

NOTE: Racks longer than 400 mm (15.75 in.) that support more than 8 module slots are not compatible with DIN rail mounting. Do not mount a BMXXBP1200 (PV:02 or later)(H), BMEXBP1002(H), or BMEXBP1200(H) rack on a DIN rail.

NOTE: When mounted on a DIN rail, the system is more susceptible to mechanical stress.

Mounting a rack on a DIN rail:

Step	Action	Illustration
1	Position the rack on the top of the DIN rail and press down the top of the rack to compress the springs in contact with the DIN rail.	
2	Tilt the bottom of the rack backwards to flatten it against the DIN rail.	
3	Release the rack to lock it.	

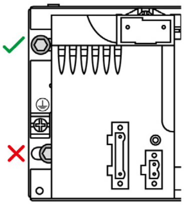
To remove a rack from a DIN rail:

Step	Action
1	Press down the top of the rack to compress the springs in contact with the DIN rail.
2	Tilt the bottom of the rack forward to disengage it from the DIN rail.
3	Release the freed rack.

Mounting on a Wall

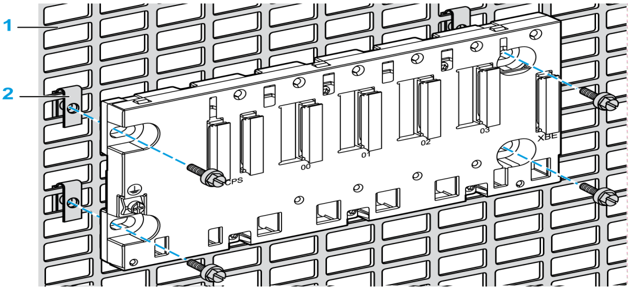
You can mount a rack on a wall inside or out of an enclosure with M4, M5, M6, or UNC #6 screws inserted in the fastening holes.

Place the 2 left side screws (near the power supply) as close as possible to the left edge of the rack. This enables you to access the screws after the power supply is mounted.



Mounting on Telequick Grid AM1-PA and AM3-PA Mounting Grids

You can mount a rack on a Telequick AM1-PA or AM3-PA mounting grid using M4, M5, M6, or UNC #6 screws.



Extending a Rack

Introduction

When your installation has more than one rack in the local rack or at a remote drop, install a BMXXBE1000 rack extender module on the main rack and the extended racks. Rack extender modules are connected together by X Bus extension cables.

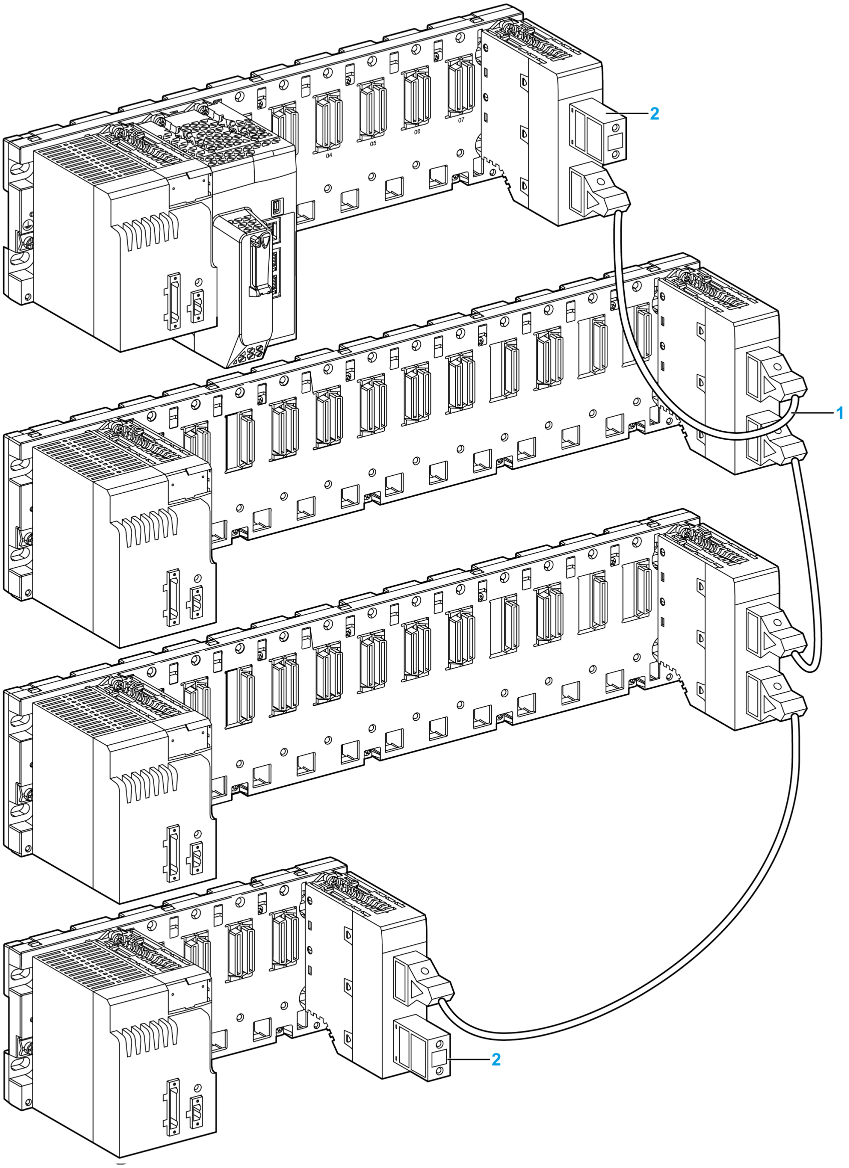
NOTE: For information on how to install and connect rack extender modules, refer to the topic *Modicon X80 Rack Extender Modules Installation* in the *Modicon M580 Hardware Reference Manual*.

Building an M580 Safety System Using Extended Local Racks

Using the BMXXBE1000 extender modules and cables, you can add to your M580 safety PAC:

- up to seven extended racks to the local main rack.
- one extended rack to a remote main rack.

Example of an Ethernet local main rack with extended racks and extender modules and cables:



1 The same station can contain racks of different sizes that are interconnected by extension cables.

2 The extender modules located at the extremities of the interconnected cables are terminated.

Section 6.2
Installing M580 CPU, Copro, Power Supply, and I/O

Introduction

This section describes how to install an M580 safety CPU, coprocessor, power supply, and I/O modules.

What Is in This Section?

This section contains the following topics:

Installing the CPU and Coprocessor

Introduction

You can install the BME•58•040S CPU and BMEP58CPROS3 coprocessor only in either a BMEXBP••00 or BMEXBP••02 Ethernet rack.

Installation Precautions

An M580 CPU is powered by the rack bus. Confirm that the rack power supply is turned off before installing the CPU.

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK

Remove all power sources before installing the CPU.

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

Remove the protective cover from the rack slot connectors before plugging the module in the rack.

⚠ WARNING

UNEXPECTED EQUIPMENT OPERATION

Check that the CPU does not contain an unsupported SD memory card before powering up the CPU.

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

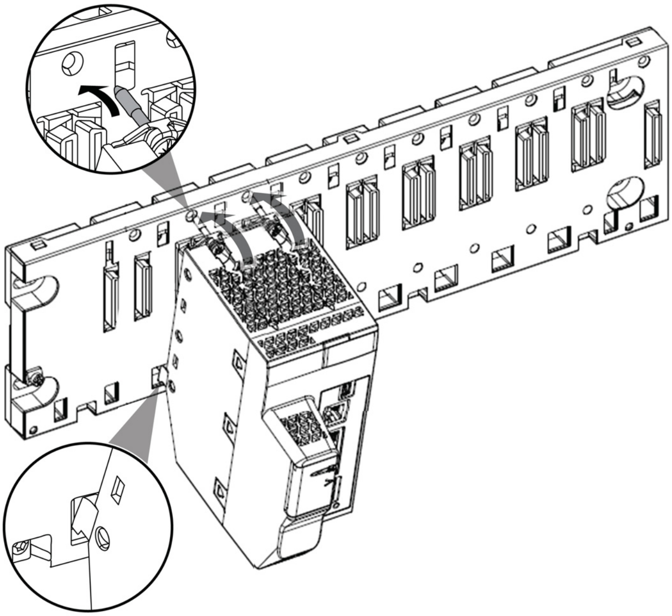
NOTE:
- Check that the memory card slot door is closed after a memory card is inserted in the CPU.
- Refer to `%SW97` to check the status of the SD card.

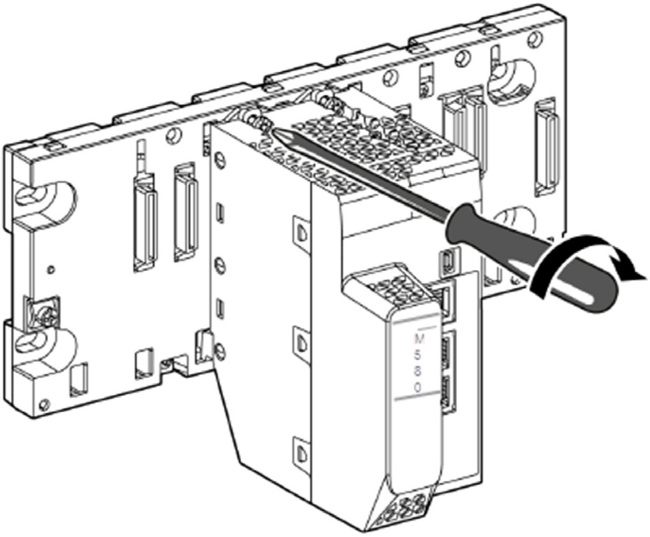
Installing the CPU and Copro in the Rack

Install the CPU and Copro in the rack at the following slot locations:

- CPU: slots **00** and **01**.
- Copro: slots **02** and **03**

Follow these steps to install a CPU and Copro in a rack:

Step	Action	
1	Verify that the power supply is turned off.	
2	Verify the following: ● If an SD memory card is used, it is supported by the CPU. ● The connectors' protective covers are removed. ● The CPU is placed on the slots marked **00** and **01**.	
3	Position the locating pins situated at the bottom rear of the module in the corresponding slots on the rack.	
4	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack. The module is now set in position.	

Step	Action	
5	Tighten the 2 screws on top of the CPU to maintain the module in place on the rack. tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).	
6	To install the Copro module, place it in slots **02** and **03** and follow steps 3, 4, and 5, above.	

Grounding

Follow all local and national safety codes and standards.

> **⚠ ⚠ DANGER**
>
> **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.
>
> **Failure to follow these instructions will result in death or serious injury.**

For information on grounding the CPU and coprocessor, refer to the topic *Grounding Considerations* in the *Modicon M580 Hardware Reference Manual*.

Installing a Power Supply Module

Introduction

Install the M580 safety power supply module in any X Bus or Ethernet rack that will contain other M580 safety modules. The safety power supply module can be used in racks that require either a single power supply, or dual redundant power supplies.

⚠ **WARNING**

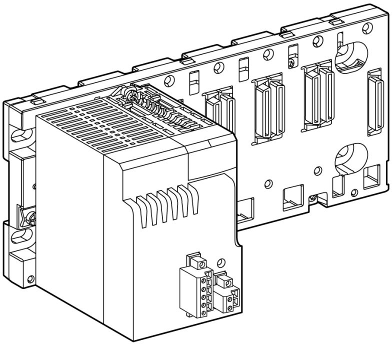
LOSS OF THE ABILITY TO PERFORM THE SAFETY FUNCTION

Use only the BMXCPS4002S, BMXCPS4022S, or BMXCPS3522S safety power supply on any rack that also includes at least one safety module.

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

For a rack that requires only a single power supply, place an M580 safety power supply module into the rack in the two slots marked **CPS**. For a BMEXBP••02 dual power supply rack *(see Modicon M580, Hardware, Reference Manual)*, place two M580 safety power supply modules side-by-side into the four slots marked **CPS**.

Example of a single power supply module installed in a BMEXBP0400 rack:



NOTE: The power supply module design allows it to be placed only in the dedicated slots marked **CPS**.

Installation Precautions

The M580 safety power supply module cannot be hot swapped. Confirm that the module is powered off when it is either inserted into the backplane, or extracted from the backplane.

NOTICE

RISK OF UNINTENDED SYSTEM BEHAVIOR

Confirm that power is turned off when either removing an M580 safety power supply module from a rack, or inserting it into a rack.

Failure to follow these instructions can result in equipment damage.

Do not plug in, or unplug, the main input removable terminal block when voltage is being applied to the M580 safety power supply module. Confirm that power to the module from the upstream breaker is OFF before performing either of these tasks.

NOTICE

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.

Failure to follow these instructions can result in equipment damage.

Do not plug in, or unplug, the alarm relay removable terminal block when the M580 safety power supply module is operating. Confirm that the module is de-energized before performing either of these tasks.

NOTICE

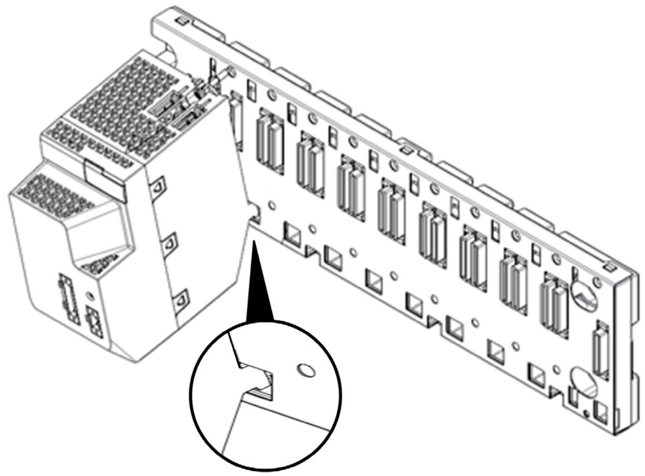
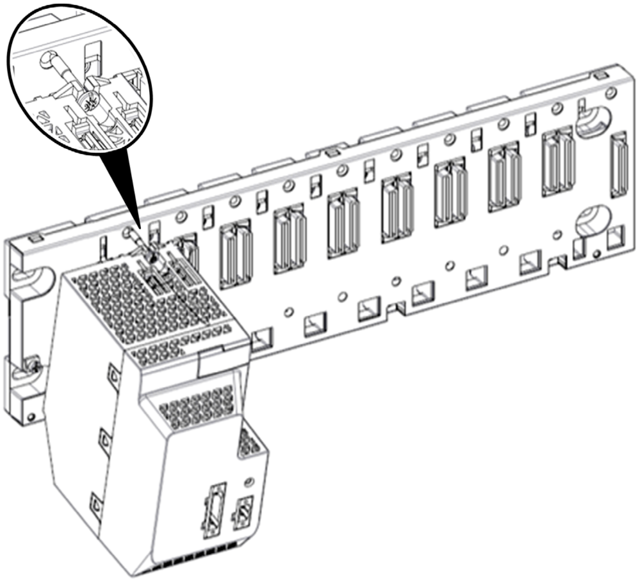
RISK OF UNINTENDED SYSTEM BEHAVIOR

Confirm that the M580 safety power supply module is de-energized before plugging in, or unplugging the module’s alarm relay removable terminal block.

Failure to follow these instructions can result in equipment damage.

Installing the Power Supply in the Rack

Follow these steps to install the safety power supply module in the rack slots marked **CPS**:

Step	Action	
1	Verify that the power supply module is placed in the slots marked **CPS**.	
2	Position the locating pins situated at the bottom rear of the module in the corresponding slots on the rack.	
3	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack. The module is now set in position.	
4	Tighten the single screw on top of the power supply to maintain the module in place on the rack. tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).	
5	For racks requiring dual power supplies, repeat steps 2, 3, and 4 for a second power supply.	

Grounding the Power Supply Module

Follow all local and national safety codes and standards.

⚠ ⚠ DANGER

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.

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

For information on grounding the power supply, refer to the topic *Grounding the Rack and Power Supply Module*.

Installing M580 Safety I/O

Introduction

You can install an M580 safety I/O module in any X Bus or Ethernet rack by placing it into any slot not reserved for the safety power supply or CPU (in the case of a local main rack).

NOTE: Use only a BMXCPS4002S, BMXCPS4022S, or BMXCPS3522S safety power supply for any rack that includes safety I/O modules.

You can hot swap M580 safety I/O.

General Cabling Precautions

To limit a DC load from interfering with an AC source, separate the power circuit cables (for example, cables leading to the power supply) from both input cables from sensors and output cables leading to actuators.

Place cables connecting the CPU to I/O modules in a sheath that is enclosed by metal ducting. Keep the sheathing for I/O cables separate from power cabling that is placed in its own sheathing. Place sheathed power cables in separate ducting from the I/O cables. Power cables and I/O cables need to be separated by a minimum distance of 100 mm.

Grounding Precautions

Each M580 safety I/O module is equipped with ground connection contacts.

Schneider Electric recommends the use of a BMXXSP•••• bar to help protect the rack from electromagnetic disturbances.

For the BMXSAI0410 safety analog input module, in particular, the use of a BMXXSP•••• bar is recommended. Connect the cable sheathing to the grounding bar by clamping it to the grounding bar on the module side.

⚠ ⚠ DANGER

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 voltage supplying the sensors or actuators.

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

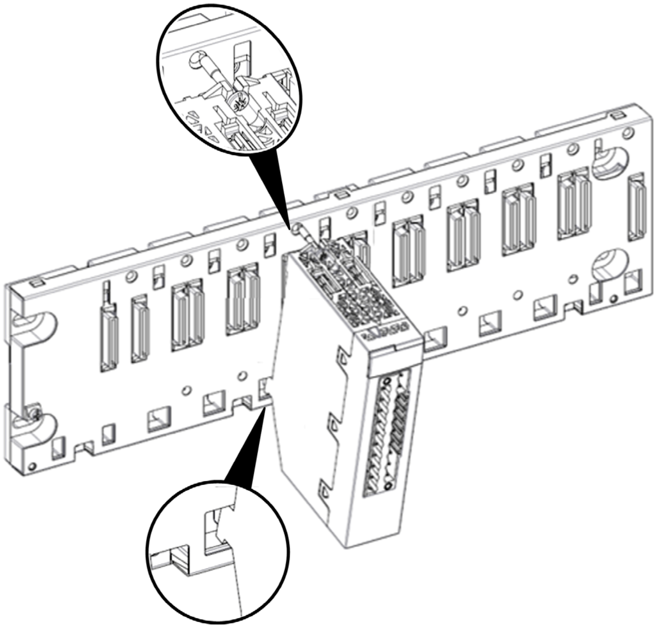
Input Module Sensor Placement (In Relation to the Ground)

When placing sensors in your system:

- Place sensors in close proximity to each other, separated by not more than a few meters.
- Reference all sensors to a single point, and connect that point to the PAC ground.

Installing a Safety I/O Module in the Rack

An M580 safety I/O modules requires a single rack slot. You can install a safety I/O module into any slot not reserved for the power supply or CPU. Follow these steps to install a safety I/O module in a rack:

Step	Action	
1	Position the locating pins situated at the bottom rear of the module in the corresponding slots on the rack.	
2	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack. The module is now set in position.	
3	Tighten the single screw on top of the module to maintain the module in place on the rack. Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).	
4	For each additional module, repeat steps 1, 2, and 3 until all modules are installed on the rack.	

Grounding the I/O Modules

For information on grounding, refer to the topic *Grounding the Rack and Power Supply Module*.

NOTE: For the BMXSAI0410 safety analog input module, Schneider Electric recommends that you also use a BMXXSP•••• grounding bar. For information on how to install this piece of equipment refer to the topic *Shielding connection Kit*.

Installing an SD Memory Card in a CPU

Introduction

The BME•58•040S CPU supports the use of the BMXRMS004GPF 4GB SD memory card.

Memory Card Maintenance

To keep the memory card in normal working order:

- Avoid removing the memory card from its slot when the CPU accesses the card (memory card access green LED ON or blinking).
- Avoid touching the memory card connectors.
- Keep the memory card away from electrostatic and electromagnetic sources as well as heat, sunlight, water, and moisture.
- Avoid impact on the memory card.
- Before sending a memory card by post (mail), check the postal service security policy. In some countries, the postal service exposes mail to high levels of radiation as a security measure. These high levels of radiation may erase the contents of the memory card and render it unusable.
- If a card is extracted without generating a rising edge of the bit %S65 and without checking that the memory card access green LED is OFF, the data (files, application, and so on) may be lost or become unreliable.

Memory Card Insertion Procedure

Procedure for inserting a memory card into a BME•58•040S CPU:

Step	Description
1	Open the SD memory card protective door.
2	Insert the card in its slot.
3	Push the memory card until you hear a click. **Result:** The card should now be clipped into its slot. **Note:** Insertion of the memory card does not force an application restore.
4	Close the memory card protective door.

Memory Card Removal Procedure

NOTE: Before removing a memory card, a rising edge on bit %S65 needs to be generated. If a card is extracted without generating a rising edge of the bit `%S65` and without checking that the memory card access green LED is OFF, the data may be lost.

Procedure for removing a memory card from a BME•58•040S CPU:

Step	Description
1	Generate a rising edge on bit `%S65`.
2	Check that the memory card access green LED is OFF.
3	Open the SD memory card protective door.
4	Push the memory card until you hear a click, then release the pressure on the card. **Result:** The card should release from its slot.
5	Remove the card from its slot. **Note:** The memory card access green LED is ON when the memory card is removed from the CPU.
6	Close the memory card protective door.

Chapter 7
Upgrading M580 Safety CPU Firmware

Upgrading CPU Firmware

Upgrading CPU Firmware

You can update the CPU firmware by downloading a new firmware version with Unity Loader.

Download the firmware through a connection to one of these:

- CPU mini-B USB connector
- CPU service port
- Ethernet network

NOTE: For a description of the download procedure, refer to the *Unity Loader, a SoCollaborative software User Manual*

Enabling CPU Firmware Update

To enable the firmware update, you first need to unlock security for the CPU, as follows:

Step	Action
1	In the **PLC Bus** window, right-click on the Ethernet ports of the CPU.
2	Select **Open Submodule**.
3	Click on the **Security** tab.
4	Click **Unlock Security**.

CPU Firmware File

Select the firmware file (**.ldx*) for the BME•58•040S safety CPU. The .ldx file contains firmware upgrades for the safety and process areas of the CPU and for its web pages.

CPU Firmware Update Procedure

To upgrade the CPU firmware, follow these steps:

Step	Action
1	Install Unity Loader software.
2	Connect the PC that is running Unity Loader to the CPU.
3	Launch Unity Loader.
4	Click **Firmware** tab.
5	In the **PC** list box, select the *.ldx* file that contains the firmware file.
6	When connected with Ethernet, check that the MAC address indicated in the **PLC** box corresponds to the MAC address marked on the CPU.
7	Check that transfer sign is green to allow transfer from PC to CPU.
8	Click **Transfer**. **NOTE:** During the firmware download process, the green **DL** LED on the CPU turns ON indicating the CPU is communicating only with the Unity Loader Software,
9	Click **Close**.

After the firmware upgrade process finishes:

- The CPU reboots with the new firmware.
- The application program stored in flash memory is preserved.
- The CPU performs a cold start and enters STOP mode, even if **Automatic start in Run** is selected in the CPU **Configuration** tab.

NOTE: If the firmware upgrade process is interrupted (for example, by a lost connection or a power outage), reset the CPU, which in this case will re-start using the old firmware.

Other M580 Safety Module Firmware

Upgrading the CPU firmware also upgrades the firmware of the coprocessor. Each time the coprocessor boots, it receives its operating system from the CPU.

Firmware for the M580 safety power supply and I/O modules is not upgradable.

Chapter 8
Operating an M580 Safety System

Introduction

This chapter provides information on how to operate an M580 safety system.

What Is in This Chapter?

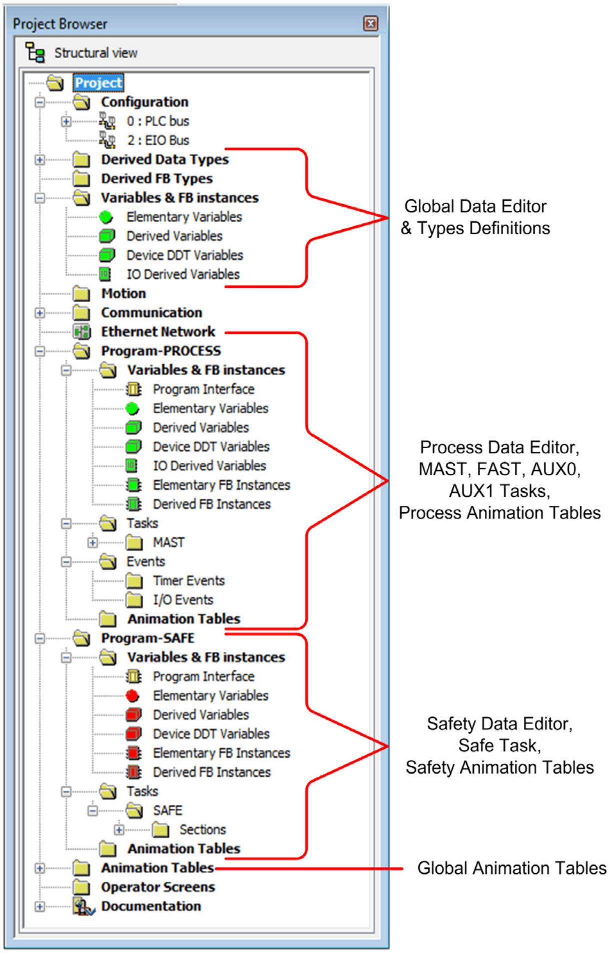
This chapter contains the following sections:

Section 8.1
Process, Safety and Global Data Areas in Control Expert

Data Separation in Control Expert

Data Areas in Control Expert

The **Structural View** of the **Project Browser** displays the separation of data in Control Expert. As shown below, each data area has its own data editor and collection of animation tables:



Global Data Editor
& Types Definitions

Process Data Editor,
MAST, FAST, AUX0,
AUX1 Tasks,
Process Animation Tables

Safety Data Editor,
Safe Task,
Safety Animation Tables

Global Animation Tables

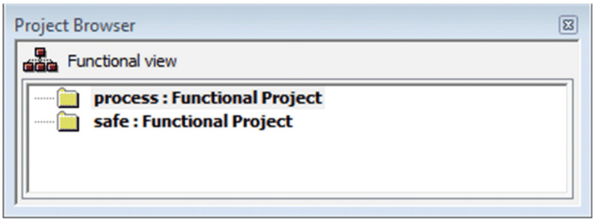
Looking at the **Project Browser** you will notice that:

- The safe area contains a Safety Data Editor, safety logic, and function block instances used by the SAFE task. However, note that:
  - I/O events, timer events, and sub-routines are not supported in a safety program.
  - IODDT variables are not supported by the SAFE task, and are not included in the safe area.
  - Red icons are used to indicate the SAFE parts of the program.
- The process area contains a Process Data Editor, process logic, and function block instances used by the non-safe tasks (i.e., MAST, FAST, AUX0 and AUX1).
- The global area contains a Global Data Editor, derived data and function block types instantiated in the process and safety programs.

NOTE: The term *Global Data* used in this topic refers to the application wide – or global – scope of data objects in a safety project. It does not refer to the Global Data service that is supported by many Schneider Electric Ethernet modules.

Project Browser in Functional View

The **Functional View** of the Control Expert. **Project Browser** for an M580 safety system presents two functional projects – one for the process namespace, one for the safe namespace:



process : Functional Project

safe : Functional Project

Management of each functional project in an M580 safety system is the same as managing a project in the functional view of an M580 non-safety system, except for animation tables and code sections.

Effect on Structural View:

When you add a code section or animation table to a functional project, it becomes associated with the namespace associated with that functional project. Adding a code section or animation table to:

- the **process : Functional Project** adds it to the process namespace of the project in structural view.
- the **safe : Functional Project** adds it to the safe namespace of the project in structural view.

Availability of Language and Task Selections:

When you create a new code section for a functional project (by selecting **Create → New Section...**), the available **Language** and **Task** selections depend on the functional project:

When you create a new code section for a functional project (by selecting **Create → New Section...**), the available **Language** and **Task** selections depend on the associated functional project:

Functional Project	Available Languages and Tasks	
	Languages[1]	Tasks[2]
process : Functional Project	● IL ● FBD ● LD ● LL984 segment ● SFC ● ST	● MAST ● FAST ● AUX0 ● AUX1
safe : Functional Project	● FBD ● LD	● SAFE

1. Selected in the **General** tab of the new section dialog.
2. Selected in the **Localization** tab of the new section dialog. The MAST task is available by default. Other sections are available for selection only after they have been created in the process program.

Color Coded Icons

To help you distinguish between the process and safe parts of the project, red colored icons are used to identify the safe parts of your application.

Section 8.2
Operating Modes, Operating States, and Tasks

Introduction

This section describes the operating modes, operating states, and tasks supported by the M580 safety PAC.

What Is in This Section?

This section contains the following topics:

M580 Safety PAC Operating Modes

Two Operating Modes

The M580 safety PAC presents two operating modes:

- Safety mode: the default operating mode used for safety operations.
- Maintenance mode: an optional operating mode that can be entered temporarily to debug and modify the application program, or change the configuration.

Control Expert XL Safety software is the exclusive tool you can use to manage operating mode transitions.

NOTE: The operating mode setting of a Hot Standby safety PAC – either safety mode or maintenance mode – is not included in the transfer of an application from the primary PAC to the standby PAC. On a switchover, when a safety PAC switches from standby PAC to primary PAC, the operating mode is automatically set to safety mode.

Safety Mode and its Limitations

Safety mode is the default mode of safety PAC. When the safety PAC is powered ON with a valid application present, the PAC enters safety mode. Safety mode is used to control execution of the safety function. You can upload, download, run and stop the project in safety mode.

When the M580 safety PAC is operating in safety mode, the following functions are **not** available:

- Downloading a changed configuration from Control Expert to the PAC.
- Editing and/or forcing safety variable values and safety I/O states.
- Debugging application logic, by means of breakpoints, watchpoints, and step-through code execution.
- Using animation tables or UMAS requests (for example, from an HMI) to write to safety variables and safety I/O.
- Changing the configuration settings of safety modules via CCOTF. (Note that the use of CCOTF for non-interfering modules is supported.)
- Performing online modification of the safety application.
- Using link animation.

NOTE: In safety mode, all safety variables and safety I/O states are read-only. You cannot directly edit the value of a safety variable.

You can create a global variable, and use it to pass a value between a linked process (non-safe) variable and a linked safety variable using the interface tabs of the Process Data Editor and the Safety Data Editor. After the link is made, the transfer is executed as follows:

- At the beginning of each SAFE task, the non-safe variable values are copied to the safe variables.
- At the end of the SAFE task, the safe output variable values are copied to the non-safe variables.

Maintenance Mode Functionality

Maintenance mode is comparable to the normal mode of a non-safety M580 CPU. It is used only to debug and tune the application SAFE task. Maintenance mode is temporary because the safety PAC automatically enters safety mode if communication between Control Expert and the PAC is lost, or upon the execution of a disconnect command. In maintenance mode, persons with the appropriate permissions can both read and write to safety variables and safety I/O that are configured to accept edits.

In maintenance mode, dual execution of SAFE task code is performed, but the results are not compared.

When the M580 safety PAC is operating in maintenance mode, the following functions are available:

- Downloading a changed configuration from Control Expert to the PAC.
- Editing and/or forcing safety variable values and safety I/O states.
- Debugging application logic, by means of breakpoints, watchpoints, and step-through code execution.
- Using animation tables or UMAS requests (for example, from an HMI) to write to safety variables and safety I/O.
- Changing the configuration via CCOTF.
- Performing online modification of the safety application.
- Using link animation.

In maintenance mode, the SIL level of the Safety PLC is not guaranteed.

⚠ WARNING

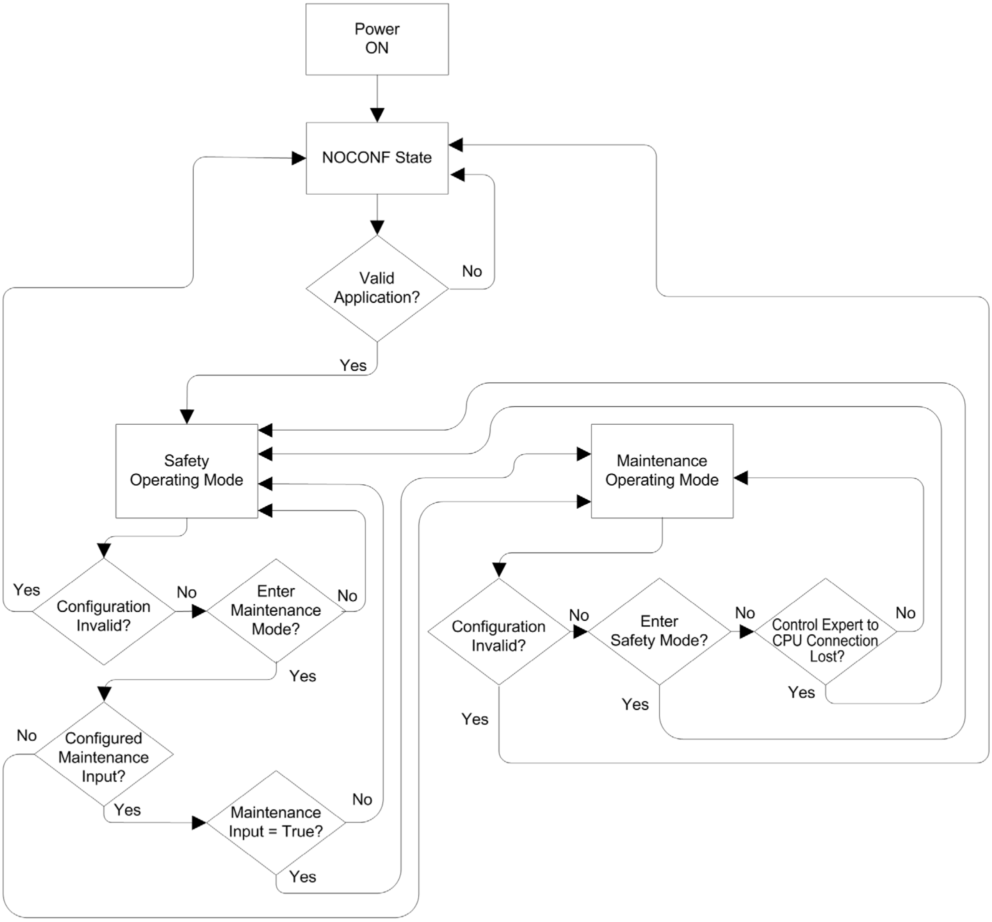
LOSS OF THE SAFETY INTEGRITY LEVEL

While the safety PAC is in maintenance mode, you need to take appropriate measures to ensure the safe state of the system.

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

Operating Mode Transitions

The following diagram shows how the M580 safety PAC enters, then transitions between safety mode and maintenance mode:



When switching between safety mode and maintenance mode:

- It is OK to switch from maintenance mode to safety mode with forcing ON. In this case, the forced variable value or I/O state remains forced after the transition until another transition from safety to maintenance mode occurs.
- The transition from maintenance mode to safety mode can be accomplished in the following ways:
  - Manually, by menu or toolbar command in Control Expert.
  - Automatically, by the safety PAC, when communication between Control Expert and the PAC is lost for about 50 seconds.
- The maintenance input function, when it is configured, operates as a check on the transition from safety mode to maintenance mode. The maintenance input function is configured in Control Expert in the CPU **Configuration** tab by:
  - Selecting the **Maintenance Input** setting, and
  - Entering the topological address of an input bit (%I) for a non-interfering digital input module on the local rack.

  When the maintenance input is configured, the transition from safety mode to maintenance mode takes into account the state of the designated input bit (%I). If the bit is set to 0 (false), the PAC is locked in safety mode. If the bit is set to 1 (true), a transition to maintenance mode can occur.

Switching Between Safety Mode and Maintenance Mode in Control Expert

Switching the safety PAC from maintenance mode to safety mode is not possible if:

- The PAC is in debug mode.
- A breakpoint is activated in a SAFE task section.
- A watchpoint is set in a SAFE task section.

When debug mode is not active, no SAFE task breakpoint is activated, and no SAFE task watchpoint is set, you can manually activate a transition between safety mode and maintenance mode, as follows:

- To switch from safety mode to maintenance mode, either:
  - Select **PLC → Maintenance**, or
  - Click the toolbar button.
- To switch from maintenance mode to safety mode, either:
  - Select **PLC → Safety**, or
  - Click the toolbar button.

NOTE: Entering and exiting safety mode events are logged in the SYSLOG server in the CPU.

Determining the Operating Mode

You can determine the current operating mode of an M580 safety PAC using either the **SMOD** LEDs of the CPU and coprocessor, or Control Expert.

When the **SMOD** LEDs of the CPU and coprocessor are:

- *Flashing* ON, the PAC is in maintenance mode.
- *Solid* ON, the PAC is in safety mode.

When Control Expert is connected to the PAC, it identifies the operating mode of the M580 safety PAC in several places:

- System words %SW12 (coprocessor) and %SW13 (CPU) *(see page 204)* together indicate the operating mode of the PAC, as follows:
  - ❍ if %SW12 is set to 16#A501 (hex) and %SW13 is set to 16#501A (hex), the PAC is in maintenance mode.
  - ❍ if either or both of these system words is set to 16#5AFE (hex), the PAC is in safety mode.
- Both the **Task** and **Information** sub-tabs of the CPU **Animation** tab display the operating mode of the PAC.
- The task bar, at the bottom of the Control Expert main window, indicates the operating mode as either MAINTENANCE or SAFETY.

M580 Safety PAC Operating States

Operating States

The M580 safety PAC operating states are described below.

NOTE: For a description of the relationship between M580 safety PAC operating states and M580 Hot Standby PAC operating states, refer to the document *Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures* and the topics *Hot Standby System States (see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)* and *Hot Standby State Assignments and Transitions (see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)*.

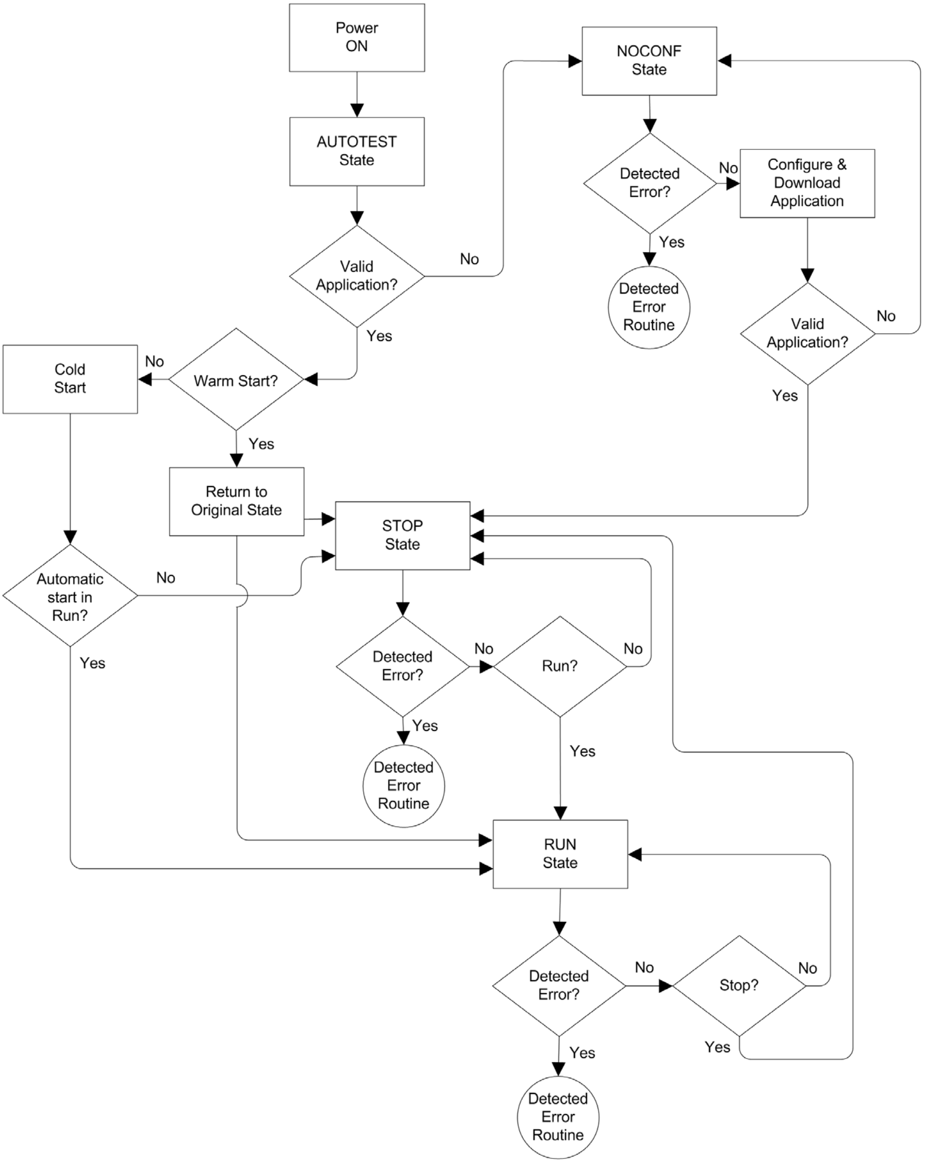
Operating State	Applies to...	Description
AUTOTEST	PAC	The CPU is executing internal self-tests. **NOTE:** If extended racks are connected to the main local rack and line terminators are not plugged into the unused connectors on the rack extender module, the CPU remains in AUTOTEST after the self-tests have completed.
NOCONF	PAC	The application program is not valid.
STOP	PAC or Task	The PAC has a valid application and no error is detected, but operation has stopped because: ● At startup **Automatic start in Run** is not set (safety mode *(see page 112)*). ● Execution stopped by execution of a STOP command (safe *(see page 112)* or maintenance *(see page 113)* mode). ● Breakpoints were set in maintenance mode, then the connection between Control Expert and the CPU was lost for more than 50 seconds. The CPU reads the inputs associated with each task, but does not refresh outputs, which enter their fallback state. The CPU can be restarted when you are ready. **NOTE:** Issuing a STOP command in Control Expert stops all tasks. The STOP event is recorded in the SYSLOG server of the CPU.

Operating State	Applies to...	Description
HALT	Task	The M580 safety PAC presents two independent HALT states: ● Process HALT applies to the non-SAFE tasks (MAST, FAST, AUX0, and AUX1). When any process task enters the HALT state, all other process tasks also enter the HALT state. The SAFE task is not affected by a process HALT condition. ● SAFE HALT applies only to the SAFE task. Process tasks are not affected by a SAFE HALT condition. In each case, task operations are halted because an unexpected blocking condition has been encountered, resulting in a recoverable *(see Modicon M580, Safety Manual)* condition. The CPU reads the inputs associated with each halted task, but does not refresh outputs, which are in fallback state.
RUN	PAC or Task	With a valid application and no error detected, the CPU reads the inputs associated with each task, executes the code associated with each task, and refreshes the associated outputs. ● in safety mode *(see page 112)*: the safety function is performed, and all limitations are applied. ● in maintenance mode *(see page 113)*: the PAC operates like any non-safety CPU. Dual execution of SAFE task code is performed, but the results are not compared. **NOTE:** Issuing a RUN command in Control Expert starts all tasks. The RUN event is recorded in the SYSLOG server of the CPU
WAIT	PAC	The CPU is in a transitory state while it backs up data when a power down condition is detected. The CPU starts again only when power is restored and the supply reserve is replenished. Because WAIT is a transitory state, it may not be visible. The CPU performs a warm restart *(see page 124)* to exit the WAIT state.
ERROR	PAC	The CPU is stopped because an non-recoverable *(see Modicon M580, Safety Manual)* hardware or system error is detected. The ERROR state triggers the safety function *(see Modicon M580, Safety Manual)*. When the system is ready to be restarted, perform a cold start *(see page 124)* of the CPU to exit the ERROR state, either by cycling power or performing a RESET.
OS DOWNLOAD	PAC	A CPU or COPRO firmware download is in progress.

Refer to the *M580 CPU LED Diagnostics (see Modicon M580, Safety Manual)* and *M580 Safety Coprocessor LED Diagnostics (see Modicon M580, Safety Manual)* topics for information on the operating states of the PAC.

Operating State Transitions

The transitions between the several states in an M580 safety PAC are described, below:



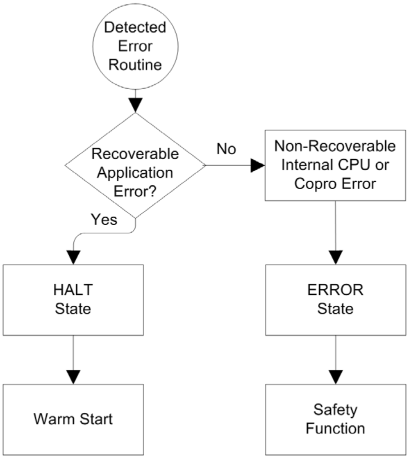
Refer to the topic *Detected Error Processing (see page 120)* for information on how the safety system handles detected errors.

Detected Error Processing

The M580 safety PAC handles the following kinds of CPU detected errors:

- Recoverable application detected errors: These events cause the related task(s) to enter the HALT state.
  NOTE: Because the MAST, FAST, and AUX tasks operate in the same memory area, an event that causes one of these tasks to enter HALT state causes the other non-safe tasks also to enter HALT state. Because the SAFE task operates in a separate memory area, the non-safe tasks are not affected if the SAFE task enters HALT state.
- Non-recoverable application detected errors: Internal CPU or coprocessor detected errors: These events cause the PAC to enter the ERROR state. The safety function is applied to the affected portion of the safety loop.

The logic of the detected error handling process is described below:


Detected Error Routine
Recoverable Application Error?
No
Yes
Non-Recoverable Internal CPU or Copro Error
HALT State
ERROR State
Warm Start
Safety Function

The impact of detected errors on individual tasks is described below:

Detected Error Type	Task State			
	FAST	SAFE	MAST	AUX
FAST task watchdog overrun	HALT	RUN[1]	HALT	HALT
SAFE task watchdog overrun	RUN	HALT[2]	RUN	RUN
MAST task watchdog overrun	HALT	RUN	HALT	HALT
AUX task watchdog overrun	HALT	RUN	HALT	HALT
CPU dual code execution detected error	RUN	HALT[2]	RUN	RUN
Safety watchdog overrun[3]	ERROR	ERROR[2]	ERROR	ERROR
CPU internal detected error	ERROR	ERROR[2]	ERROR	ERROR

1.Because FAST task has a higher priority than the SAFE task, delay of the FAST task may cause the SAFE task to enter HALT or ERROR state instead of RUN state.
2. The ERROR and HALT states on the SAFE task causes the safe outputs to be set to their user configurable state (fallback or maintain).
3. The safety watchdog is set equal to 1.5 times the SAFE task watchdog.

Task Bar Safety Status Viewer

When Control Expert is connected to the M580 safety PAC, the task bar includes a field describing the combined operating states of the SAFE task and the process tasks (MAST, FAST, AUX0, AUX1), as follows:

Process task(s) state	SAFE task state	Message
STOP (all process tasks in STOP state)	STOP	STOP
STOP (all process tasks in STOP state)	RUN	RUN
STOP (all process tasks in STOP state)	HALT	SAFE HALT
RUN (at lease one process task in RUN state)	STOP	RUN
RUN (at lease one process task in RUN state)	RUN	RUN
RUN (at lease one process task in RUN state)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

Start Up Sequences

Introduction

The M580 safety PAC can enter the start-up sequence in the following circumstances:

- At initial power-up.
- In response to a power interruption.

Depending on the type of task, and the context of the power interruption, the M580 safety PAC may perform either a cold start *(see page 124)* or a warm start *(see page 124)* when power is restored.

Initial Start-Up

At initial start-up, the M580 safety PAC performs a cold start. All tasks, including both the SAFE task and the non-safe (MAST, FAST, AUX0, AUX1) tasks, enter the STOP state unless **Automatic start in RUN** is enabled, in which case all tasks enter the RUN state.

Start-Up after a Power Interruption

The M580 safety power supply provides a power reserve that continues to supply all modules on the rack for up to 10 ms in case of a power interruption. When the power reserve is depleted, the M580 safety PAC performs a complete power cycle.

Before powering down the system, the safety CPU stores the following data that defines the operating context at power down:

- Date and time of the power down (stored in %SW54...%SW58).
- State of each task.
- State of event timers.
- Values of running counters.
- Signature of the application.
- Application data (current values of application variables)
- Application check sum.

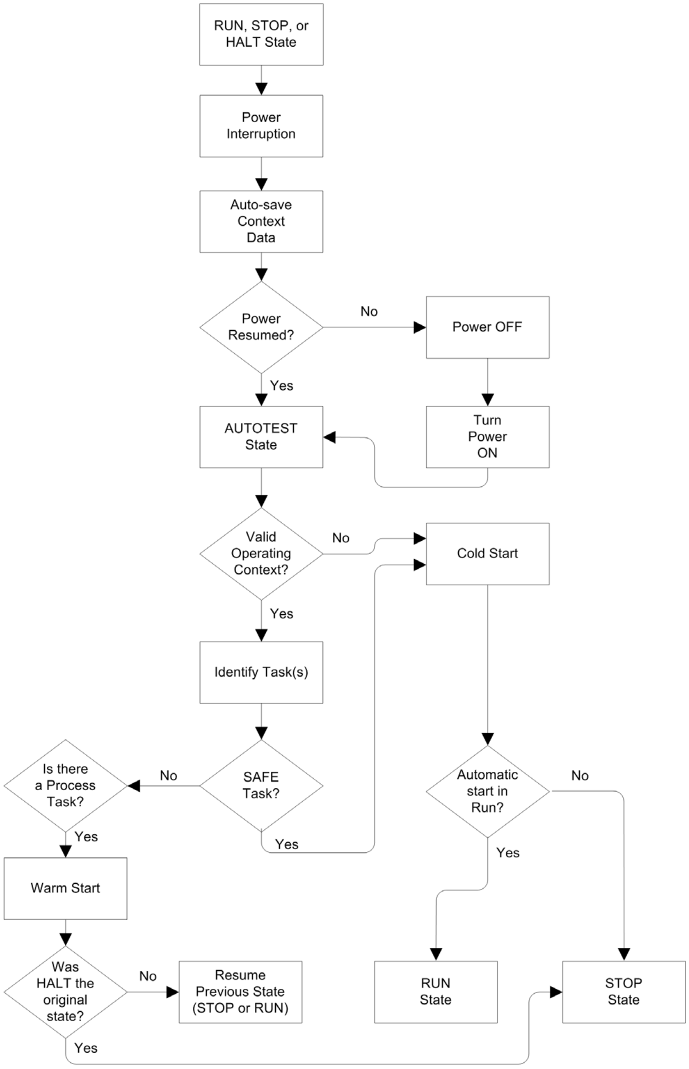
After power down, the start-up can be either automatic (if power was restored before completion of the shut-down) or manual (if not).

Next, the M580 safety PAC performs self-tests and checks the validity of the operating context data that was saved at power down, as follows:

- The application check sum is verified.
- The SD memory card is read to confirm that is contains a valid application.
- If the application in the SD memory card is valid, the signatures are checked to confirm they are identical.
- The saved application signature is verified by comparing it to the stored application signature.

If the operating context is valid, the non-safe tasks perform a warm start. If the operating context is not valid, the non-safe tasks perform a cold start. In either case, the SAFE task performs a cold start.

This start-up sequence after a power interruption is presented, below:



Cold Start

A cold start causes all tasks, including both the SAFE task and the non-safe (MAST, FAST, AUX0, AUX1) tasks, enter the STOP state, unless **Automatic start in RUN** is enabled, in which case all tasks enter the RUN state.

A cold start performs the following operations:

- Application data (including internal bits, I/O data, internal words, and so forth) are assigned the initial values defined by the application.
- Elementary functions are set to their default values.
- Elementary function blocks and their variables are set to their default values.
- System bits and words are set to their default values.
- Initializes all forced variables by applying their default (initialized) values.

A cold start can be executed for data, variables and functions in the process namespace by selecting **PLC → Init** in Control Expert *(see page 140)*, or by setting the system bit %S0 (COLDSTART) to 1. The %S0 system bit has no effect on the data and functions belonging to the safe namespace.

NOTE: Following a cold start, the SAFE task cannot start until after the MAST task has started.

Warm Start

A warm start causes each process task – including the (MAST, FAST, AUX0, AUX1) tasks – to re-enter its operating state as of the time of the power interruption. By contrast, a warm start causes the SAFE task to enter the STOP state, unless **Automatic start in RUN** is selected.

NOTE: If a task was in the HALT state or in breakpoint at the time of power interruption, that task enters the STOP state after the warm start.

A warm start performs the following operations:

- Restores the last held value to process namespace variables.
- Initializes safe namespace variables by applying their default (initialized) values.
- Initializes all forced variables by applying their default (initialized) values.
- Restores the last held value to application variables.
- Sets %S1 (WARMSTART) to 1.
- Connections between the PAC and CPU are reset.
- I/O modules are re-configured (if necessary) using their stored settings.
- Events, the FAST task, and the AUX tasks are disabled.
- The MAST task is re-started from the beginning of the cycle.
- %S1 is set to 0 at the conclusion of the first execution of the MAST task.
- Events, the FAST task, and the AUX tasks are enabled.

If a task was in the process of execution at the time of power interruption, after warm start the task resumes execution at the beginning of the task.

⚠ WARNING

UNEXPECTED EQUIPMENT OPERATION

You are responsible to confirm that selecting **Automatic start in RUN** is compliant with the correct behavior of your system. If it is not, de-activate this feature.

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

M580 Safety PAC Tasks

Introduction

An M580 safety PAC can execute single-task and multi-task applications. Unlike a single-task application which only executes the MAST task, a multi-task application defines the priority of each task.

The M580 safety PAC supports the following tasks:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Task Characteristics

The tasks supported by the M580 safety PAC present the following task characteristics:

Task Name	Priority	Time Model	Period Range	Default Period	Watchdog Range	Default Watchdog
FAST	1	Periodic	1...255 ms	5 ms	10...500 ms[2]	100 ms[2]
SAFE	2	Periodic	10...255 ms	20 ms	10...500 ms[2]	250 ms[2]
MAST[1]	3	Cyclic[4] or Periodic	1...255 ms	20 ms	10...1500 ms[2]	250 ms[2]
AUX0[3]	4	Periodic	10...2550 ms	100 ms	100...5000 ms[2]	2000 ms[2]
AUX1[3]	5	Periodic	10...2550 ms	200 ms	100...5000 ms[2]	2000 ms[2]

1. MAST task is required and cannot be deactivated.
2. If CCOTF is enabled (by selecting **Online modification in RUN or STOP** in the **Configuration** tab of the CPU properties dialog), the minimum **Watchdog** setting is 64 ms.
3. Supported by standalone BMEP58•040S safety PACs. Not supported by BMEH58•040S safety Hot Standby PACs.
4. Standalone BMEP58•040S safety PACs support both cyclic and periodic time models. BMEH58•040S safety Hot Standby PACs support only the periodic time model.

Task Priority

M580 Safety PACs execute pending tasks according to their priority. When a task is running, it can be interrupted by another task with a higher relative priority. For example, when a periodic task is scheduled to execute its code, it would interrupt a lower priority task, but would wait until the completion of a higher priority task.

Task Configuration Considerations

All the non-safe tasks (MAST, FAST, AUX0, and AUX1) operate in the same memory area, while the SAFE task operates in its own, separate memory area. As a result:

- If one non-safe task exceeds its watchdog, all non-safe tasks enter HALT state, while the SAFE task continues to be operational.
- If the SAFE task exceeds its watchdog, only the SAFE task enters HALT state, while the non-safe tasks continue to be operational.

When creating and configuring tasks for your application, consider the following task features:

SAFE task:

Design this periodic task to execute only safety-related code sections for safety I/O modules. Because the SAFE task is assigned a lower priority than the FAST task, execution of the SAFE task may be interrupted by the FAST task.

Define the maximum execution time for the SAFE task by setting the appropriate watchdog value. Consider the time required to execute code and to read and write safe data. If the time to execute the SAFE task exceeds the watchdog setting, the SAFE task enters HALT state, and the %SW125 system word displays the detected error code 16#DEB0.

NOTE:

- Because FAST task has a higher priority than the SAFE task, you may want to include a component for FAST task delay time in the SAFE task watchdog setting.
- If the overrun of the SAFE task execution equals the “Safety watchdog” (which is a value equal to one and one-half times the SAFE task watchdog setting), the CPU and Copro will enter the ERROR state and the safety function will be applied.

MAST task:

This task can be configured as either cyclic or periodic. When operating in cyclic mode, define a maximum execution time by inputting an appropriate MAST watchdog value. Add a small time interval to this value at the end of each cycle to allow for the execution of other lower priority system tasks. Because the AUX tasks carry a lower priority than MAST, if this time slot is not provided, the AUX tasks may never be executed. Consider adding a time interval equal to 10% of cycle execution time, with a minimum of 1 ms and a maximum of 10 ms.

If the time to execute a cyclic MAST task exceeds the watchdog setting, the MAST task and all other non-SAFE tasks enter HALT state, and the %SW125 system word displays the detected error code 16#DEB0.

When operating in periodic mode, it is possible for the MAST task to exceed its period. In that case the MAST task runs in cyclic mode and the system bit %S11 is set.

FAST task:

The purpose of this periodic task is to execute a high-priority part of the application. Define a maximum execution time by setting the FAST watchdog value. Because the FAST task interrupts execution of all other tasks – including the SAFE task – it is recommended to configure the execution time of the FAST task to be as short as possible. A FAST task watchdog value not much greater than the FAST period is recommended.

If the time to execute the FAST task exceeds the watchdog setting, the FAST task and all other non-SAFE tasks enter HALT state, and the %SW125 system word displays the detected error code 16#DEB0.

AUX tasks:

AUX0 and AUX1 are optional periodic tasks. Their purpose is to execute a low priority part of the application. The AUX tasks are executed only after execution of the MAST, SAFE and FAST tasks has finished.

Define a maximum execution time for the AUX tasks by setting the appropriate watchdog value. If the time to execute an AUX task exceeds the watchdog setting, the AUX task and all other non-SAFE tasks enter HALT state, and the %SW125 system word displays the detected error code 16#DEB0.

Section 8.3
Building an M580 Safety Project

What Is in This Section?

This section contains the following topics:

Building an M580 Safety Project

Building an M580 Safety Project

The Control Expert for Safety **Build** menu presents three different build commands, and a Safe Signature command, as follows:

Command	Description
Build Changes	Compiles only the changes that have been made to the application program since the previous build command, and adds them to the previously generated application program.
Rebuild All Project	Re-compiles the entire application program, replacing the previously generated build of the application program. **NOTE:** For M580 safety I/O modules, this command does not generate a new module unique identifier (MUID) value. Instead, the previously generated MUID value is retained.
Renew Ids & Rebuild All	Re-compiles the entire application program, replacing the previously generated build of the application program. **NOTE:** ● Execute this command only when the safety I/O modules are unlocked *(see page 138)*. ● For M580 safety I/O modules, this command generates a new module unique identifier (MUID) value and replaces the existing MUID value with the new value.
Update Safe Signature	Use this to manually generate a SourceSafeSignature *(see page 131)* value for the safe application. **NOTE:** This command is enabled only when the **General** → **Build Settings** → **Safe Signature management** parameter is set to **On user request**.

Safe Signature

Introduction

M580 safety PACs - both standalone and Hot Standby - include a mechanism for producing an SHA256 algorithmic fingerprint of the safe application: the SourceSafeSignature. When transferring the application from the PC to the PAC, Control Expert compares the SourceSafeSignature in the PC with the SourceSafeSignature in the PAC to determine if the safe application in the PC is the same as, or different from the safe application in the PAC.

The safe signature feature is optional. Generating a SourceSafeSignature can be a time-consuming process, depending on the size of the safe application. Using the safe signature management options, you can generate a SourceSafeSignature value that creates an algorithmic value for your safe application

- on every build, or
- only when you want to manually generate a SourceSafeSignature and add it to the most recent build, or
- not at all

Actions that Change the SourceSafeSignature

Both configuration edits and variable value changes can cause the SourceSafeSignature to change.

Configuration changes: The following configuration actions lead to a signature change:

Device	Action
Safety CPU	Change CPU reference via **Replace Processor...**
	Change CPU version via **Replace Processor...**
	Edit any parameter on the CPU **Configuration** or **Hot Standby** configuration tabs.
	Edit any parameter on any tab of the CPU Ethernet Communicator Head (**Security**, **IP Config**, **RSTP**, **SNMP**, **NTP**, **ServicePort**, **Safety** ..).
Safety Coprocessor	Not applicable, as the coprocessor is not configurable.
Other Safety Module	**Add**/**Delete**/**Move** a module, either: ● Directly (via command) ● Indirectly (for example, by replacing an 8-slot Ethernet backplane - with a safety module in slot 7 - with a 4-slot Ethernet backplane, thereby deleting a module)
	Edit of any safety module parameter, located on the **Configuration** tab (for example **Short circuit to 24V detection**, **Open wire detection**) and on the left pane of the editor (for example **Function**, **Fallback**).
	Modification of module ID via **Renew Ids and Rebuild All** command.
	Modification of Device DDT instance name.

Device	Action
CIP Safety Module	**Add/Delete** a module.
	Modification of any CIP Safety module parameter in either the CIP Safety device DTM editor, or the **Device List** of the CPU master DTM editor.
	Modification of Device DDT instance name.
Safety Power Supply	**Add/Delete** a safety power supply.
Other Safety-Related Equipment	Modification of any topological address of equipment supporting a safety device, for example: ● Move a rack containing a safety device. ● Move a bus or drop containing a safety device.

Value Changes: Except as noted, the following items are included in the SourceSafeSignature computation. A change to their values causes a SourceSafeSignature change:

Type	Items
Program	SAFE task and related code sections.
Variables	All safe area variables and their attributes.
DDTs	Each safe DDT attribute, except date and version attributes.
	The variables inside each DDT, including their attributes.
	The safe DDTs, even if they are not used in the safe application.
DFBs	Each safe DFB attribute, except date and version attributes.
	The variables inside each DFB, including their attributes.
	The safe DFBs, even if they are not used in the safe application.
Safe Scope Settings	All **Project Settings** for **Scope** = safe.
1. These variables are not exported, but any change to their values change the configuration partial signature.	

Type	Items
Common Scope Settings	The following **Project Settings** for **Scope** = common:
	Variables ● Allow leading digits ● Character set ● Allow usage of EBOOL edge ● Allow INT/DINT in place of ANY_BIT ● Allow bit extraction of INT, WORD and BYTE ● Directly represented array variables ● Enable fast scanning for trending ● Force references initialization
	Program → Languages → Common ● Allow procedures ● Allow nested comments ● Allow multi assignment [a:=b:=c] (ST/LD) ● Allow empty parameters in non-formal call (ST/IL) ● Maintain output links on disabled EF (EN=0) ● Display complete comments of structure element
	Program → Languages → LD ● Single scan edge detection for EBOOL
	General → Time[1] ● Custom TimeZone ● Time Zone ● Time Offset ● Automatically adjust clock for daylight saving ❍ All START and END settings under Automatically adjust clock for daylight saving

[1] These variables are not exported, but any change to their values change the configuration partial signature.

Managing the SourceSafeSignature

The SourceSafeSignature is managed in Control Expert in the **Tools → Project Settings** window, by selecting **General → Build Settings**, then selecting one of the following **Safe Signature management** settings:

- **Automatic** (default): generates a new SourceSafeSignature every time a **Build** command is executed.
- **On user request**: generates a new SourceSafeSignature when the **Build → Update Safe Signature** command is executed.

NOTE: If you select **On user request**, Control Expert generates a SourceSafeSignature value of 0 on every build. If you do not execute the **Build → Update Safe Signature** command, you are electing not to use the Safe Signature feature.

Transferring an Application from the PC to the PLC

When you download an application from the PC to the PAC, Control Expert compares the SourceSafeSignature in the downloaded application with one in the PAC. Control Expert behaves as follows:

New Safe Signature	PAC Safe Signature	Control Expert Displays
Any	No application	Transfer confirmation
Any (except 0)	0	Transfer confirmation
0	0	Transfer confirmation
0	Any (except 0)	Transfer confirmation; Followed by a notice “This will reset the Safe Signature”; Followed by a new transfer confirmation
XXXX = YYYY[2]	YYYY	Transfer confirmation
XXXX ≠ YYYY[3]	YYYY	Transfer confirmation; Followed by a notice “This will modify the Safe Signature”; Followed by a new transfer confirmation

1. The value “0” indicates a SourceSafeSignature was not generated automatically or manually.
2. The safe application in the PC (XXXX) and the safe application in the PAC (YYYY) are EQUAL.
3. The safe application in the PC (XXXX) and the safe application in the PAC (YYYY) are DIFFERENT.

Viewing the SourceSafeSignature

When used, each SourceSafeSignature consists of a series of hexadecimal values, and can be very long, which makes direct readings and comparisons of the value very difficult for a human user. However, it is possible to copy a SourceSafeSignature value and paste it into an appropriate text tool to make comparisons. The SourceSafeSignature value can be found in the following Control Expert locations:

- **Properties of Project** → **Identification** tab: In the **Project Browser**, right click on **Project** and select **Properties**.
- **PLCScreen** → **Information** tab *(see EcoStruxure™ Control Expert, Operating Modes)*: In the **Project Browser**, navigate to **Project** → **Configuration** → **PLC bus** → **<CPU>**, right-click and select **Open**, then select the **Animation** tab.
- **PC < - - > PLC Comparison** dialog *(see EcoStruxure™ Control Expert, Operating Modes)*: Select this command from the **PLC** menu.
- **Transfer Project to PLC** dialog: Select this command from the **PLC** menu (or in the **PC < - - > PLC Comparison** dialog.

Comparing the SourceSafeSignature and the SAId

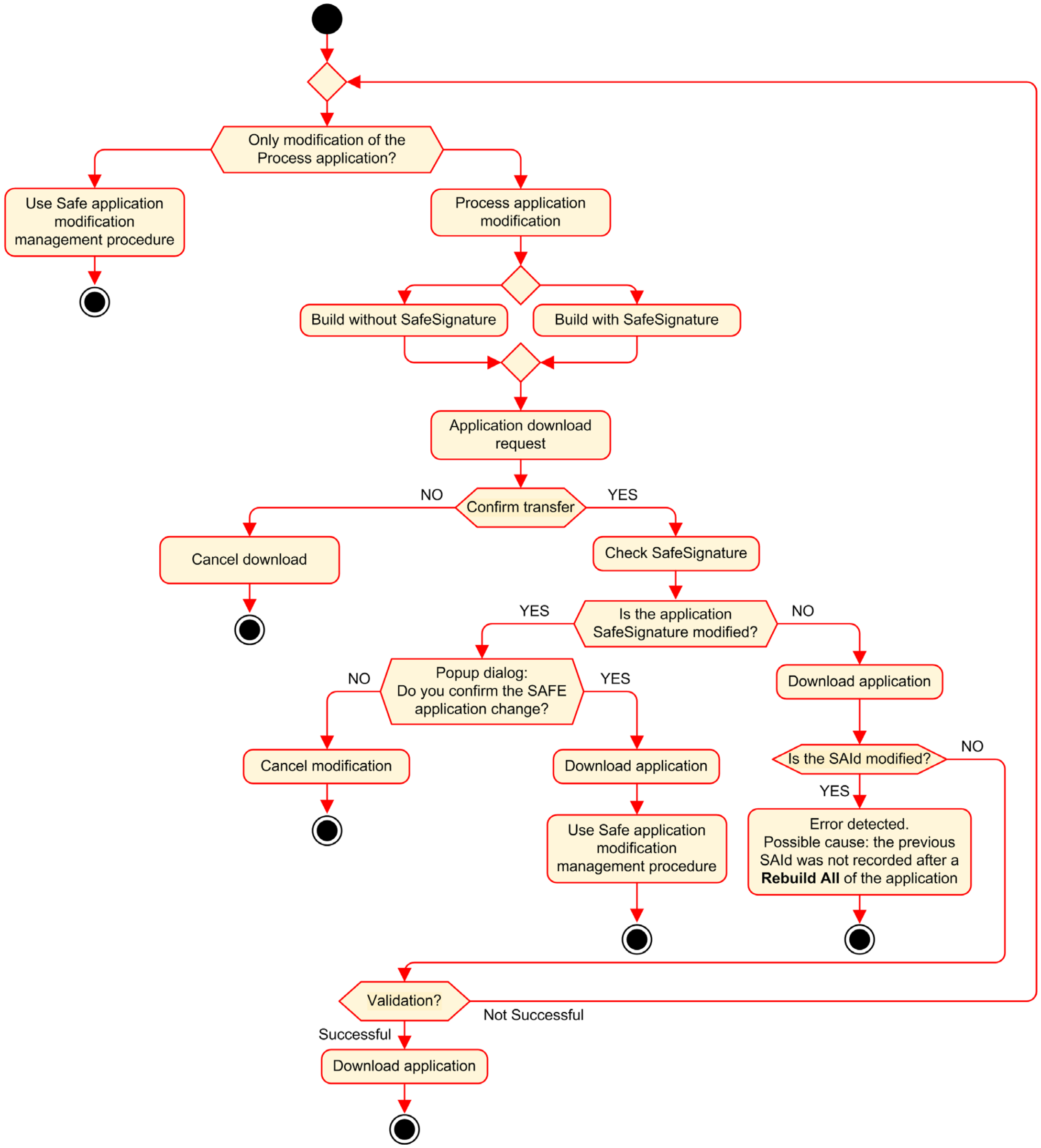
The SourceSafeSignature was introduced to provide an *a priori* verification that the safe application is unchanged. It is recommended to use this feature each time the process application is modified *(see page 136)* to avoid unintended modification of the safe application.

The SourceSafeSignature is a reliable mechanism, but is not sufficient for safety applications because the same source code may correspond to different binary (executable) codes, depending on the kind of build used after the last modification of the safe code.

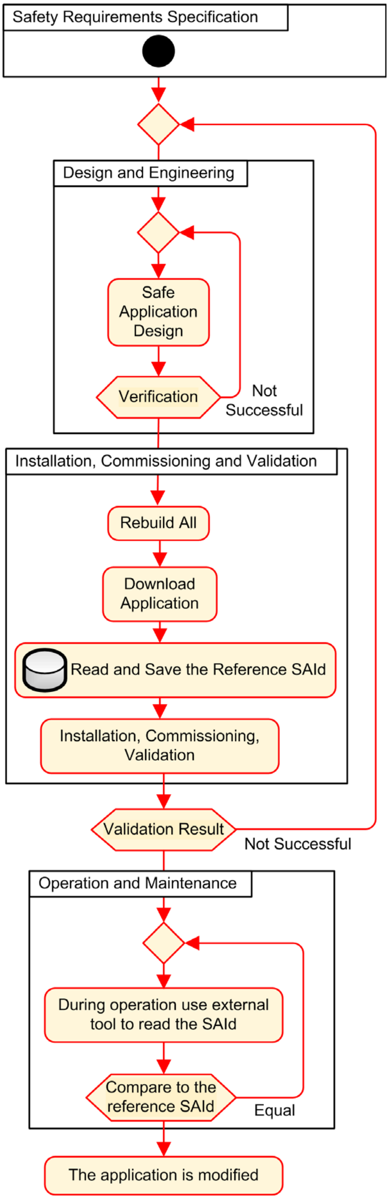
The SAId can be evaluated only at run time. Its calculation is double executed and compared by both the CPU and the COPRO, based on the binary code that is executed by the safe application. Because the SAId is sensitive to all modifications, including those that may be introduced by a **Rebuild All** command after a build change, it is recommended that you use a **Rebuild All** command to generate a reference version of the safe application. This process *(see page 137)* lets you use any form of build (**Rebuild All**, **Build Changes** online or offline) for the process application changes without any change made to the SAId.

The SAId is the recommended method used to confirm that the safe application is the one that was validated. The SAId value is not automatically tested by the application. For this reason, it is recommended that you regularly verify the SAId by any convenient mean (for example, using Control Expert or an HMI) by reading the output of the S_SYST_STAT_MX function block or the content of system word %SW169 *(see page 204)*.

Modification of the Process Application Simplified Process


Only modification of the Process application?
Use Safe application modification management procedure
Process application modification
Build without SafeSignature
Build with SafeSignature
Application download request
NO
Confirm transfer
YES
Cancel download
Check SafeSignature
YES
Is the application SafeSignature modified?
NO
NO
Popup dialog: Do you confirm the SAFE application change?
YES
Download application
Cancel modification
Download application
Is the SAId modified?
NO
YES
Use Safe application modification management procedure
Error detected. Possible cause: the previous SAId was not recorded after a **Rebuild All** of the application
Validation?
Not Successful
Successful
Download application

SAId Management


Safety Requirements Specification
Design and Engineering
Safe Application Design
Verification
Not Successful
Installation, Commissioning and Validation
Rebuild All
Download Application
Read and Save the Reference SAId
Installation, Commissioning, Validation
Validation Result
Not Successful
Operation and Maintenance
During operation use external tool to read the SAId
Compare to the reference SAId
Equal
The application is modified

Section 8.4
Locking M580 Safety I/O Module Configurations

Locking M580 Safety I/O Module Configurations

Locking a Safety I/O Module Configuration

Each safety I/O module has a configuration locking button *(see page 67)*, which you can find at the top front of the module. The purpose of the locking function is to help prevent unintended changes to I/O module configuration. For example, locking the I/O module's current configuration can stop an attempt to assign the module a fake configuration, or merely help protect against configuration mistakes.

To achieve the intended safety integrity level (SIL), lock each safety I/O module after it has been configured, but before you begin or resume operations.

⚠ WARNING

RISK OF UNINTENDED DEGRADATION TO PROJECT SAFETY INTEGRITY LEVEL

You must lock each safety I/O module after it is configured but before beginning operations.

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

The lock and unlock mechanisms work as follows:

- To lock a safety I/O module configuration, press and hold down the lock button for more than 3 seconds, then release the button.
- To unlock a safety I/O module configuration, press and hold down the lock button for more than 3 seconds, then release the button.

Scenarios for Locking Safety I/O Module configurations

The procedure you follow to lock the configuration of SIL3 safety I/O modules will vary, depending on the scenario, which can be:

- First configuration of the I/O modules
- Fast device replacement of I/O modules
- Perform a change configuration on the fly (CCOTF) for I/O modules

The procedure for each scenario is described below.

First configuration of SIL3 I/O safety modules:

Step	Action
1	Connect Control Expert to the M580 safety PAC.
2	Use the **Transfer project from PLC** command to load the project from the PAC into Control Expert.
3	In the **PLC bus** window in Control Expert, open each SIL3 safety I/O module and confirm that each module is accurately configured.
4	In an animation table in Control Expert, view the DDDT for each SIL3 safety I/O module and confirm that the configuration of each module is the same as in step 3, above.
5	Lock the configuration of each SIL3 I/O module by pressing and holding down the configuration locking button *(see page 67)* for more than 3 seconds, then release the button.
6	Check in an animation table the validity of the lock bit status (CONF_LOCKED) for each SIL3 I/O module.

Fast device replacement of a SIL3 I/O safety module:

Step	Action
1	Replace the SIL3 safety I/O module with a new one.
2	Connect Control Expert to the M580 safety PAC in maintenance operating mode *(see page 113)*.
3	In the **PLC bus** window in Control Expert, open each SIL3 safety I/O module and confirm that each module is accurately configured.
4	In an animation table in Control Expert, view the DDDT for each SIL3 safety I/O module and confirm that the configuration of each module has not changed and is the same as in step 3, above.
5	Lock the configuration of each SIL3 I/O module by pressing and holding down the configuration locking button *(see page 67)* for more than 3 seconds, then release the button.
6	Check in an animation table the validity of the lock bit status (CONF_LOCKED) for each SIL3 I/O module.

Performing CCOTF to add a new SIL3 I/O safety module:

Step	Action
1	Connect Control Expert to the M580 safety PAC in maintenance operating mode *(see page 113)*.
2	Add a new SIL3 safety I/O module to the configuration, and edit the module settings if necessary.
3	Execute the **Build** → **Build Changes** command.
4	In the **PLC bus** window in Control Expert, open each SIL3 safety I/O module and confirm that each module is accurately configured.
5	In an animation table in Control Expert, view the DDDT for each SIL3 safety I/O module and confirm that the configuration of each module has not changed and is the same as in step 3, above.
6	Lock the configuration of each SIL3 I/O module by pressing and holding down the configuration locking button *(see page 67)* for more than 3 seconds, then release the button.
7	Check in an animation table the validity of the lock bit status (CONF_LOCKED) for each SIL3 I/O module.
8	In the **PLC** menu of Control Expert, command the PAC to enter safety mode *(see page 112)*.

Section 8.5
Initializing Data in Control Expert

Initializing Data in Control Expert for the M580 Safety PAC

Two Init Commands

The **PLC** menu in Control Expert provides two separate commands for the initialization of data:

- The **Init** command initializes data for the process (or non-safe) namespace, which can be used by the MAST, FAST, AUX0 and AUX1 tasks. You can execute this command if the PAC is operating in either safety or maintenance mode while the PAC is in the STOP state. This command is the equivalent of setting the system bit %S0 (COLDSTART) to 1.
  NOTE: Setting the %S0 bit to 1 initializes data in the process namespace only. It does not affect data in the safe namespace.
- The **Init Safety** command initializes data only for the safe namespace, which data can be used exclusively by the SAFE task. You can execute this command only if the SAFE task is operating in maintenance mode while the SAFE task is in the STOP or HALT state. Executing this command when the SAFE task is in the HALT state causes the SAFE task to restart in the STOP state.

Both the **Init** and the **Init Safety** commands perform a cold start. *(see page 124)*

Section 8.6
Working with Animation Tables in Control Expert

Animation Tables and Operator Screens

Introduction

A M580 safety PAC supports three kinds of animation tables, each associated with one of the following data areas:

- Process area animation tables can include only data in the process namespace.
- Safety area animation tables can include only data in the safe namespace.
- Global animation tables can include data for the entire application, including data created for the safe and process namespaces, and global variables.
  NOTE: In a global animation table, data variable names include a prefix indicating the source namespace, as follows:

- A data variable from the Safe namespace is displayed as “SAFE.<varname>”.
- A data variable from the Process namespace is displayed as “PROCESS.<variable name>”.
- A data variable from the Global (or Application) namespace displays only its <variable name>, with no namespace prefix.

Both process and safety data from an M580 safety PAC are also accessible by external processes (for example, SCADA or HMI).

Your ability to create and modify an animation table, and the ability to execute animation table functions, depend on the namespace of the affected variables and the operating mode of the safety project.

Conditions for Creating and Editing Animation Tables

Creating and editing animation tables involves adding or deleting data variables. Your ability to add data variables to, or delete data variables from an animation table depends on:

- The namespace (safe or process) in which the data variable resides.
- The operating mode (safety or maintenance) of the M580 safety PAC.

When Control Expert is connected to the M580 safety PAC, you can create and edit animation tables as follows:

- Adding process namespace variables to, or deleting process namespace variables from a process or global animation table is supported while the M580 safety PAC is operating in either safety mode or maintenance mode.
- Adding safe namespace variables to, or deleting safe namespace variables from a safety animation table is supported while the M580 safety PAC is operating in maintenance mode.
- Adding safe namespace variables to, or deleting safe namespace variables from a safety animation table is supported while the M580 safety PAC is operating in safety mode only if the project settings do not include animation tables in the upload information.

NOTE: Animation tables are included in, or excluded from, upload information in Control Expert by selecting **Tools → Project Settings...** to open the **Project Settings...** window, then navigating to **Project Settings → General → PLC embedded data → Upload information → Animation tables**.

Conditions for Operating Animation Tables

You can use animation tables to force a variable value, unforce a variable value, modify a single variable value, or modify multiple variable values. Your ability to perform these functions depends on the namespace in which a variable resides and the operating mode of the M580 safety PAC, as follows:

- Process or global variable values can be read or written in both safety operating mode and maintenance operating mode.
- Safety variable values can be read or written in maintenance operating mode.
- Safety variable values can only be read in safety operating mode.

Process for Creating Animation Tables in the Safety or Process Namespace in Control Expert

Control Expert provides two ways to create animation tables for either the safety or process namespace:

- From a safety or process code section window, right click in the code window, then select either:
  - **Initialize Animation Table** to add the data object to an existing animation table in safety or process namespace, or
  - **Initialize New Animation Table** to add the data object to a new animation table in the safety or process namespace.

  In each case, all the variables in the code section are added to the existing or new animation table.
- From the **Project Browser**, in either the process or safety data area, right click on the **Animation Tables** folder, then select **New Animation Table**. Control Expert creates a new, empty animation table. You can then add individual variables from the namespace (safety or process) related to the table.

Process for Creating Globally Scoped Animation Tables

Create a global animation table in the **Project Browser** by right clicking the global **Animation Tables** folder, then selecting **New Animation Table**. You can add variables to the new animation table in several ways:

- *Drag and drop*: You can drag a variable from a data editor and drop it into the global animation table. Because the scope of the animation table includes the entire application, you can drag the variable from the **Safety Data Editor**, the **Process Data Editor**, or the **Global Data Editor**.
- *Instance Selection dialog*: You can double-click in a row in the animation table, then click the ellipsis button to open the **Instance Selection** dialog. Use the filtering list in the top right part of the dialog to select a one of the following project areas:

  - ❍ SAFE: to display data objects associated with the safety area.
  - ❍ PROCESS: to display data object associated with the process area.
  - ❍ APPLICATION: to display higher-level application scope data objects.

  Select a data object, then click **OK** to add the item to the animation table.

NOTE: Data objects added to a global animation table from the:
- Process area have the prefix “PROCESS” affixed to the variable name (for example PROCESS.variable_01
- Safety area have the prefix “SAFE” affixed to the variable name (for example SAFE.variable_02
- Global area have no such prefix added to the variable name.

Displaying Data on Operator Screens

You can display data on an operator screen – such as an HMI, SCADA or FactoryCast application – in the same way that you link to data in an animation table. The data variables available for selection are those variables that are included in the Control Expert data dictionary.

You can enable the data dictionary by opening the **Tools** → **Project Settings...** window, then in the **Scope** → **common** area of the window, selecting **General** → **PLC embedded data** → **Data dictionary**.

The data dictionary makes data variables available to operator screens as follows:
- Safe namespace variables always include the “SAFE” prefix, and can be reached only by using the format “SAFE.<variable name>”.
- Global or application namespace variables do not include a prefix, and can be reached only by using the “<variable name>” without a prefix.
- The **Usage of Process Namespace** setting determines how an operator screen can reach Process namespace variables.
  - ❍ If you select **Usage of Process Namespace**, the operator screen can read process area variables only by using the format “PROCESS.<variable name>”.
  - ❍ If you de-select **Usage of Process Namespace**, the operator screen can read process area variables only by using the format “<variable name>” without the PROCESS prefix.
    NOTE: If two variables are declared with the same name, one in the Process namespace and one in the Global namespace, only the variable from the Global Namespace is accessible by an HMI, SCADA, or Factory Cast application.

You can use the **Instance Selection** dialog to access individual data objects.

⚠ CAUTION

UNEXPECTED VARIABLE VALUE

- Be sure that your application has the correct project settings.
- Verify the syntax to access the variables in the different namespaces.

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

To prevent from accessing the incorrect variable:

- Use different names for the variables you declare in the Process namespace and in the Global namespace, or
- select **Usage of Process Namespace** and use the following syntax to access the variables with the same name:
  - “PROCESS.<variable name>” for variables declared in the Process namespace.
  - “<variable name>” without a prefix for variables declared in the Global namespace

Trending Tool

The Control Expert Trending Tool is not supported for use with an M580 safety project.

Section 8.7
Adding Code Sections

What Is in This Section?

This section contains the following topics:

Adding Code to an M580 Safety Project

Working with Tasks in Control Expert

In the process namespace, Control Expert includes the MAST task by default. The MAST task cannot be removed. However, you can add the tasks FAST, AUX0, and AUX1. Note that creating a task in the process part of a safety project is the same as creating a task in a non-safety project. Refer to the topic *Create and Configure a Task (see EcoStruxure ™ Control Expert, Operating Modes)* in the *EcoStruxure ™ Control Expert Operating Modes* manual for more information.

In the safe namespace, Control Expert includes the SAFE task by default. The SAFE task cannot be removed, and no other tasks can be added to the **Program Safety** section of the **Project Browser** in Control Expert. You can add multiple sections to the SAFE task.

Configuring the SAFE Task Properties

The SAFE task supports only periodic task execution (cyclic execution is not supported). Both the SAFE task **Period** and **Watch Dog** settings are input in the **Properties of SAFE** dialog and can support the following value range:

- SAFE task period: 10...255 ms with a default of 20 ms.
- SAFE task watchdog: 10...500 ms, in increments of 10 ms, with a default of 250 ms.

Set the SAFE task **Period** to a minimum value depending on the safe data size and the PLC model. The minimum SAFE task period can be calculated according to the following formulas:

- Absolute minimum necessary for safe I/O communication:
  - 10 ms
- Time (in ms) necessary to transfer and compare the safe data between the CPU and the COPRO:
  - (0.156 x Data_Safe_Size) + 2 ms (for BMEP584040S, BMEH584040S, and BMEH586040S)
  - (0.273 x Data_Safe_Size) + 2 ms (for BMEP582040S and BMEH582040S)

  Where the Data_Safe_Size is the size in Kbytes of the safe data.
- Additional time (in ms) needed by Hot Standby PACs to transfer the safe data from the primary PAC to the standby PAC:
  - (K1 x Task_{kb} + K2 x Task_{DFB}) / 500

  In this formula:
  - Task_{DFB} = the number of DFBs declared in the safe part of the application.
  - Task_{kb} = the size (in Kbytes) of the safe data exchanged by the SAFE task between the primary and standby PACs.
  - K1 and K2 are constants, with values determined by the specific CPU module used in the application:

Coefficient	BMEH582040S	BMEH584040S, and BMEH586040S
K1	32.0	10.0
K2	23.6	7.4

NOTE:

- The value produced by these formulas is an absolute minimum for the SAFE task period valuable only for a first estimation of the SAFE cycle time limit. It does not include the time necessary for user code execution or for the margin necessary for the intended operation of the PAC multi-task system. Refer to the topic System Throughput Considerations in the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures*.
- By default, Data_Safe_Size and $\text{Size}_{\text{kbytes}}$ are equal. Their values can be viewed, respectively, in the **PLC → Memory Consumption** menu and the **PLC → Hot Standby** screen.

Example Calculations

Sample results of calculating the minimum SAFE task period are set forth below

Minimum Safe Task Period (ms)					
$\text{Size}_{\text{kbytes}}$[1]	$\text{Nb}_{\text{DFB\_Inst)}}$	BMEP582040S	BMEP584040S	BMEH582040S	BMEH584040S or BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29
200	10	57	33	70	37
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179
1. $\text{Size}_{\text{kbytes}}$ and Data_Safe_Size are assumed to be equal.					

NOTE: Configure the SAFE task watchdog with a value that is greater than the SAFE task **Period**.

Refer to the topic *Process Safety Time (see Modicon M580, Safety Manual)*, for information regarding how the SAFE task configuration affects process safety time.

Refer to the topic *M580 Safety PAC Tasks (see page 126)* for information describing the execution priority of the SAFE task.

Creating Code Sections

Right click on the **Section** folder for a task and select **New Section...** to open a configuration dialog. For the safety and process tasks, the following program languages are available:

Language	Safety tasks	Process tasks			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
LL984 segment	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓: available – : not available					

Except for these limitations on programming language availability for the SAFE task, the new section configuration dialog operates the same as for a non-safety M580 project. Refer to the topic *Properties Dialog Box for FBD, LD, IL, or ST Sections (see EcoStruxure™ Control Expert, Operating Modes)* in the *EcoStruxure™ Control Expert Operating Modes* manual for more information.

Adding Data to Code Sections

Because the SAFE task is separated from the process tasks, only data accessible in the **Safety Data Editor** is available to be added to a SAFE task code section. This data includes:

- Unlocated safety variables (i.e. with no %M or %MW address) created in the **Safety Data Editor**.
- Data objects that are part of M580 safety module device DDT structures.

Similarly, data available to non-safety task code sections includes all data within the scope of the process namespace. This includes all project data except:

- Data exclusively available to the SAFE namespace (see above).
- Data objects created in the **Global Data Editor**.

Code Analysis

When you analyze or build a project, Control Expert displays a detected error message if:

- Data belonging to the process namespace is included in the SAFE task.
- Data belonging to the safe namespace is included in a process task (MAST, FAST, AUX0, AUX1).
- Located bits (%M) or words (%MW) are included in a SAFE task section.

Diagnostic Request

Introduction

The diagnostic request is available only for M580 safety power supplies located on a main rack, using the PWS_DIAG function block. A main rack is one with an address of 0 and a CPU or communication adapter module (CRA) in slot 0 or 1. An extension rack is not a main rack.

The CPU can make a diagnostic request of redundant power supplies on the local rack and, via a communications adapter (CRA), of redundant power supplies on a remote rack. If the master and slave power supplies are operational, the master power supply enters master diagnostic mode and the slave power supply enters slave diagnostic mode. The LEDs indicate the test is ongoing.

NOTE: This request is not implemented when power cycles ON

After the diagnostic test finishes, the master returns to normal operating state and the slave transitions to either normal or error state, depending on the outcome of the tests. Test results are stored in power supply memory,

Diagnostic Request Returned Data

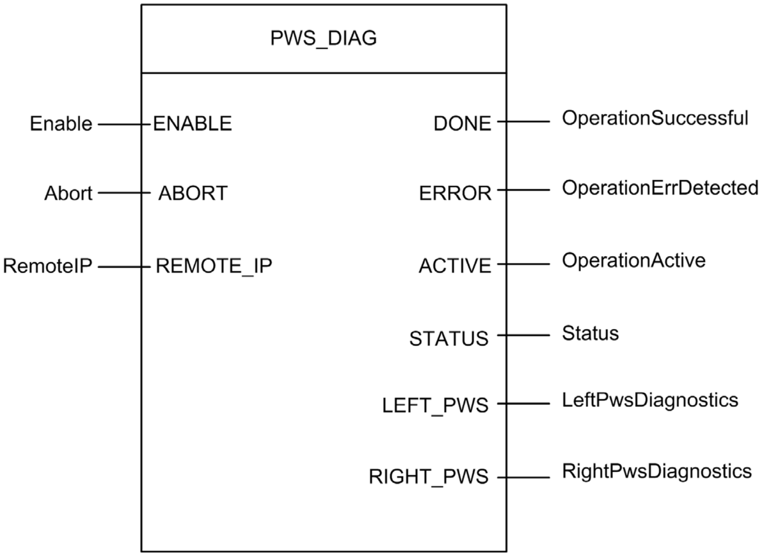
Diagnostic information sent to the CPU by the power supplies includes:

- Power supply ambient temperature.
- Voltage and current on 3.3V backplane line.
- Voltage and current on 24V backplane line.
- Power supply total cumulated energy since manufacturing on the 3.3V and 24V backplane lines.
- Operating time as master since last power-on and manufacture.
- Total operating time as slave since last power-on and manufacture.
- Remaining life time in percent (LTPC): the time before preventive maintenance from 100% to 0%.

  NOTE: No swap when at 0%.
- Number of times power supply has powered ON.

  NOTE: From the SCADA, it is possible to reset the number of power on since installation and all others diagnostics.
- Number of times BMXCPS4002S main voltage fell below under-voltage level 1 (95 Vac).
- Number of times BMXCPS4002S main voltage rises above over-voltage level 2 (195 Vac).
- Number of times BMXCPS4022S main voltage fell below under-voltage level 1 (20 Vdc).
- Number of times BMXCPS4022S main voltage rises above over-voltage level 2 (40 Vdc).
- Number of times BMXCPS3522S main voltage fell below under-voltage level 1 (110 Vdc).
- Number of times BMXCPS3522S main voltage rises above over-voltage level 2 (140 Vdc).
- Current status of the power supply (master/slave/inoperable).

Representation in FBD



Parameters

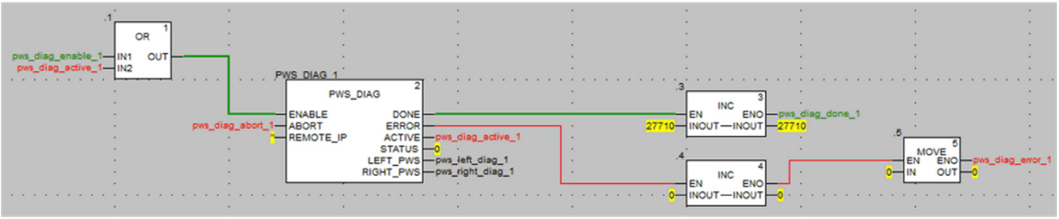
Input Parameters:

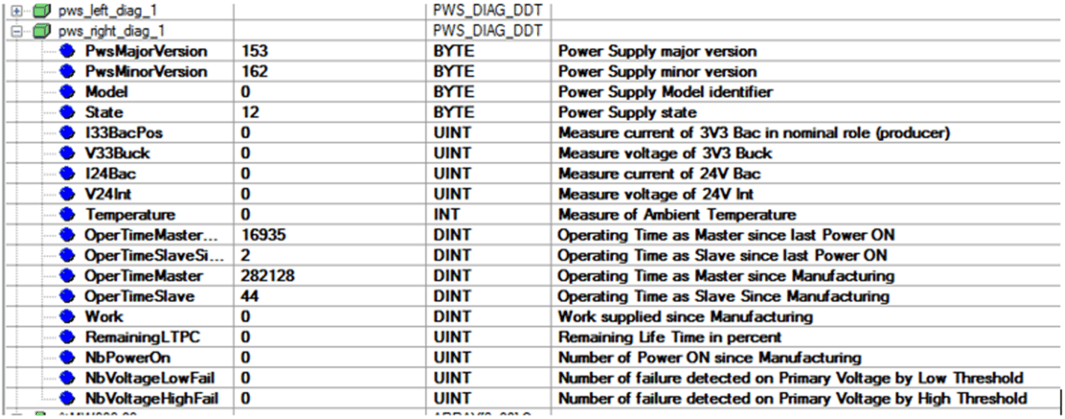
Parameter Name	Data Type	Description
ENABLE	BOOL	When ON, the operation is enabled.
ABORT	BOOL	When ON, the currently active operation is aborted.
REMOTE_IP	STRING	IP Address ("ip1.ip2.ip3.ip4") of the drop that contains the power supply module. Leave this field an empty string ("") or attach no variable to its pin to address the power supply in the local rack.

Output Parameters:

Parameter Name	Data Type	Description
DONE	BOOL	ON when the operation concludes successfully.
ERROR	BOOL	ON when the operation is aborted without success.
ACTIVE	BOOL	ON when the operation is active.
STATUS	WORD	Detected error identifier.
LEFT_PWS	ANY	Diagnostic data for left power supply. Use variable of type PWS_DIAG_DDT_V2 for correct interpretation.
RIGHT_PWS	ANY	Diagnostic data for right power supply. Use variable of type PWS_DIAG_DDT_V2 for correct interpretation.

Example





⊞ pws_left_diag_1		PWS_DIAG_DDT	
⊟ pws_right_diag_1		PWS_DIAG_DDT	
● PwsMajorVersion	153	BYTE	Power Supply major version
● PwsMinorVersion	162	BYTE	Power Supply minor version
● Model	0	BYTE	Power Supply Model identifier
● State	12	BYTE	Power Supply state
● I33BacPos	0	UINT	Measure current of 3V3 Bac in nominal role (producer)
● V33Buck	0	UINT	Measure voltage of 3V3 Buck
● I24Bac	0	UINT	Measure current of 24V Bac
● V24Int	0	UINT	Measure voltage of 24V Int
● Temperature	0	INT	Measure of Ambient Temperature
● OperTimeMaster...	16935	DINT	Operating Time as Master since last Power ON
● OperTimeSlaveSi...	2	DINT	Operating Time as Slave since last Power ON
● OperTimeMaster	282128	DINT	Operating Time as Master since Manufacturing
● OperTimeSlave	44	DINT	Operating Time as Slave Since Manufacturing
● Work	0	DINT	Work supplied since Manufacturing
● RemainingLTPC	0	UINT	Remaining Life Time in percent
● NbPowerOn	0	UINT	Number of Power ON since Manufacturing
● NbVoltageLowFail	0	UINT	Number of failure detected on Primary Voltage by Low Threshold
● NbVoltageHighFail	0	UINT	Number of failure detected on Primary Voltage by High Threshold

Swap and Clear Commands

Introduction

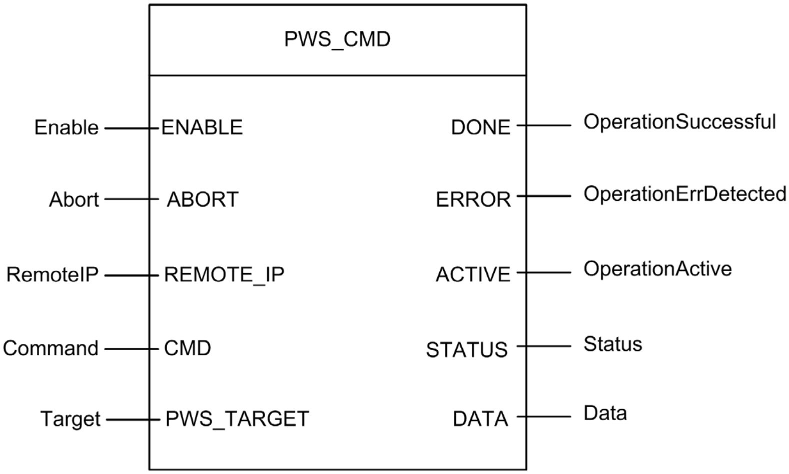
The PWS_CMD function block can be used to issue two commands:

- Swap request: This command specifies the power supply to serve as the master. If both power supplies are operational, the specified power supply becomes the master, the other becomes the slave.
- Clear request: This command resets the counters of the number of times:
  - main voltage fell below under-voltage level 1.
  - main voltage fell below under-voltage level 2.
  - power supply has powered ON.

Both requests are available only for power supplies on the main rack. A main rack is one with an address of 0 and a CPU or communication adapter module (CRA) in slot 0 or 1. An extension rack is not a main rack.

The LEDs indicate the command is ongoing. A record of the event is stored in power supply memory.First paragraph of fact block.

Representation in FBD



Parameters

Input Parameters:

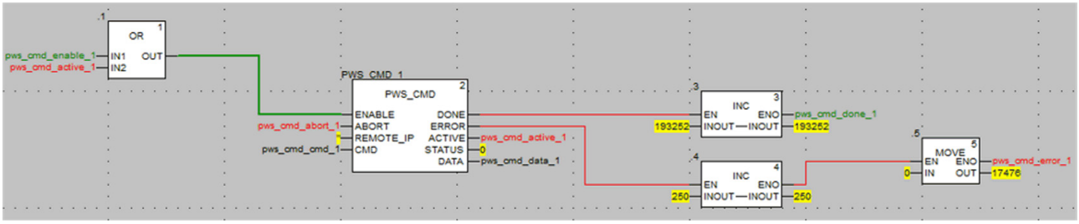
Parameter Name	Data Type	Description
ENABLE	BOOL	When ON, the operation is enabled.
ABORT	BOOL	When ON, the currently active operation is aborted.
REMOTE_IP	STRING	IP Address ("ip1.ip2.ip3.ip4") of the drop that contains the power supply module. Leave this field an empty string ("") or attach no variable to its pin to address the power supply in the local rack.
CMD	ANY	Use variable of type PWS_CMD_DDT for correct interpretation. Available command code: ● 1 = swap ● 3 = clear
PWS_TARGET	BYTE	Power supply to address: ● 1 = left ● 2 = right ● 3 = both

Output Parameters:

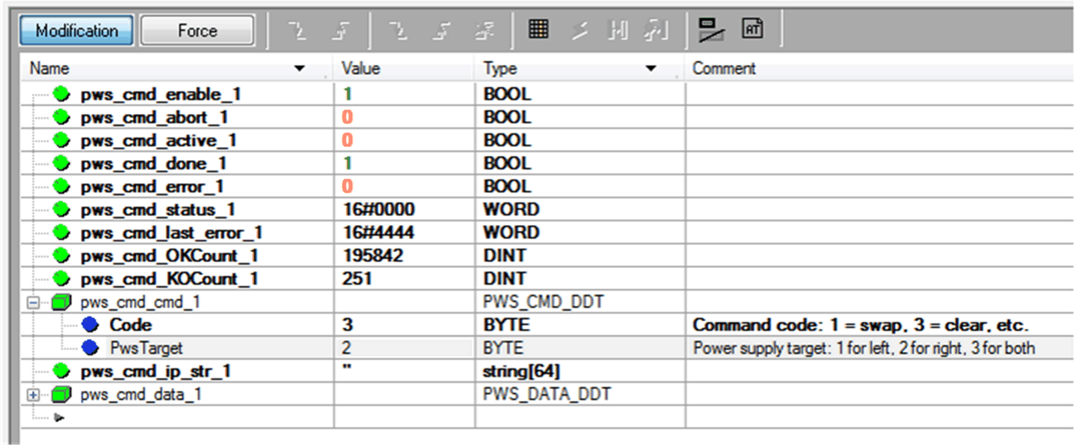
Parameter Name	Data Type	Description
DONE	BOOL	ON when the operation concludes successfully.
ERROR	BOOL	ON when the operation is aborted without success.
ACTIVE	BOOL	ON when the operation is active.
STATUS	WORD	Detected error identifier.
DATA	ANY	Response data (depending of command code). No data are reported for swap and clear commands.

Example

The following diagram demonstrated a PWS_CMD block used for a swap request:



The following data editor screen shows the variable values of a swap request:



Name	Value	Type	Comment
pws_cmd_enable_1	1	BOOL	
pws_cmd_abort_1	0	BOOL	
pws_cmd_active_1	0	BOOL	
pws_cmd_done_1	1	BOOL	
pws_cmd_error_1	0	BOOL	
pws_cmd_status_1	16#0000	WORD	
pws_cmd_last_error_1	16#4444	WORD	
pws_cmd_OKCount_1	195842	DINT	
pws_cmd_KOCount_1	251	DINT	
pws_cmd_cmd_1		PWS_CMD_DDT	
Code	3	BYTE	Command code: 1 = swap, 3 = clear, etc.
PwsTarget	2	BYTE	Power supply target: 1 for left, 2 for right, 3 for both
pws_cmd_ip_str_1	''	string[64]	
pws_cmd_data_1		PWS_DATA_DDT	

Section 8.8
Application Security Management

Introduction

Control Expert lets you restrict access to the M580 safety PAC to users with assigned passwords. This section references the password assignment processes available in Control Expert.

What Is in This Section?

This section contains the following topics:

Application Password Protection

Overview

Control Expert provides a password mechanism to help guard against unauthorized access to the application. Control Expert uses the password when you:

- Open the application in Control Expert.
- Connect to the PAC in Control Expert.

NOTE: Use of a password is optional. The application protection by password mechanism is disabled if no password is configured in the application (the default setting).

Application protection by password helps prevent unwanted application modification, download, or the opening of (.STU and .STA files). The password is stored encrypted in the application.

Application Password

An M580 safety project is not password protected by default. If you do not manually assign a password when you create the safety project, Control Expert applies an empty string as the password.

In this case, when you next open your Control Expert M580 safety project, the **Password** dialog opens. To access your project, enter **no** password text, thereby accepting the empty string, and click **OK**. Thereafter, you can follow the steps set forth below to create a new password.

It is possible to create or change a password at any time.

The password is case-sensitive and has a length from 8 to 16 characters. The password robustness is increased when it contains a mix of upper and lower case, alphabetical, numerical, and special characters.

Creating a Password

Procedure for creating the application protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Project & Controller Protection** tab.
4	In the **Application** field, click **Change password ...**. **Result**: The **Modify Password** window appears.
5	Enter the new password in the **Entry** field.
6	Enter the confirmation of the new password in the **Confirmation** field.
7	Click **OK** to confirm.
8	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Changing the Password

Procedure for changing the application protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Project & Controller Protection** tab.
4	In the **Application** field, click **Change password ...**. **Result**: The **Modify Password** window appears.
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Deleting the Password

Procedure for clearing the application protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Project & Controller Protection** tab.
4	In the **Application** field, click **Clear password...**. **Result**: The **Password** window appears.
5	Enter the password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Auto-Lock Feature

There is an optional auto-lock feature that limits access to the Control Expert software programming tool after a configured time of inactivity. You can activate the auto-lock feature with the check box **Auto-lock** and select the time-out for the time of inactivity via **Minutes before lock**.

The default values are:

- **Auto-lock** is not activated
- **Minutes before lock** is set to 10 minutes (possible values: 1...999 minutes)

If the auto-lock feature is enabled and the configured inactivity time elapses, a modal dialog box is displayed requiring the entry of the application password. Behind the modal dialog box, all opened editors remain open in the same position. As a result, anybody can read the current content of the Control Expert windows but cannot continue to work with Control Expert.

NOTE: If you have not assigned a password to the project, the modal dialog box is not displayed.

Password Request Condition

Open an existing application (project) in Control Expert:

Password Management	
When an application file is opened, an **Application Password** dialog box opens.	
Enter the password.	
Click **OK**.	If the password is correct, the application opens.
	If the password is wrong, a message box indicates an incorrect password was entered, and a new **Application Password** dialog box opens.
If you click **Cancel**, the application is not opened	

Accessing the application in Control Expert after an auto-lock, when Control Expert is not connected to the PAC or when the project in Control Expert is EQUAL to the project in the PAC:

Password Management	
When auto-lock time is elapsed, an **Application Password** dialog box opens:	
Enter the password.	
Click **OK**.	If the password is correct, Control Expert becomes active again.
	If the password is wrong, a message box indicates an incorrect password was entered, and a new **Application Password** dialog box opens.
If you click **Close**, the application is closed without being saved.	

Accessing the application in the PAC after an auto-lock, when Control Expert is connected to the PAC and the application in Control Expert is DIFFERENT from the application in the PAC:

Password Management	
On connection, if Control Expert software application and the CPU application are not equal, an **Application Password** dialog box opens:	
Enter the password.	
Click **OK**.	If the password is correct, the connection is established.
	If the password is wrong, a message box indicates an incorrect password was entered, and a new **Application Password** dialog box opens.
If you click **Cancel**, the connection is not established.	
NOTE: On connection, if Control Expert software application and the CPU applications are equal, there is no password request. If no password has been initially entered (left empty on project creation), click **OK** to establish the connection on password prompt.	

NOTE: After three failed password attempts, you will have to wait an increasing amount of time between each subsequent password attempt. The wait period increases from 15 seconds to 1 hour, with the wait increment increasing by a factor of 2 after each successive failed attempt.

NOTE: In case of password loss, contact Schneider Electric support *(see page 170)*.

Safe Area Password Protection

At a Glance

Safety CPUs include a safe area password protection function, which is accessible from the **Properties** screen of the project. This function is used to help protect project elements located within the safe area of the safety project.

NOTE: When the safe area password protection function is active, the safe parts of the application cannot be modified

Modifications to the following safe area parts are not permitted when safe area password protection is enabled:

Safe Part	Forbidden action (offline AND online)
Configuration	Modify CPU characteristics
	Add, Delete, Modify a Safety module in the rack
	Modify Safety Power supply
Types	Create, Delete, Modify a Safe DDT
	Change a DDT attribute: from not safe->safe
	Change a DDT attribute: from safe->not safe
	Create, Delete, Modify a Safe DFB
	Change a DFB attribute: from not safe->safe
	Change a DFB attribute: from safe->not safe
Program-SAFE	Any Change under the **Variables an FB instances** node
	Create Task
	Import Task
	Modify Task
	Create Section
	Delete Section
	Import Section
	Modify Section
Project Settings	Modify SAFE project settings
	Modify COMMON project settings

Encryption

The safe area password uses the standard encryption SHA-256 with a salt.

Safe Area Password Function versus Safety Project User Rights

The activation of the safe area password and the implementation of user rights created in the **Security Editor** are mutually exclusive security functions, as follows:

- If the user launching Control Expert has been assigned a user profile, that user can access the safe areas of the safety application if the user knows the safe area password and has been granted access rights in the **Security Editor**.
- If user profiles have not been assigned, a user can access the safe areas of the safety application by knowing the safe area password.

Visual Indicators in Control Expert

The state of the safe area protection function can be visibly detected by viewing the **Program-SAFE** node in the **Project Browser**:

- A locked padlock indicates a safe area password has been created and activated.
- An unlocked padlock indicates a safe area password has been created but not activated.
- No padlock indicates a safe area password has not been created.

NOTE: If a safe area password has been created but not activated, and the safety application is closed then re-opened, the safe area password is automatically activated on re-opening. This behavior serves as a precaution if the safe are password was unintentionally not re-activated.

Compatibility

The safe area password function exists for Control Expert configuration software v14.0 and higher, for M580 safety CPUs with firmware version 2.8 and higher.

NOTE:

- Application program .STU, .STA, and .ZEF files, which are created in Control Expert v14.0 and higher, cannot be opened in Unity Pro version 13.1 and earlier.
- Replacing an M580 safety CPU in a Control Expert v14.0 application has the following effect:
  - Upgrading from firmware version 2.7 to 2.8 (or higher) adds the safe area password functionality to the **Program & Safety Protection** tab of the **Project → Properties** window.
  - Downgrading from firmware version 2.8 (or higher) to 2.7 removes the safe area password functionality.

Activating Protection and Creating Password

Procedure for activating the protection of sections and creating the password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, activate the protection by checking the **Protection active** box. **Result**: The **Modify Password** dialog box appears.

Step	Action
5	Enter a password in the **Entry** field.
6	Enter the confirmation of the password in the **Confirmation** field.
7	Click **OK** to confirm.
8	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Changing the Password

Procedure for changing the project sections protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, click **Change password ....** **Result**: The **Modify Password** dialog box appears:
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Deleting the Password

Procedure for deleting the project sections protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, click **Clear password....** **Result**: The **Access control** dialog box appears:
5	Enter the previous password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Section Protection

At a Glance

The section protection function is accessible from the **Properties** screen of the project in offline mode.

This function is used to help protect individual program sections, for which a level of protection has been configured.

NOTE: The section protection is not active as long as the protection has not been activated in the project.

NOTE:
The project protection is effective to the marked sections only. This does not prevent:
- Connecting to the CPU
- Uploading application from the CPU
- Changing the configuration
- Adding new sections
- Changing the logic in a new section (without section protection)

Activating Protection and Creating Password

Procedure for activating the protection of sections and creating the password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Sections & Program Units** area, activate the protection by checking the **Protection active** box. **Result**: The **Modify Password** dialog box appears.
5	Enter a password in the **Entry** field.
6	Enter the confirmation of the password in the **Confirmation** field.
7	Select the **Crypted** check box if an enhanced password protection is required. **NOTE:** A project with a crypted password cannot be edited with a Unity Pro version lower than 4.1. **NOTE:** Unity Pro is the former name of Control Expert for version 13.1 or earlier.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Notes

If a section *(see EcoStruxure™ Control Expert, Operating Modes)* is configured with a protection (read or read/write), when protection has been activated this will be indicated by a locked padlock at the section level.

If the section is configured with a protection but the protection is disabled, an open padlock is displayed at the section level.

Changing the Password

Procedure for changing the project sections protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Sections & Program Units** area, click **Change password ...**. **Result**: The **Modify Password** dialog box appears:
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Select **Crypted** check box if an enhanced password protection is required. **NOTE:** A project with a crypted password cannot be edited with a Unity Pro version lower than 4.1.
9	Click **OK** to confirm.
10	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Deleting the Password

Procedure for deleting the project sections protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Sections** field, click **Clear password...**. **Result**: The **Access control** dialog box appears:
5	Enter the previous password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Firmware Protection

Overview

Firmware protection by a password helps prevent unwanted access to the module firmware via FTP.

Password

The firmware is password protected by default with the following password: `fwdownload`.

It is possible to change a password at any time.

The password is case-sensitive and contains 8 to 16 alphanumeric characters. The password robustness is increased when it contains a mix of upper and lower case, alphabetical, numerical, and special characters.

NOTE: When importing a ZEF file, the firmware password of the module is set to its default value.

Changing the Password

NOTE: Firmware default password: `fwdownload`

Procedure for changing the firmware protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select **Project & Controller Protection** tab.
4	In the **Firmware** field, click **Change password ...**. **Result**: The **Modify Password** window appears.
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Resetting the Password

Resetting the password assigns its default value to the firmware password (**`fwdownload`**) once the current password is confirmed. Proceed as follows:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select **Project & Controller Protection** tab.
4	In the **Firmware** field, click **Reset password...**. **Result**: The **Password** window appears.
5	Enter current password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. The new password is the default password: **`fwdownload`**. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Data Storage Protection

Overview

Data storage protection by a password helps prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the CPU).

Password

The data storage area is password protected by default with the following password: **`datadownload`**.

It is possible to change a password at any time.

The password is case-sensitive and it must have a size from 8 to 16 alphanumeric characters. The password robustness is increased when it contains a mix of upper and lower case, alphabetical, numerical, and special characters.

NOTE: When importing a ZEF file, the data storage password of the application is set to its default value.

Changing the Password

NOTE: Data storage default password: **`datadownload`**

Procedure for changing the data storage protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select **Project & Controller Protection** tab.
4	In the **Data Storage** field, click **Change password ...**. **Result**: The **Modify Password** window appears.
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Resetting the Password

Resetting the password assigns its default value to the data storage password (**`datadownload`**) once the current password is confirmed. Proceed as follows:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select **Project & Controller Protection** tab.
4	In the **Data Storage** field, click **Reset password...**. **Result**: The **Password** window appears.
5	Enter current password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. The new password is the default password: **`datadownload`**. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Loss of Password

Overview

If you forget a password, proceed as indicated in the following procedures and contact Schneider Electric support.

Control Expert Passwords

Schneider Electric support needs a number displayed from the **Password** dialog box reached in following conditions:

- At open time, select the application and the **Password** dialog box is displayed.
- At auto-lock time, the **Password** dialog box is displayed. If you do not remember the password, select **Close**. Open the application again and the **Password** dialog box is displayed.
  NOTE: When the application is closed without entering a password after an auto-lock, all modifications are lost.

Procedure for resetting the application password:

Step	Action
1	**Condition:** The **Password** dialog box is displayed.
2	Press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **NOTE:** The password is a temporary password, available as long as the application is not modified.
5	Enter this password.
6	Modify the password (old password = password provided by Schneider Electric support).
7	Click **Build → Build Changes**.
8	**Save** the application.

CPU Application Password

Procedure for resetting the CPU application password if the respective **.STU* file is available:

Step	Action
1	Open the respective **.STU* file.
2	When the password dialog box is displayed press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **Note:** The password is a temporary password, available as long the application is not modified.
5	Enter this password.
6	Modify the password (old password = password provided by Schneider Electric support).
7	**Connect** to the PLC.
8	Click **Build** → **Build Changes**.
9	**Save** the application.

Procedure for resetting the CPU application password if the respective **.STU* file is not available:

Step	Action
1	**Condition:** At connection time, the **Password** dialog box is displayed.
2	Press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **Note:** The password provided by Schneider Electric support is a temporary password, available as long as the application is not modified.
5	Enter this password.
6	Upload the application from CPU.
7	**Save** the application.
8	Modify the password (old password = the one provided by Schneider Electric support).
9	Click **Build** → **Build Changes**.
10	**Save** the application.

Safe Area Password

Schneider Electric support needs a number displayed from the **Password** dialog box reached in following condition:

- In **Properties of Project** → **Program & Safety Protection** → **Safety** field, click **Clear password...** and the **Password** dialog box is displayed.

Procedure for resetting the firmware password:

Step	Action
1	**Condition:** The **Password** dialog box is displayed.
2	Press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **Note:** The password is a temporary password, available as long as you do not modify the application.
5	Enter this password and click **OK** to close the **Password** dialog.
6	Click **Change Password** and change the password (note, the old password = password provided by Schneider Electric support).
7	Click **OK** to close the **Modify Password** dialog, then click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Firmware Password

Schneider Electric support needs a number displayed from the **Password** dialog box reached in following condition:

- In **Properties of Project** → **Project & Controller Protection** → **Firmware** field, click **Reset password...** and the **Password** dialog box is displayed.

Procedure for resetting the firmware password:

Step	Action
1	**Condition:** The **Password** dialog box is displayed.
2	Press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **Note:** The password is a temporary password, available as long as you do not modify the application.
5	Enter this password and click **OK** to close the **Password** dialog.
6	Click **Change Password** and change the password (note, the old password = password provided by Schneider Electric support).
7	Click **OK** to close the **Modify Password** dialog, then click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Data Storage Password

Schneider Electric support needs a number displayed from the **Password** dialog box reached in following condition:

- In **Properties of Project** → **Project & Controller Protection** → **Data Storage** field, click **Reset password...** and the **Password** dialog box is displayed.

Procedure for resetting the data storage password:

Step	Action
1	**Condition:** The **Password** dialog box is displayed.
2	Press `SHIFT+F2`. **Result:** A grayed number is displayed in the right side of the **Password** dialog box.
3	Give this number to Schneider Electric support.
4	Receive the generated password from Schneider Electric support. **Note:** The password is a temporary password, available as long as you do not modify the application.
5	Enter this password and click **OK** to close the **Password** dialog.
6	Click **Change Password** and change the password (note, the old password = password provided by Schneider Electric support).
7	Click **OK** to close the **Modify Password** dialog, then click **OK** or **Apply** in the **Properties of Project** window to confirm all changes. If you click **Cancel** in the **Properties of Project** window, all changes are canceled.

Section 8.9
Workstation Security Management

Introduction

Schneider Electric provides the **Security Editor** access management tool that you can use to limit and control access to the workstation on which your Control Expert software is installed. This section describes the features of this tool that uniquely relate to M580 safety projects.

What Is in This Section?

This section contains the following topics:

Managing Access to Control Expert

Introduction

Schneider Electric provides the **Security Editor** configuration tool that lets you manage access to the Control Expert software installed on a workstation. Using he *Security Editor* configuration tool to manage access to the Control Expert software is optional.

NOTE: Access management relates to the hardware – typically a workstation – on which Control Expert software is installed and not to the project, which has its own protection system.

For more information about the **Security Editor**, refer to the *Access security management (see EcoStruxure™ Control Expert, Operating Modes)* section of the *EcoStruxure™ Control Expert Operating Modes* manual.

NOTE: Safety user profiles also require rights to access the process part of the safety application. When you create or modify a user profile, it is your responsibility to confirm that all necessary modifications are properly made.

Categories of Users

The **Security Editor** supports two categories of users:

- **Super User (Supervisor):**
  The super user is the only person to manage access security for the software. The super user specifies who can access the software and their access rights. During installation of Control Expert on the workstation, only the super user can access the security configuration without any limitation of rights (without a password).
  NOTE: The user name reserved for the super user is Supervisor.
- **Users:**
  Software users are defined in the list of users by the super user, if Control Expert access security is active. If your name is in the user list, you can access a software instance by entering your name (exactly as it appears on the list) and your password.

User Profile

The user profile comprises all of the access rights for a user. The user profile can be custom-defined by the super user, or can be created by applying a preconfigured profile that comes with the **Security Editor** tool.

Preconfigured User Profiles

The **Security Editor** offers the following preconfigured user profiles, which apply to either the safety program or the process program:

Profile	Applicable program type		Description
	Process	Safety	
ReadOnly	✓	✓	The user can only access the project in read mode, except for the PAC address, which can be modified. The user can also copy or download the project.
Operate	✓	–	The user has the same rights as with a **ReadOnly** profile, with the added possibility of modifying process program execution parameters (constants, initial values, task cycle times, etc.).
Safety_Operate	–	✓	The user has similar rights as with the **Operate** profile, but with respect to the safety program, except that: ● Transferring data values to the PAC is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Adjust	✓	–	The user has the same rights as with an **Operate** profile, with the added possibility of uploading a project (transfer to the PAC) and modifying the PAC operating mode (**Run**, **Stop**, ...)
Safety_Adjust	–	✓	The user has similar rights as with the **Adjust** profile, but with respect to the safety program, except that: ● Transferring data values to the PAC is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Debug	✓	–	The user has the same rights as with an **Adjust** profile, with the added possibility of using the debugging tools.
Safety_Debug	–	✓	The user has similar rights as with the **Debug** profile, but with respect to the safety program, except that: ● Stopping or starting the program is not permitted. ● Updating initialization values is not permitted. ● Transferring data values to the PAC is not permitted. ● Forcing inputs, outputs or internal bits is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Program	✓	–	The user has the same rights as with a **Debug** profile, with the added possibility of modifying the program.

Profile	Applicable program type		Description
	Process	Safety	
Safety_Program	–	✓	The user has similar rights as with the **Program** profile, but with respect to the safety program, except that: ● Stopping or starting the program is not permitted. ● Updating initialization values is not permitted. ● Transferring data values to the PAC is not permitted. ● Restoring the project to the PAC from a saved backup is not permitted. ● Forcing inputs, outputs or internal bits is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Disabled	✓	✓	User cannot access the project.

Assigning a Preconfigured User

The super user can assign a preconfigured user, derived from a preconfigured profile, to a specific user in the **Users** tab of the **Security Editor**. The following preconfigured user selections are available:

- safety_user_Adjust
- safety_user_Debug
- safety_user_Operate
- safety_user_Program
- user_Adjust
- user_Debug
- user_Operate
- user_Program

Refer to the topic *User Functions (see EcoStruxure™ Control Expert, Operating Modes)* in the *EcoStruxure™ Control Expert Operating Modes* manual for more information about how a super user can assign a preconfigured profile to a user.

Access rights

Introduction

Control Expert access rights are classified in the following categories:

- project services
- adjustment/debugging
- libraries
- global modification
- elementary modification of a variable
- elementary modification of DDT compound data
- elementary modification of a DFB type
- elementary modification of a DFB instance
- bus configuration editor
- input/output configuration editor
- runtime screens
- cyber security
- safety

This topic presents the access rights available for each of the preconfigured user profiles.

Project services

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Create a new project	–	–	–	–	–	–	✓	✓
Open an existing project	✓	✓	✓	✓	✓	✓	✓	✓
Save a project	–	–	–	–	–	–	✓	✓
SaveAs a project	✓	✓	✓	✓	✓	✓	✓	✓
Import a project	–	–	–	–	–	–	✓	✓
Build off-line	–	–	–	–	–	–	✓	✓
Build on-line STOP	–	–	–	–	–	–	✓	✓
Build on-line RUN	–	–	–	–	–	–	✓	✓
Start, stop or initialize the PAC*	✓	–	✓	–	–	–	✓	✓
Update init values with current values (only non-safe data)	–	–	✓	–	–	–	✓	✓
Transfer project from PAC	✓	✓	✓	✓	✓	✓	✓	✓
Transfer project to PAC	✓	✓	✓	✓	–	–	✓	✓
Transfer data values from file to PAC (only non-safe data)	✓	–	✓	–	✓	–	✓	✓
Restore project backup in PAC	–	–	–	–	–	–	✓	✓
Save to project backup in PAC	–	–	–	–	–	–	✓	✓
Set address	✓	✓	✓	✓	✓	✓	✓	✓
Modify options	✓	✓	✓	✓	✓	✓	✓	✓

* Only process tasks are started or stopped. For a non-safety PAC, this means the PAC is started or stopped. For an M580 safety PAC, this means that tasks other than the SAFE task are started or stopped.

✓ : Included

– : not included

Adjustment/Debugging

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Modify variable values	✓	–	✓		✓		✓	✓
Modify safety variable values	–	✓	–	✓	–	✓	–	✓
Force internal bits	–	–	✓	–	–	–	✓	✓
Force outputs	–	–	✓	–	–	–	✓	✓
Force inputs	–	–	✓	–	–	–	✓	✓
Task management	–	–	✓	–	–	–	✓	✓
SAFE Task management	–	–	–	✓	–	–	–	✓
Task cycle time modification	✓	–	✓		✓	–	✓	✓
SAFE Task cycle time modification	–	✓	–	✓	–	✓	–	✓
Suppress message in viewer	✓	✓	✓	✓	✓	✓	✓	✓
Debug the executable	–	–	✓	✓	–	–	✓	✓
Replace a project variable	–	–	–	–	–	–	✓	✓
Replace a safety project variable	–	–	–	–	–	–	–	✓
✓ : Included – : not included								

Libraries

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Create libraries or families	–	–	–	–	–	–	✓	✓
Create safety libraries or families	–	–	–	–	–	–	–	✓
Delete libraries or families	–	–	–	–	–	–	✓	✓
Delete safety libraries or families	–	–	–	–	–	–	–	✓
Put an object into library	–	–	–	–	–	–	✓	✓
Put an object into safety library	–	–	–	–	–	–	–	✓
Delete an object from library	–	–	–	–	–	–	✓	✓
Delete an object from safety library	–	–	–	–	–	–	–	✓
Get an object from a library	–	–	–	–	–	–	✓	✓
Get an object from the safety library	–	–	–	–	–	–	–	✓
✓ : Included – : not included								

Global modification

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Modify the documentation	✓	✓	✓	✓	✓	✓	✓	✓
Modify the functional view	–	–	–	–	–	–	✓	✓
Modify the animation tables	✓	✓	✓	✓	✓	✓	✓	✓
Modify constants value	✓	–	✓	–	✓	–	✓	✓
Modify safety constants value	–	✓	–	✓	–	✓	–	✓
Modify the program structure	–	–	–	–	–	–	✓	✓
Modify the safety program structure	–	–	–	–	–	–	–	✓
Modify program sections	–	–	–	–	–	–	✓	✓
Modify safety program sections	–	–	–	–	–	–	–	✓
Modify project settings	–	–	–	–	–	–	✓	✓
✓ : Included – : not included								

Elementary modification of a variable

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Variable add/remove	–	–	–	–	–	–	✓	✓
Safety Variables add/remove	–	–	–	–	–	–	–	✓
Variable main attributes modifications	–	–	–	–	–	–	✓	✓
Safety Variables main attributes modifications	–	–	–	–	–	–	–	✓
Variable minor attributes modifications	✓	–	✓	–	✓	–	✓	✓
Safety Variables minor attributes modifications	–	✓	–	✓	–	✓	–	✓
✓ : Included – : not included								

Elementary modification of DDT compound data

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DDT add/remove	–	–	–	–	–	–	✓	✓
DDT modifications	–	–	–	–	–	–	✓	✓
✓ : Included – : not included								

Elementary modification of a DFB type

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DFB type add/remove	–	–	–	–	–	–	✓	✓
Safety DFB type add/remove	–	–	–	–	–	–	–	✓
DFB type structure modification	–	–	–	–	–	–	✓	✓
Safety DFB type structure modification	–	–	–	–	–	–	–	✓
DFB type sections modification	–	–	–	–	–	–	✓	✓
Safety DFB type sections modification	–	–	–	–	–	–	–	✓
✓ : Included – : not included								

Elementary modification of a DFB instance

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DFB instance modification	–	–	–	–	–	–	✓	✓
Safety DFB instance modification	–	–	–	–	–	–	–	✓
DFB instance minor attributes modification	✓	–	✓	–	✓	–	✓	✓
Safety DFB instance minor attributes modification	–	✓	–	✓	–	✓	–	✓
✓ : Included – : not included								

Bus configuration editor

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Modify the configuration	–	–	–	–	–	–	✓	✓
Modify the safety configuration	–	–	–	–	–	–	–	✓
I/O sniffing	–	–	–	–	–	–	✓	✓
✓ : Included – : not included								

Input/output configuration editor

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Modify the I/O configuration	–	–	–	–	–	–	✓	✓
Modify the safety I/O configuration	–	–	–	–	–	–	–	✓
Adjust the I/O	✓	–	✓	–	✓	–	✓	✓
Adjust the safety I/O	–	✓	–	✓	–	✓	–	✓
Save_param	–	–	✓	–	–	–	✓	✓
Restore_param	–	–	✓	–	–	–	✓	✓
✓ : Included – : not included								

Runtime screens

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify screens	–	–	–	–	–	–	✓	✓
Modify messages	–	–	–	–	–	–	✓	✓
Add/remove screens or families	–	–	–	–	–	–	✓	✓
✓ : Included – : not included								

Cyber Security

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Create or modify application password	–	–	–	–	–	–	✓	✓
Enter Maintenance mode	–	✓	–	✓	–	✓	–	✓
Adapt Auto-Lock timeout	✓	✓	✓	✓	✓	✓	✓	✓
✓ : Included – : not included								

Safety

The access rights for this category are as follows:

Access right	Preconfigured User Profile							
	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Enter Maintenance mode	–	✓	–	✓	–	✓	–	✓
✓ : Included – : not included								

Section 8.10
M580 Safety Project Settings

Project Settings for an M580 Safety Project in Control Expert

Scope-Specific Project Settings

Select **Tools → Project Settings...** in the Control Expert main menu to open a window where you can configure and view the project settings for an M580 safety project. Project settings are divided into three groups, depending on the applicable **Scope** of the settings, as follows:

- **common**: These settings apply to the entire application, and can impact the global, process, and safe areas of the project.
- **process**: These settings apply only to the process area of the project.
- **safe**: These settings apply only to the process area of the project.

This topic describes only those parts of the **Project Settings** window that vary from an M580 non-safety project. Refer to the *Project Settings (see EcoStruxure™ Control Expert, Operating Modes)* section of the *EcoStruxure™ Control Expert Operating Modes* manual for information regarding features that are common to both M580 safety and non-safety projects.

Common Project Settings

The following **Scope → common** settings apply to the global, safe, and process project areas, but differently from the same settings in an M580 non-safety project:

Group	Setting	Description
General settings:		
Build settings	Free data memory (in kbytes)	This setting is disabled. **NOTE:** In an M580 safety system, the allocation of data is performed dynamically, and a fixed size data block does not need to be reserved.
	Virtual connected mode	This setting is disabled and de-selected.

Group	Setting	Description
PLC embedded data	Data dictionary ● Usage of Process Namespace	Determines how an operator screen can access and read process namespace variables: ● If selected, the operator screen can read process area variables only by using the format “PROCESS.<variable name>”. ● If de-selected, the operator screen can read process area variables only by using the format “<variable name>” without the PROCESS prefix. **NOTE:** All variables in the safe area are accessed using the format “SAFE.<variable name>”.
	Optimize data on-line change	Applies to the: ● Process program in both safety and maintenance operating modes. ● Safety program only in maintenance operating mode.
PLC diagnostics	Rack Viewer diagnostics information ● Rack Viewer variable names	Both of these settings are available to both process and safety variables.
	Program Viewer information	This setting is available for both process and safety code sections.
Time	Time Stamping Mode	This setting is available for both process and safety programs, with the exception that time stamping for safety variables is not supported.
Operator Screen settings:		
Controlled Screen	Displaying screens controlled via the PLC	This setting is available in the M580 safety PAC for the selected variable.

Common Project Settings that do not affect the Safe Area of the Project

The following **Scope** → **common** settings apply to the process program, but not to the safety program in an M580 safety project:

Group	Setting	Description
General settings:		
PLC Behaviour	Reset %M on Stop->Run transition	LL984 code sections are not supported in the safety program.
Configuration	M580 preferred I/O data type (Local I/O)	Only the device DDDT data type is available for safety I/O modules.
Variables settings:		
–	Directly represented array variables	%MW access is not supported in the safety program.
	Enable fast scanning for trending	Trending tool is not supported in the safety program. It is supported only in the MAST task of the process program.
	Force references initialization	References are not allowed in the safety program.
Program settings:		
Languages ● Common	Allow nested comments	Supported only for non-safe tasks (MAST, FAST, AUX0, and AUX1).
	Allow multi assignment (a:=b:=c) (ST/LD)	● The ST language, which includes the Operate block, is not supported by the safety program. ● The LD language in the safety program does not support
	Allow empty parameters in non-formal call (ST / IL)	The ST and IL languages are not supported in the safety program.
Languages ● ST	Allow jump and label	The ST language is not supported in the safety program.

Project Settings that Impact the Process and Safe Project Areas Differently

Both the **Scope** → **safe** and the **Scope** → **process** present the same collection of program settings. However, the following settings are treated differently in each scope in an M580 safety project

Group	Setting	Description
General settings:		
Build settings	Optimized code	● Enabled for the process scope. ● Disabled and de-selected for the safe scope.
	Safe Signature management	● Disabled for the process scope. ● Enabled and set to **Automatic** by default, for the safe scope.

Group	Setting	Description
PLC diagnostics	Application diagnostics ● Application diagnostic level	● Enabled for the process scope. ● Disabled and de-selected for the safe scope. **NOTE:** DFB language is not available for safety program code sections.
Variables settings:		
–	Allow dynamic arrays	These settings are: ● Enabled for the process scope. ● Disabled and de-selected for the safe scope. **NOTE:** Dynamic arrays are not supported for safety program variables.
	Disable array size compatibility check	
Program settings:		
Languages	Function Block Diagram (FBD)	Enabled for both the process and safe scopes.
	Ladder (LD)	
	Sequential Function Chart (SFC)	● Enabled for the process scope. ● Disabled and de-selected for the safe scope.
	List (IL)	
	Structured Test (ST)	
	Ladder Logic 984 (LL984)	
Languages ● Common	Allow subroutines	● Enabled for the process scope. ● Disabled and de-selected for the safe scope. **NOTE:** Subroutines are not supported in the safety program.
	Usage of ST expressions (LD/FBD)	● Enabled for the process scope. ● Disabled and de-selected for the safe scope. **NOTE:** ST expressions are not supported in the safety program.
	Enable implicit type conversion	● Enabled for the process scope. ● Disabled and de-selected for the safe scope. **NOTE:** Implicit type conversions are not supported in the safety program.

Appendices

Introduction

The appendices contain information on the IEC 61508 and its SIL policy. Further, technical data of the Safety and non-interfering modules are provided and example calculations are carried out.

What Is in This Appendix?

The appendix contains the following chapters:

Appendix A
IEC 61508

Introduction

This chapter provides information on the Safety concepts of the IEC 61508 in general and its SIL policy in particular.

What Is in This Chapter?

This chapter contains the following topics:

General Information on the IEC 61508

Introduction

Safety-Related Systems are developed for use in processes in which risks to humans, environment, equipment and production are to be kept at an acceptable level. The risk depends on the severity and likelihood, thereby defining the necessary measures of protection.

Concerning the Safety of processes, there are 2 sides to be considered:

- the regulations and requirements defined by official authorities in order to help protect humans, environment, equipment, and production
- the measures by which these regulations and requirements are fulfilled

IEC 61508 Description

The technical standard defining the requirements for Safety-Related Systems is

- the IEC 61508.

It deals with the Functional Safety of electrical, electronic or programmable electronic Safety-Related Systems. A Safety-Related System is a system that is required to perform 1 or more specific functions to ensure risks are kept at an acceptable level. Such functions are defined as Safety Functions. A system is defined functionally Safe if random, systematic, and common cause failures do not lead to malfunctioning of the system and do not result in injury or death of humans, spills to the environment and loss of equipment and production.

The standard defines a generic approach to all lifecycle activities for systems that are used to perform Safety Functions. It constitutes procedures to be used for the design, the development, and the validation of both hardware and software applied in Safety-Related Systems. Further, it determines rules concerning both the management of Functional Safety and documentation.

IEC 61511 Description

The Functional Safety requirements defined in the IEC 61508 are refined specifically for the process industry sector in the following technical standard:

- the IEC 61511: Functional safety - safety instrumented systems for the process industry sector

This standard guides the user in the application of a Safety-Related System, starting from the earliest phase of a project, continuing through the start up, covering modifications and eventual decommissioning activities. In summary, it deals with the Safety Lifecycle of all components of a Safety-Related System used in the process industry.

Risk Description

The IEC 61508 is based on the concepts of risk analysis and Safety Function. The risk depends on severity and probability. It can be reduced to a tolerable level by applying a Safety Function that consists of an electrical, electronic or programmable electronic system. Further, it should be reduced to a level that is as low as reasonably practicable.

In summary, the IEC 61508 views risks as follows:

- Zero risk can never be reached.
- Safety is to be considered from the beginning.
- Intolerable risks are to be reduced.

SIL Policy

Introduction

The SIL value evaluates the robustness of an application against failures, thus indicating the ability of a system to perform a Safety Function within a defined probability. The IEC 61508 specifies 4 levels of Safety performance depending on the risk or impacts caused by the process for which the Safety-Related System is used. The more dangerous the possible impacts are on community and environment, the higher the Safety requirements are to lower the risk.

SIL Value Description

Discrete level (1 out of a possible 4) for specifying the Safety Integrity requirements of the Safety Functions to be allocated to the Safety-Related Systems, where Safety Integrity Level 4 has the highest level of Safety Integrity and Safety Integrity Level 1 has the lowest, see *SILs for Low Demand, page 197*.

SIL Requirements Description

To achieve Functional Safety, 2 types of requirements are necessary:

- Safety Function requirements, defining what Safety Functions have to be performed
- Safety Integrity requirements, defining what degree of certainty is necessary that the Safety Functions are performed

The Safety Function requirements are derived from hazard analysis and the Safety Integrity ones from risk assessment.

They consist of the following quantities:

- Mean time between failures
- Probabilities of failure
- Failure rates
- Diagnostic coverage
- Safe failure fraction
- Hardware fault tolerance

Depending on the level of Safety Integrity, these quantities must range between defined limits.

NOTE: Mixing different safety integrity level devices on a network or safety function requires a high degree of care with respect to the requirements of IEC 61508, and produces design and operational implications.

SIL Rating Description

As defined in the IEC 61508, the SIL value is limited by both the Safe Failure Fraction (SFF) and the hardware fault tolerance (HFT) of the subsystem that performs the Safety Function. A HFT of n means that n+1 faults could cause a loss of the Safety Function, the Safe state cannot be entered. The SFF depends on failure rates and diagnostic coverage.

The following table shows the relation between SFF, HFT, and SIL for complex Safety-Related subsystems according to IEC 61508-2, in which the failure modes of all components cannot be completely defined:

SFF	HFT=0	HFT=1	HFT=2
SFF ≤ 60%	-	SIL1	SIL2
60% < SFF ≤ 90%	SIL1	SIL2	SIL3
90% < SFF ≤ 99%	SIL2	SIL3	SIL4
SFF > 99%	SIL3	SIL4	SIL4

There are 2 ways to reach a certain Safety Integrity Level:

- via increasing the HFT by providing additional independent shutdown paths
- via increasing the SFF by additional diagnostics

SIL-Demand Relation Description

The IEC 61508 distinguishes between low demand mode and high demand (or continuous) mode of operation.

In low demand mode, the frequency of demand for operation made on a Safety-Related System is not greater than 1 per year and not greater than twice the proof test frequency. The SIL value for a low demand Safety-Related System is related directly to its average probability of failure to perform its Safety Function on demand or, simply, probability of failure on demand (PFD).

In high demand or continuous mode, the frequency of demand for operation made on a Safety-Related System is greater than 1 per year and greater than twice the proof test frequency. The SIL value for a high demand Safety-Related System is related directly to its probability of a dangerous failure occurring per hour or, simply, probability of failure per hour (PFH).

SILs for Low Demand

The following table lists the requirements for a system in low demand mode of operation:

Safety Integrity Level	Probability of Failure on Demand
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

SILs for High Demand

The following table lists the requirements for a system in high demand mode of operation:

Safety Integrity Level	Probability of Failure per Hour
4	≥ 10^{-9} to < 10^{-8}
3	≥ 10^{-8} to < 10^{-7}
2	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-6} to < 10^{-5}

For SIL3, the required probabilities of failure for the complete Safety integrated system are:

- PFD ≥ 10^{-4} to < 10^{-3} for low demand
- PFH ≥ 10^{-8} to < 10^{-7} for high demand

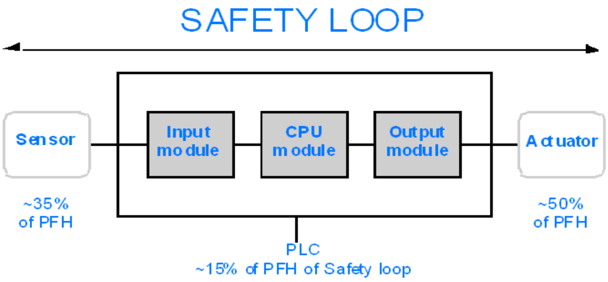
Safety Loop Description

The Safety loop to which the M580 Safety PAC consists of the following 3 parts:

- Sensors
- M580 Safety PAC with safety power supply, safety CPU, safety Coprocessor, and safety I/O modules
- Actuators

A backplane or a remote connection that includes a switch or a CRA does not destroy a Safety Loop. Backplanes, switches, and CRA modules are part of a the black channel. This means that the data exchanged by I/O and PAC cannot be corrupted without detection by the receiver.

The following figure shows a typical Safety loop:



As shown in the figure above, the contribution of the PAC is only 10-20% because the probability of failure of sensors and actuators is usually quite high.

A conservative assumption of 10% for the Safety PAC’s contribution to the overall probability leaves more margin for the user and results in the following required probabilities of failure for the Safety PAC:

- PFD $\geq 10^{-5}$ to $< 10^{-4}$ for low demand
- PFH $\geq 10^{-9}$ to $< 10^{-8}$ for high demand

PFD Equation Description

The IEC 61508 assumes that half of the failures end in a Safe state. Therefore, the failure rate λ is divided into

- λ_S - the safe failure and
- λ_D - the dangerous failure, itself composed of
  - λ_{DD} - dangerous failure detected by the internal diagnostic
  - λ_{DU} - dangerous failure undetected.

The failure rate can be calculated by using the mean time between failures (MTBF), a module specific value, as follows:

$\lambda = 1/MTBF$

The equation for calculating the probability of failure on demand is:

$PFD(t) = \lambda_{DU} \times t$

t represents the time between 2 proof tests.

The probability of failure per hour implies a time interval of 1 hour. Therefore, the PFD equation is reduced to the following one:

$PFH = \lambda_{DU}$

Appendix B
System Objects

Introduction

This chapter describes the system bits and words of the M580 Safety PAC.

NOTE: The symbols associated with each bit object or system word mentioned in the descriptive tables of these objects are not implemented as standard in the software, but can be entered using the data editor.

What Is in This Chapter?

This chapter contains the following topics:

M580 Safety System Bits

System Bits for SAFE Task Execution

The following system bits apply to the M580 safety PAC. For a description of system bits that apply to both the M580 safety PAC and non-safety M580 PACs, refer to the presentation of *System Bits (see EcoStruxure™ Control Expert, System Bits and Words, Reference Manual)* in the *EcoStruxure™ Control Expert System Bits and Words Reference Manual*.

These system bits are related to the execution SAFE task, but are not directly accessible in safety program code. They can be accessed only via the `S_SYST_READ_TASK_BIT_MX` and `S_SYST_RESET_TASK_BIT_MX` blocks.

Bit Symbol	Function	Description	Initial State	Type
%S17 `CARRY`	Rotate shift output	During a rotate shift operation in the SAFE task, this bit takes the state of the outgoing bit.	0	R/W
%S18 `OVERFLOW`	Overflow or arithmetic error detected	Normally set to 0, this bit is set to 1 in the event of a capacity overflow if there is: ● A result greater than + 32 767 or less than - 32 768, in single length. ● A result greater than + 65 535, in unsigned integer. ● A result greater than + 2 147 483 647 or less than - 2 147 483 648, in double length ● A result greater than +4 294 967 296, in double length or unsigned integer. ● Division by 0. ● The root of a negative number. ● Forcing to a non-existent step on a drum. ● Stacking up of an already full register, emptying of an already empty register.	0	R/W
%S21 `1RSTTASKRUN`	First SAFE task scan in RUN	Tested in the SAFE task, this bit indicates the first cycle of this task. It is set to 1 at the start of the cycle and reset to 0 at the end of the cycle. **NOTE:** ● The first cycle of the task status can be read using the `SCOLD` output of the `S_SYST_STAT_MX` system function block. ● This bit is not effective for M580 Safety Hot Standby systems.	0	R/W

Notes Regarding Non-Safety-Specific System Bits

System Bit	Description	Notes
%S0	cold start	Can be used only in process (non-SAFE) tasks and has no influence on SAFE task.
%S9	outputs set to fallback	Has no influence on Safety output modules.
%S10	Global I/O detected error	Reports some, but not all, of the possible detected errors relating to safety I/O modules.
%S11	watchdog overflow	Takes into account an overrun on SAFE task.
%S16	task I/O detected error	Reports some, but not all, of the possible detected errors relating to safety I/O modules.
%S19	task period overrun	Information for SAFE task overrun is not available.
%S40...47	rack *n* I/O detected error	Reports some, but not all, of the possible detected errors relating to safety I/O modules.
%S78	STOP on detected error	Applies to both process tasks and the SAFE task. If the bit is set, for example if a %S18 overflow error rises, the SAFE task enters HALT state.
%S94	save adjusted values	Does not apply to SAFE variables. The SAFE initial values are not modifiable by the activation of this bit.
%S117	RIO detected error on Ethernet I/O network	Reports some, but not all, of the possible detected errors relating to safety I/O modules.
%S119	general in rack detected error	Reports some, but not all, of the possible detected errors relating to safety I/O modules.

M580 Safety System Words

System Words for M580 Safety PACs

The following system words apply to the M580 safety PAC. For a description of system words that apply to both the M580 safety PAC and non-safety M580 PACs, refer to the presentation of *System Words (see EcoStruxure™ Control Expert, System Bits and Words, Reference Manual)* in the *EcoStruxure™ Control Expert System Bits and Words Reference Manual*.

These system words and values are related to the SAFE task. They can be accessed from application program code in the non-safety sections (MAST, FAST, AUX0 or AUX1), but not from code in the SAFE task section.

Word	Function	Type
%SW4	Period of the SAFE task defined in the configuration. The period is not modifiable by the operator.	R
%SW12	Indicates the operating mode of the Copro module: ● 16#A501 = maintenance mode ● 16#5AFE = safety mode Any other value is interpreted as a detected error.	R
%SW13	Indicates the operating mode of the CPU: ● 16#501A = maintenance mode ● 16#5AFE = safety mode Any other value is interpreted as a detected error.	R
%SW42	SAFE task current time. Indicates the execution time of the last cycle of the SAFE task (in ms).	R
%SW43	SAFE task max time. Indicate the longest task execution time of the SAFE task since the last cold start (in ms).	R
%SW44	SAFE task min time. Indicate the shortest task execution time of the SAFE task since the last cold start (in ms).	R
%SW110	Percentage of system CPU load used by the system for internal services.	R
%SW111	Percentage of system CPU load used by the MAST task.	R
%SW112	Percentage of system CPU load used by the FAST task.	R
%SW113	Percentage of system CPU load used by the SAFE task.	R
%SW114	Percentage of system CPU load used by the AUX0 task.	R
%SW115	Percentage of system CPU load used by the AUX1 task.	R
%SW116	Total system CPU load.	R

Word	Function	Type
%SW124	Contains the cause of the non-recoverable detected error when the M580 Safety PAC is in Halt state: ● 0x5AF2: RAM detected error in memory check. ● 0x5AFB: Safety firmware code error detected. ● 0x5AF6: Safety watchdog overrun error detected on CPU. ● 0x5AFF: Safety watchdog overrun error detected on coprocessor. ● 0x5B01: Coprocessor not detected at start-up. ● 0x5AC03: CIP safety non-recoverable error detected by CPU. ● 0x5AC04: CIP safety non-recoverable error detected by coprocessor. **NOTE:** The above does not constitute a complete list. Refer to the *EcoStruxure™ Control Expert System Bits and Words Reference Manual* for more information.	R
%SW125	Contains the cause of the recoverable detected error in the M580 Safety PAC: ● 0x5AC0: CIP safety configuration is not correct (detected by CPU). ● 0x5AC1: CIP safety configuration is not correct (detected by coprocessor). ● 0x5AF3: Comparison error detected by main CPU. ● 0x5AFC: Comparison error detected by coprocessor. ● 0x5AFD: Internal error detected by coprocessor. ● 0x5AFE: Synchronization error detected between CPU and coprocessor. ● 0x9690: Application program checksum error detected. **NOTE:** The above does not constitute a complete list. Refer to the *EcoStruxure™ Control Expert System Bits and Words Reference Manual* for more information.	R
%SW126	These two system words contain information that is for Schneider Electric internal use to help analyze a detected error in more detail.	R
%SW127		
%SW128	Force time synchronization between NTP time and Safe time into the safe IO modules and Safe CPU task: ● Value change from 16#1AE5 to 16#E51A forces synchronization. Refer to the topic *Procedure for Synchronizing NTP Time Settings (see Modicon M580, Safety Manual)*. ● Other sequences and values do not force synchronization.	R/W
%SW142	Contains the safety COPRO firmware version in 4 digits BCD: for example firmware version 21.42 corresponds to %SW142 = 16#2142.	R
%SW148	Count of error correcting code (ECC) errors detected by the CPU.	R
%SW152	Status of the NTP CPU time updated by Ethernet communications module (e.g BMENOC0301/11) over the X Bus backplane via the optional forced time synchronization feature (%SW128): ● 0: the CPU time is not refreshed by the Ethernet communications module. ● 1: The CPU time is refreshed by the Ethernet communications module.	R

Word	Function	Type
%SW169	Safety Application ID: Contains an ID of the safety code part of the application. The ID is automatically modified when the safe application code is modified. NOTE: - If the safe code has been changed and a **Build Changes** command has been executed since the previous **Rebuild All** command (thereby changing the Safety application ID), execution of a **Rebuild All** command may again change the Safety application ID. - The SAFE program unique identifier can be read using the `SAID` output of the `S_SYST_STAT_MX` system function block.	R
%SW171	State of the FAST tasks: - 0: No FAST tasks exist - 1: Stop - 2: Run - 3: Breakpoint - 4: Halt	R
%SW172	State of the SAFE task: - 0: No SAFE task exists - 1: Stop - 2: Run - 3: Breakpoint - 4: Halt	R
%SW173	State of the MAST task: - 0: No MAST task exists - 1: Stop - 2: Run - 3: Breakpoint - 4: Halt	R
%SW174	State of the AUX0 task: - 0: No AUX0 task exists - 1: Stop - 2: Run - 3: Breakpoint - 4: Halt	R
%SW175	State of the AUX1 task: - 0: No AUX1 task exists - 1: Stop - 2: Run - 3: Breakpoint - 4: Halt	R

Glossary

!

!

NOTE: For terms taken from the IEC 61508 standard, refer to the standard for complete definitions.

%I

According to the CEI standard, `%I` indicates a language object of type discrete IN.

%IW

According to the CEI standard, `%IW` indicates a language object of type analog IN.

%M

According to the CEI standard, `%M` indicates a language object of type memory bit.

%MW

According to the CEI standard, `%MW` indicates a language object of type memory word.

%S

ccording to the CEI standard, `%SW` indicates a language object of type system bit.

%SW

According to the CEI standard, `%SW` indicates a language object of type system word.

1oo2D diagnostic configuration

X out of Y. For example 1 out of 2. Voting and redundancy capacity of a Safety-Related System.

D in 1oo2D refers to diagnostics. Hence, D in 1oo2D means 1 out of 2 with diagnostics.

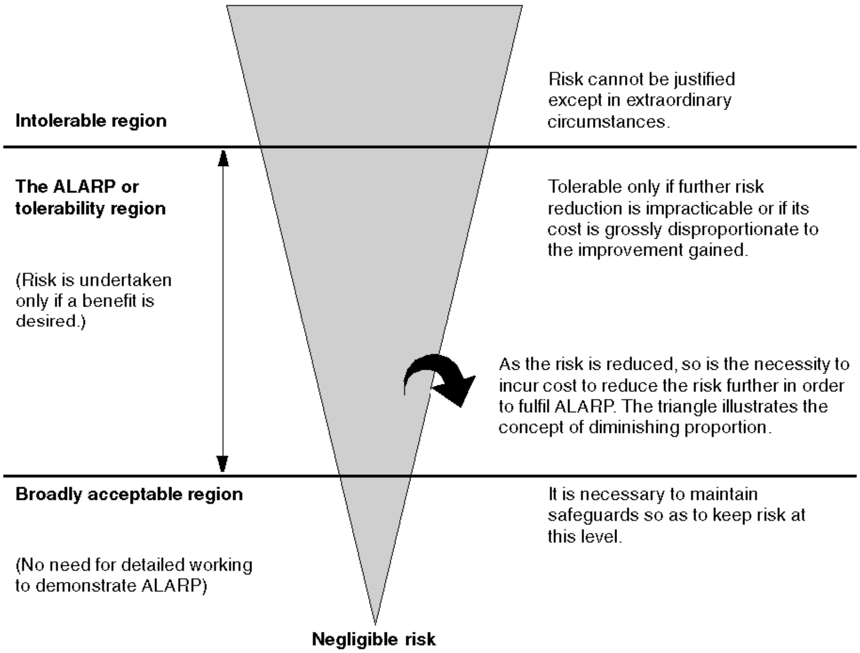
A

adapter

An adapter is the target of real-time I/O data connection requests from scanners. It cannot send or receive real-time I/O data unless it is configured to do so by a scanner, and it does not store or originate the data communications parameters necessary to establish the connection. An adapter accepts explicit message requests (connected and unconnected) from other devices.

ALARP

(*as low as reasonably practicable*) (Definition IEC 61508)


Intolerable region
Risk cannot be justified except in extraordinary circumstances.
The ALARP or tolerability region
(Risk is undertaken only if a benefit is desired.)
Tolerable only if further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained.
As the risk is reduced, so is the necessity to incur cost to reduce the risk further in order to fulfil ALARP. The triangle illustrates the concept of diminishing proportion.
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
It is necessary to maintain safeguards so as to keep risk at this level.
Negligible risk

ARRAY

An `ARRAY` is a table containing elements of a single type. This is the syntax: `ARRAY [<limits>] OF <Type>`

Example: `ARRAY [1..2] OF BOOL` is a one-dimensional table with two elements of type `BOOL`.

`ARRAY [1..10, 1..20] OF INT` is a two-dimensional table with 10x20 elements of type `INT`.

ART

(*application response time*) The time a CPU application takes to react to a given input. ART is measured from the time a physical signal in the CPU turns on and triggers a write command until the remote output turns on to signify that the data has been received.

AUX

An (AUX) task is an optional, periodic processor task that is run through its programming software. The AUX task is used to execute a part of the application requiring a low priority. This task is executed only if the MAST and FAST tasks have nothing to execute. The AUX task has two sections:

- IN: Inputs are copied to the IN section before execution of the AUX task.
- OUT: Outputs are copied to the OUT section after execution of the AUX task.

B

BCD

(*binary-coded decimal*) Binary encoding of decimal numbers.

BOOL

(*boolean type*) This is the basic data type in computing. A `BOOL` variable can have either of these values: 0 (`FALSE`) or 1 (`TRUE`).

A bit extracted from a word is of type `BOOL`, for example: `%MW10.4`.

BOOTP

(*bootstrap protocol*) A UDP network protocol that can be used by a network client to automatically obtain an IP address from a server. The client identifies itself to the server using its MAC address. The server, which maintains a pre-configured table of client device MAC addresses and associated IP addresses, sends the client its defined IP address. The BOOTP service utilizes UDP ports 67 and 68.

broadcast

A message sent to all devices in a broadcast domain.

C

CCF

(*common cause failure*) Failure, which is the result of 1 or more events, causing coincident failures of 2 or more separate channels in a multiple channel system, leading to system failure. (Definition IEC 61508) The common cause factor in a dual channel system is the crucial factor for the probability of failure on demand (PFD) for the whole system.

CCOTF

(*change configuration on the fly*) A feature of Control Expert that allows a module hardware change in the system configuration while the system is operating. This change does not impact active operations.

CIP™

(*common industrial protocol*) A comprehensive suite of messages and services for the collection of manufacturing automation applications (control, safety, synchronization, motion, configuration and information). CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the internet. CIP is the core protocol of EtherNet/IP.

cold start

Cold start refers to starting the computer from power off.

CRC

(*cyclic redundancy check*)

D

DDDT

(*device derived data type*) A DDT predefined by the manufacturer and not modifiable by user. It contains the I/O language elements of an I/O module.

DDT

(*derived data type*) A derived data type is a set of one or more types of basic data types, for example an array or structure.

determinism

For a defined application and architecture, you can predict that the delay between an event (change of value of an input) and the corresponding change of a controller output is a finite time *t*, smaller than the deadline required by your process.

device network

An Ethernet-based network within an RIO network that contains both RIO and distributed equipment. Devices connected on this network follow specific rules to allow RIO determinism.

DFB

(*derived function block*) DFBs are function blocks that can be defined by the user in ST, IL, LD or FBD language. Using these DFB types in an application makes it possible to:

- simplify the design and entry of the program
- make the program easier to read
- make it easier to debug
- reduce the amount of code generated

diagnostic coverage

Fractional decrease in the probability of dangerous hardware failures resulting from the operation of the automatic diagnostic tests. (Definition IEC 61508) The fraction of the possible dangerous failures λ_D is divided into failures which are detected by diagnostics and failures which remain undetected.

$\lambda_D=\lambda_{DD} + \lambda_{DU}$

The diagnostic coverage (DC) defines the fraction of the dangerous failures which are detected.

$\lambda_{DD} =\lambda_D$. DC

$\lambda DU=\lambda_D$ (1 - DC)

The definition may also be represented in terms of the following equation, where DC is the diagnostic coverage, λ_{DD} is the probability of detected dangerous failures and λ_D total is the probability of total dangerous failures:

$$\text{DC}= \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

DIO

(*distributed I/O*) Also known as distributed equipment. DRSs use DIO ports to connect distributed equipment.

DIO cloud

A group of distributed equipment that is not required to support RSTP. DIO clouds require only a single (non-ring) copper wire connection. They can be connected to some of the copper ports on DRSs, or they can be connected directly to the CPU or Ethernet communications modules in the *local rack*. DIO clouds **cannot** be connected to *sub-rings*.

DIO network

A network containing distributed equipment, in which I/O scanning is performed by a CPU with DIO scanner service on the local rack. DIO network traffic is delivered after RIO traffic, which takes priority in a device network.

distributed equipment

Any Ethernet device (Schneider Electric device, PC, servers, or third-party devices) that supports exchange with a CPU or other Ethernet I/O scanner service.

DLL

(*dynamic link library*)

DNS

(*domain name server/service*) A service that translates an alpha-numeric domain name into an IP address, the unique identifier of a device on the network.

DTM

(*device type manager*) A DTM is a device driver running on the host PC. It provides a unified structure for accessing device parameters, configuring and operating the devices, and troubleshooting devices. DTMs can range from a simple graphical user interface (GUI) for setting device parameters to a highly sophisticated application capable of performing complex real-time calculations for diagnosis and maintenance purposes. In the context of a DTM, a device can be a communications module or a remote device on the network.

See FDT.

E

E/E/PES

(*electrical/electronic/programmable electronic system*) (Definition IEC 61508) System for control, protection or monitoring based on 1 or more electrical/electronic programmable electronic (E/E/PE) devices. This includes elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices.

EDT

(*elementary data type*) An elementary data type is predefined.

EF

(*elementary function*) This is a block used in a program which performs a predefined logical function.

A function does not have any information on the internal state. Several calls to the same function using the same input parameters will return the same output values. You will find information on the graphic form of the function call in the [*functional block (instance)*]. Unlike a call to a function block, function calls include only an output which is not named and whose name is identical to that of the function. In FBD, each call is indicated by a unique [number] via the graphic block. This number is managed automatically and cannot be modified.

Position and configure these functions in your program in order to execute your application.

You can also develop other functions using the SDKC development kit.

EFB

(*elementary function block*) This is a block used in a program which performs a predefined logical function.

EFBs have states and internal parameters. Even if the inputs are identical, the output values may differ. For example, a counter has an output indicating that the preselection value has been reached. This output is set to 1 when the current value is equal to the preselection value.

EMC

(*electromagnetic compatibility*) The term refers to the origin, control, and measurement of electromagnetic effects on electronic systems.

EN

`EN` stands for **EN**able; it is an optional block input. When the `EN` input is enabled, an `ENO` output is set automatically.

If `EN` = 0, the block is not enabled; its internal program is not executed, and `ENO` is set to 0.

If `EN` = 1, the block's internal program is run and `ENO` is set to 1. If a runtime error is detected, `ENO` is set to 0.

If the `EN` input is not connected, it is set automatically to 1.

ENO

`ENO` stands for **E**rror **NO**tification; this is the output associated with the optional input `EN`.

If `ENO` is set to 0 (either because `EN` = 0 or if a runtime error is detected):

- The status of the function block outputs remains the same as it was during the previous scanning cycle that executed correctly.
- The output(s) of the function, as well as the procedures, are set to 0.

error

Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition. (Definition IEC 61508)

ESD

(*emergency shutdown*)

Ethernet

A 10 Mb/s, 100 Mb/s, or 1 Gb/s, CSMA/CD, frame-based LAN that can run over copper twisted pair or fiber optic cable, or wireless. The IEEE standard 802.3 defines the rules for configuring a wired Ethernet network; the IEEE standard 802.11 defines the rules for configuring a wireless Ethernet network. Common forms include 10BASE-T, 100BASE-TX, and 1000BASE-T, which can utilize category 5e copper twisted pair cables and RJ45 modular connectors.

EtherNet/IP™

A network communication protocol for industrial automation applications that combines the standard internet transmission protocols of TCP/IP and UDP with the application layer common industrial protocol (CIP) to support both high speed data exchange and industrial control.

EUC

(*equipment under control*) (Definition IEC 61508) This term designates equipment, machinery, apparatuses or plants used for manufacturing, process, transportation, medical or other activities.

explicit messaging

TCP/IP-based messaging for Modbus TCP and EtherNet/IP. It is used for point-to-point, client/server messages that include both data, typically unscheduled information between a client and a server, and routing information. In EtherNet/IP, explicit messaging is considered class 3 type messaging, and can be connection-based or connectionless.

F

failure

Termination of the ability of a functional unit to perform a required function. (Definition IEC 61508)

FAST

A FAST task is an optional, periodic processor task that identifies high priority, multiple scan requests, which is run through its programming software. A FAST task can schedule selected I/O modules to have their logic solved more than once per scan. The FAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the FAST task.
- OUT: Outputs are copied to the OUT section after execution of the FAST task.

Execution of the FAST task is given priority over all other tasks.

fault

Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function. (Definition IEC 61508)

FBD

(*function block diagram*) An IEC 61131-3 graphical programming language that works like a flowchart. By adding simple logical blocks (`AND`, `OR`, etc.), each function or function block in the program is represented in this graphical format. For each block, the inputs are on the left and the outputs on the right. Block outputs can be linked to inputs of other blocks in order to create complex expressions.

FDR

(*fast device replacement*) A service that uses configuration software to replace an inoperable product.

FFB

(*function/function block*)

FMEA

(*failure modes and effects analysis*)

FMECA

(*failure modes and effects criticality analysis*)

FTP

(*file transfer protocol*) A protocol that copies a file from one host to another over a TCP/IP-based network, such as the internet. FTP uses a client-server architecture as well as separate control and data connections between the client and server.

full duplex

The ability of two networked devices to independently and simultaneously communicate with each other in both directions.

Functional Safety

Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities. (Definition IEC 61508)

A system is defined functionally Safe if random, systematic and common cause failures do not lead to malfunctioning of the system and do not result in injury or death of humans, spills to the environment and loss of equipment or production:

- Functional Safety deals with the part of the overall Safety that depends on the correct functioning of the Safety-Related System.
- Functional Safety applies to products as well as organizations.

H

HFT

(*hardware fault tolerance*) (Definition IEC 61508)

A hardware fault tolerance of N means that N + 1 faults could cause a loss of the Safety Function, for instance:

- HFT = 0: The 1st failure could cause a loss of the Safety Function
- HFT = 1: 2 faults in combination could cause a loss of the Safety Function. (There are 2 different paths to go to a Safe state. Loss of the Safety Function means that a Safe state cannot be entered.

I

I/O scanner

An Ethernet service that continuously polls I/O modules to collect data, status, event, and diagnostics information. This process monitors inputs and controls outputs. This service supports both RIO and DIO logic scanning.

IEC

(*International Electrotechnical Commission*)

IEC 61131-3

International standard: programmable logic controllers; Part 3: programming languages

IEC 61508

The IEC 61508 standard is an international standard that addresses Functional Safety of electrical / electronic / programmable electronic Safety-Related Systems. It applies to any kind of Safety-Related System in any industry wherever there are no product standards.

IL

(*instruction list*) An IEC 61131-3 programming language that contains a series of basic instructions. It is very close to assembly language used to program processors. Each instruction is made up of an instruction code and an operand.

implicit messaging

UDP/IP-based class 1 connected messaging for EtherNet/IP. Implicit messaging maintains an open connection for the scheduled transfer of control data between a producer and consumer. Because an open connection is maintained, each message contains primarily data, without the overhead of object information, plus a connection identifier.

INT

(*INTeger*) (encoded in 16 bits) The upper/lower limits are as follows: -(2 to the power of 15) to (2 to the power of 15) - 1.

Example: `-32768`, `32767`, `2#1111110001001001`, `16#9FA4`.

IODDT

(*input/output derived data type*) A structured data type representing a module, or a channel of a CPU. Each application expert module possesses its own IODDTs.

IP address

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

L

LD

(*ladder diagram*) An IEC 61131-3 programming language that represents instructions to be executed as graphical diagrams very similar to electrical diagrams (contacts, coils, etc.).

local rack

An M580 rack containing a power supply, the CPU and – in an M580 safety system – the coprocessor. A local rack consists of one or two racks: the main rack and the extended rack, which belongs to the same family as the main rack. The extended rack is optional.

M

main ring

The main ring of an Ethernet RIO network. The ring contains RIO modules and a local rack (containing a CPU with Ethernet I/O scanner service) and a power supply module.

MAST

A master (MAST) task is a deterministic processor task that is run through its programming software. The MAST task schedules the RIO module logic to be solved in every I/O scan. The MAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the MAST task.
- OUT: Outputs are copied to the OUT section after execution of the MAST task.

MB/TCP

(*Modbus over TCP protocol*) This is a Modbus variant used for communications over TCP/IP networks.

Modbus

Modbus is an application layer messaging protocol. Modbus provides client and server communications between devices connected on different types of buses or networks. Modbus offers many services specified by function codes.

MTBF

(*mean time between failures*)

MTTF

(*mean time to failure*)

MTTR

(*mean time to repair*)

N

NFPA

(*National Fire Protection Association*): This is a body for establishing codes and standards for fire protection, electrical and machine Safety in the U.S.

non-interfering module

Non-interfering modules are modules that are not directly used to control the Safety Function. They do not interfere with the Safety modules (either during normal operation or if there is a fault).

NTP

(*network time protocol*) Protocol for synchronizing computer system clocks. The protocol uses a jitter buffer to resist the effects of variable latency.

P

PAC

(*programmable automation controller*) The PAC is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. PACs are computers suited to survive the harsh conditions of an industrial environment.

PELV

(*protected extra low voltage*)

PES

(*programmable electronic system*) (Definition IEC 61508)

System for control, protection or monitoring based on 1 or more programmable electronic devices, including elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices. PES is another term for a computer control system or PAC.

PFD

(*probability of failure on demand*) (Definition IEC 61508)

For a single channel system the average probability of a failure on demand is calculated as follows:

$$\text{PFD(t)}_{\text{Av}} = \frac{1}{2}\,\lambda_{DU} \bullet t$$

For a dual channel system the average probability of a failure on demand is calculated as follows:

$$\text{PFD(t)}_{\text{Av}} = \lambda_{DUCH1} \bullet \lambda_{DUCH2} \bullet t^2 + CC$$

For a dual channel system, also the Common Cause effect (CC) must be considered. The common cause effect ranges from 1% to 10% of PFD_{CH1} and PFD_{CH2}. (=1/RRF).

PFH

(*probability of failure per hour*) (Definition IEC 61508)

port mirroring

In this mode, data traffic that is related to the source port on a network switch is copied to another destination port. This allows a connected management tool to monitor and analyze the traffic.

project

A project is a user application in Control Expert XL Safety.

proof test

Periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition. (Definition IEC 61508)

proof test interval

The proof test interval is the time period between proof tests.

PS

(*power supply*)

PST

(*process safety time*) The process safety time is defined as the period of time between a failure occurring in EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed. (Definition IEC 61508)

Q

QoS

(*quality of service*) The practice of assigning different priorities to traffic types for the purpose of regulating data flow on the network. In an industrial network, QoS is used to provide a predictable level of network performance.

R

RAM

(*random access memory*)

random hardware failure

Failure, occurring at a random time, which results from 1 or more of the possible degradation mechanisms in the hardware. (Definition IEC 61508)

RIO

(*remote input/output*)

RIO drop

A rack of Ethernet I/O modules, managed by an RIO adapter, with inputs and outputs included in the RIO scan of the CPU. A drop can be a single rack or a main rack with an extended rack.

RIO network

A deterministic Ethernet-based network that includes a main ring with a local rack and CPU that performs an RIO scan of I/O modules, which may be located either in the local rack or in RIO drops. The RIO drops may be part of the main ring, one or more sub-rings, or both.

risk

Combination of the probability of occurrence of harm and the severity of that harm. (Definition IEC 61508)

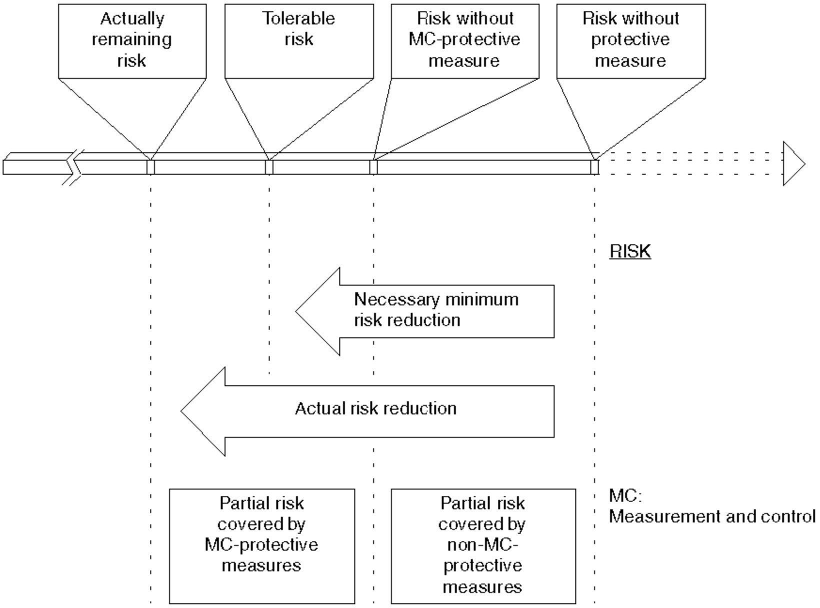
Risk is calculated using the equation R=S*H, where the letters stand for:

Letter	Meaning
R	risk
S	extent of the damage
H	frequency of occurrence of the damage

RRF

(*risk reduction factor*) (Definition IEC 61508)

The risk reduction factor equals 1/PFD.


Actually remaining risk
Tolerable risk
Risk without MC-protective measure
Risk without protective measure
RISK
Necessary minimum risk reduction
Actual risk reduction
Partial risk covered by MC-protective measures
Partial risk covered by non-MC-protective measures
MC:
Measurement and control

RSTP

(*rapid spanning tree protocol*) Allows a network design to include spare (redundant) links to provide automatic backup paths if an active link stops working, without the need for loops or manual enabling/disabling of backup links.

S

Safety Function

Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event. (Definition IEC 61508)

Safety Integrity

Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. (Definition IEC 61508)

Safety PAC

M580 safety PAC (BMEP58•040S or BMEH58•040S CPU with BMEP58CPROS3 coprocessor)

Safety variable

Variable used to implement a Safety Function in a Safety-Related System.

Safety-Related System

This term designates a system that both

- implements the required Safety Functions necessary to achieve or maintain a Safe state for the EUC and
- is intended to achieve, on its own or using other E/E/PE Safety-Related Systems, other technology Safety-Related Systems, or external risk reduction facilities, the necessary Safety Integrity for the required Safety Functions.

SCADA

(*supervisory control and data acquisition*) SCADA systems are computer systems that control and monitor industrial, infrastructure, or facility-based processes (examples: transmitting electricity, transporting gas and oil in pipelines, and distributing water).

scanner

A scanner acts as the originator of I/O connection requests for implicit messaging in EtherNet/IP, and message requests for Modbus TCP.

service port

A dedicated Ethernet port on the M580 RIO modules. The port may support these major functions (depending on the module type):

- port mirroring: for diagnostic use
- access: for connecting HMI/Control Expert/ConneXview to the CPU
- extended: to extend the device network to another subnet
- disabled: disables the port, no traffic is forwarded in this mode

SFC

(*sequential function chart*) An IEC 61131-3 programming language that is used to graphically represent in a structured manner the operation of a sequential CPU. This graphical description of the CPU's sequential behavior and of the various resulting situations is created using simple graphic symbols.

SFF

(*safe failure fraction*)

SFR

(*safety functional requirement*) Safety functional requirements are derived from the hazard analysis and define what the function does, for instance the safety function to be performed.

SIL

(*safety integrity level*) Discrete level (1 out of a possible 4) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.(Definition IEC 61508)

NOTE: For complete definitions and parameters related to SIL ratings refer to IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety related systems”. Provided here is a partial definition.

SIL3 project (application)

A project (application) that uses an M580 safety PAC to implement safety functions in a safety-related system.

simple daisy chain loop

Often referred to as SDCL, a simple daisy chain loop contains RIO modules only (no distributed equipment). This topology consists of a local rack (containing a CPU with Ethernet I/O scanner service), and one or more RIO drops (each drop containing an RIO adapter module).

SIR

(*safety integrity requirement*) Safety integrity requirements are derived from a risk assessment and describe the likelihood of a Safety Function to be performed satisfactorily, for instance the degree of certainty necessary for the Safety Function to be carried out.

SRS

(*safety requirements specification*) Specification containing all the requirements of the safety functions that have to be performed by the safety-related systems. (Definition IEC 61508)

SRT

(*system reaction time*) The system reaction time is the period of time between detection of a signal at the input module terminal and the reaction of setting an output at the output module terminal.

SSC

(*system safety concept*) This is a detailed description of the system architecture, configuration and diagnostics required to achieve Functional Safety.

ST

(*structured text*) An IEC 61131-3 programming language that presents structured literal language and is a developed language similar to computer programming languages. It can be used to organize a series of instructions.

Statement of Consequence

This is the last line within all special messages. It begins with "**Failure to follow these instructions**..."

sub-ring

An Ethernet-based network with a loop attached to the main ring, via a dual-ring switch (DRS) or BMENOS0300 network option switch module on the main ring. This network contains RIO or distributed equipment.

switch

A multi-port device used to segment the network and limit the likelihood of collisions. Packets are filtered or forwarded based upon their source and destination addresses. Switches are capable of full-duplex operation and provide full network bandwidth to each port. A switch can have different input/output speeds (for example, 10, 100 or 1000Mbps). Switches are considered OSI layer 2 (data link layer) devices.

systematic failure

Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. (Definition IEC 61508)

T

TCP

(*transmission control protocol*) A key protocol of the internet protocol suite that supports connection-oriented communications, by establishing the connection necessary to transmit an ordered sequence of data over the same communication path.

TCP/IP

Also known as *internet protocol suite*, TCP/IP is a collection of protocols used to conduct transactions on a network. The suite takes its name from two commonly used protocols: transmission control protocol and internet protocol. TCP/IP is a connection-oriented protocol that is used by Modbus TCP and EtherNet/IP for explicit messaging.

TÜV

(*Technischer Überwachungsverein*) (German for Association for Technical Inspection)

U

UDP

(*user datagram protocol*) A transport layer protocol that supports connectionless communications. Applications running on networked nodes can use UDP to send datagrams to one another. Unlike TCP, UDP does not include preliminary communication to establish data paths or provide data ordering and checking. However, by avoiding the overhead required to provide these features, UDP is faster than TCP. UDP may be the preferred protocol for time-sensitive applications, where dropped datagrams are preferable to delayed datagrams. UDP is the primary transport for implicit messaging in EtherNet/IP.

UMAS

(*Unified Messaging Application Services*) UMAS is a proprietary system protocol that manages communications between Control Expert and a controller.

UTC

(*coordinated universal time*) Primary time standard used to regulate clocks and time worldwide (close to former GMT time standard).

V

VDE

(*Verband Deutscher Elektroingenieure*) This is the German equivalent of the IEEE.

W

warm start

Warm start refers to restarting the computer without turning the power off.

Index