

Section 8.2

M580 Safety Module SIL & MTTF Values

Safety Integrity Level Calculations

Classification of the Schneider Electric Products

The M580 safety PAC can consist of:

- Safety modules, which can perform safety functions, including:
 - CPU and coprocessor
 - I/O modules
 - power supply
- Non-interfering modules (*see page 25*), which do not perform safety functions, but enable you to add non-safety elements to your safety project.

NOTE:

- Because non-interfering modules are not part of the safety loop, they are not part of safety integrity level calculations.
- An error detected in a non-interfering module does not negatively impact the execution of the safety functions.
- The BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S power supplies are certified. Because they present a negligible dangerous failure rate (<1% of the SIL3 target), the power supply is not included in safety integrity level calculations for the safety loop. As a consequence, neither PFH nor PFD are provided for the power supply modules.

PFD/PFH Values for M580 Safety Modules

Schneider Electric offers the following safety modules certified for use in safety applications. The safety modules are listed with their corresponding probabilities of failure (*see page 142*) (PFD/PFH) values for different proof test intervals (*see page 144*) (PTIs). The PFD/PFH are expressed as values that contribute to the overall PFD/PFH of the entire safety loop (*see page 16*).

The tables below list the safety modules and their PFD/PFH values for SIL2 and SIL3 applications, where applicable:

Product Type	Product Reference	SIL	PTI = 1 year	
			PFD _G	PFH _G
CPU with Copro	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.26E-07	9.73E-11
Analog input	BMXSAI0410	SIL3 ²	5.76E-06	1.31E-09
Digital input	BMXSDI1602	SIL3 ²	6.81E-06	1.56E-09
Digital output	BMXSDO0802	SIL3 ¹	5.75E-06	1.31E-09
Digital relay output	BMXSRA0405	SIL2 ³	5.85E-06	1.58E-09
		SIL3 ⁴	5.84E-06	1.34E-09
		SIL3 ⁵	–	1.35E-09
Power supply	BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S	SIL3	–	–
1. 1 output @ 80° C 2. 1 input @ 80° C 3. 1 relay per output @ 80° C 4. 2 relays per output @ 80° C 5. 4 relays per output @ 80° C				

Product Type	Product Reference	SIL	PTI = 5 years	
			PFD _G	PFH _G
CPU & Copro	BME•58•040S & BMEP58CPROS3	SIL3 ¹	2.14E-06	9.81E-11
Analog input	BMXSAI0410	SIL3 ²	2.88E-05	1.31E-09
Digital input	BMXSDI1602	SIL3 ²	3.41E-05	1.56E-09
Digital output	BMXSDO0802	SIL3 ¹	2.88E-05	1.31E-09
Digital relay output	BMXSRA0405	SIL2 ³	2.92E-05	1.68E-09
		SIL3 ⁴	2.92E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09
Power supply	BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S	SIL3	–	–
1. 1 output @ 80° C 2. 1 input @ 80° C 3. 1 relay per output @ 80° C 4. 2 relays per output @ 80° C 5. 4 relays per output @ 80° C				

Product Type	Product Reference	SIL	PTI = 10 years	
			PFD _G	PFH _G
CPU & Copro	BME•58•040S & BMEP58CPROS3	SIL3 ¹	4.37E-06	9.91E-11
Analog input	BMXSAI0410	SIL3 ²	5.76E-05	1.31E-09
Digital input	BMXSDI1602	SIL3 ²	6.81E-05	1.56E-09
Digital output	BMXSDO0802	SIL3 ¹	5.75E-05	1.31E-09
Digital relay output	BMXSRA0405	SIL2 ³	5.84E-05	1.68E-09
		SIL3 ⁴	5.84E-05	1.34E-09
		SIL3 ⁵	–	1.35E-09
Power supply	BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S	SIL3	–	–
1. 1 output @ 80° C 2. 1 input @ 80° C 3. 1 relay per output @ 80° C 4. 2 relays per output @ 80° C 5. 4 relays per output @ 80° C				

Product Type	Product Reference	SIL	PTI = 20 years	
			PFD _G	PFH _G
CPU & Copro	BME•58•040S & BMEP58CPROS3	SIL3 ¹	8.74E-06	7.01E-10
Analog input	BMXSAI0410	SIL3 ²	1.15E-04	1.31E-09
Digital input	BMXSDI1602	SIL3 ²	1.36E-04	1.56E-09
Digital output	BMXSDO0802	SIL3 ¹	1.15E-04	1.31E-09
Digital relay output	BMXSRA0405	SIL2 ³	1.17E-04	1.68E-09
		SIL3 ⁴	1.17E-04	1.34E-09
		SIL3 ⁵	–	1.35E-09
Power supply	BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S	SIL3	–	–
1. 1 output @ 80° C 2. 1 input @ 80° C 3. 1 relay per output @ 80° C 4. 2 relays per output @ 80° C 5. 4 relays per output @ 80° C				

MTTF Values for M580 Safety Modules

The M580 safety modules present the following MTTF characteristics:

Product Type	Product Reference	MTTF (years)		
		25° C	55° C	>60° C
CPU	BME•58•040S	73.8	38.3	21.1
Coprocessor	BMEP58CPROS3	108.0	56.0	30.1
Analog input	BMXSAI0410	54.2	26.1	14.2
Digital input	BMXSDI1602	31.5	13.0	6.1
Digital output	BMXSDO0802	45.8	25.0	13.4
Digital relay output	BMXSRA0405	36.9	26.5	17.9
Power supply	BMXCPS4002S, BMXCPS4022S, and BMXCPS3522S	88.0	47.5	25.4

Probabilities of Failure for SIL3 Applications

For SIL3 applications, the IEC 61508 defines the following probabilities of failure on demand (PFD) and probabilities of failure per hour (PFH) for each safety loop, depending on the mode of operation:

- $PFD \geq 10^{-4}$ to $< 10^{-3}$ for low demand mode of operation
- $PFH \geq 10^{-8}$ to $< 10^{-7}$ for high demand mode of operation

The M580 Safety PAC is certified for use in low and high demand systems.

Safety Integrity Level Sample Calculation

This sample calculation shows you how to determine:

- The risk contribution of the Schneider Electric safety modules to your safety application; and
- The remaining amount of risk that other devices in the safety loop (for example, sensors and actuators) can contribute to your safety application for a given safety integrity level and mode of operation.

NOTE: When calculating the risk contribution of sensors and actuators to your safety application, contact the manufacturers of these devices and obtain the PFD/PFH values for the appropriate proof test interval.

The following Schneider Electric safety modules are included in this example:

- 1: BMEP584040S CPU
- 1: BMEP58CPROS3 Copro
- 1: BMXSAI0410 Analog input
- 1: BMXSDO0802 Digital output
- 1: BMXCPS4002S Power supply

The following calculation employs PFH_G values for a high demand mode of operation for a SIL3 safety loop with a PTI of 20 years. The maximum permissible PFH value for this safety application is 10^{-7} (or $1.0E-7$):

Safety module		Contribution (Scientific Notation)	Remaining Contribution for Sensors & Actuators
CPU with Copro		7.01E-10	–
Analog input		1.31E-09	
Digital output		1.31E-09	
Power Supply		–	
Total	numeric	2.72E-09	97.28E-09
	% max	2.72%	97.28%
note 1: The relay output uses four relays to support one output.			

Values for M580 Safety Modules for Machinery

Schneider Electric offers the following safety modules certified for use in safety machinery applications according to ISO13849-1 standard. The table below list the safety modules and their values, category and level where applicable:

Product Type	Product Reference	Configuration	Category	Performance Level	MTTFd (years)	DCav
CPU with Copro	BME•58•040S & BMEP58CPROS3	NA	4	e	235	High (>99%)
Analog input	BMXSAI0410	using 1 channel	2	d	255	99.66%
		using 2 channels	4	e	255	99.66%
Digital input	BMXSDI1602	using 1 channel	2	d	231	99.69%
		using 2 channels	4	e	231	99.69%
Digital output	BMXSDO0802	NA	4	e	253	99.63%
Digital relay output	BMXSRA0405	using 1 channel	2	c	156	99.77%
		using 2 channels	4	e	156	99.77%

Safety Times Description

The M580 safety PAC has a minimum PAC cycle time of 10 ms, which is necessary for processing the signals from the I/O modules, executing the program logic, and setting the outputs. For calculating the maximum PAC reaction time, you need to know the maximum reaction time of the sensors and actuators that are being used. In addition, the maximum PAC reaction time depends on the process safety time (PST) (*see page 146*) required for your process.

Proof Test Interval

The proof test is a periodic test you need to perform to detect failures in a safety-related system so that, if necessary, the system can be restored to a like new condition or as close as practical to this condition. The time period between these tests is the proof test interval.

The proof test interval depends on the targeted safety integrity level, the sensors, actuators and the PAC application. The M580 safety system is suitable for use in a SIL3 application and a proof test interval of 20 years.