Enabling Engineering
Breakthroughs that Lead to a
Better Tomorrow

vibro-meter

VM600 MK2 SIL2

presented by Michaël Hafner,

Product Manager

May 2024

Parker MEGGiTT

AGENDA

1. What is the SIL about and SIL certification
2. VM600 MK2 SIL
    - Presentation of VM600 Mk2 SIL and product evolution
    - High level comparison of VM600 Mk1, Mk2 and SIL certifications
    - Integration with Parker-Meggitt SIL2 measurement chains
    - SIL2 certificate
    - Safety manual
    - Next product evolution (road map)

1. What is the SIL about and SIL certification

SIL Certification

What is functional safety?

RISK

To what risk am I exposed?

Height?

5 seconds? 15 minutes?
Every day?

Landing zone?

Risk reduction measures

Probability of failures?

Was the gear well designed?
Well manufactured?

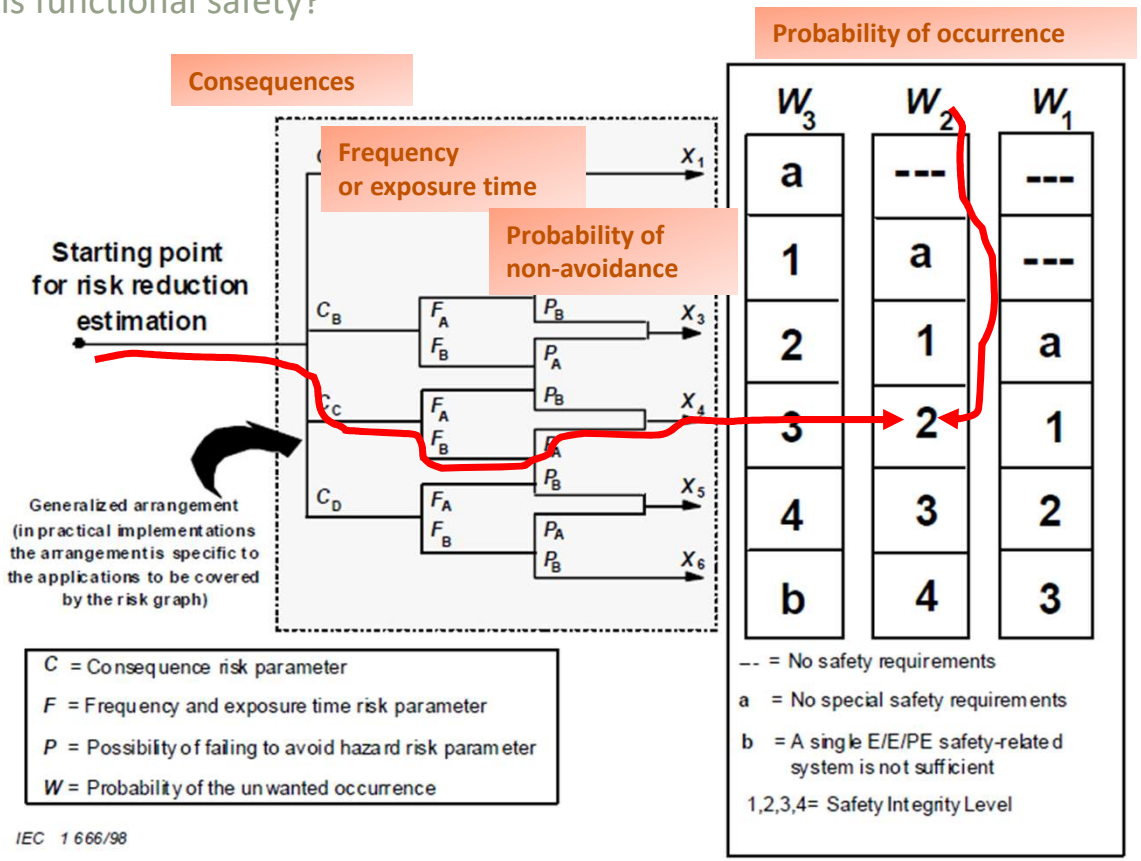
Is there a defect?
Is it scratching on a rock?

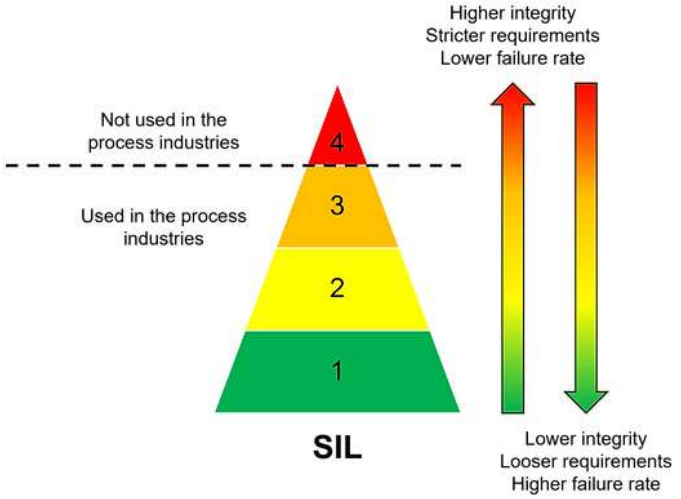
The main goal of functional safety is to ensure that: **"…The safety function will be performed correctly, or the system will fail in a predictable and safe manner. "**

SIL Certification

What is functional safety?

To what risk am I exposed?





Evaluation of risk

SIL Certification

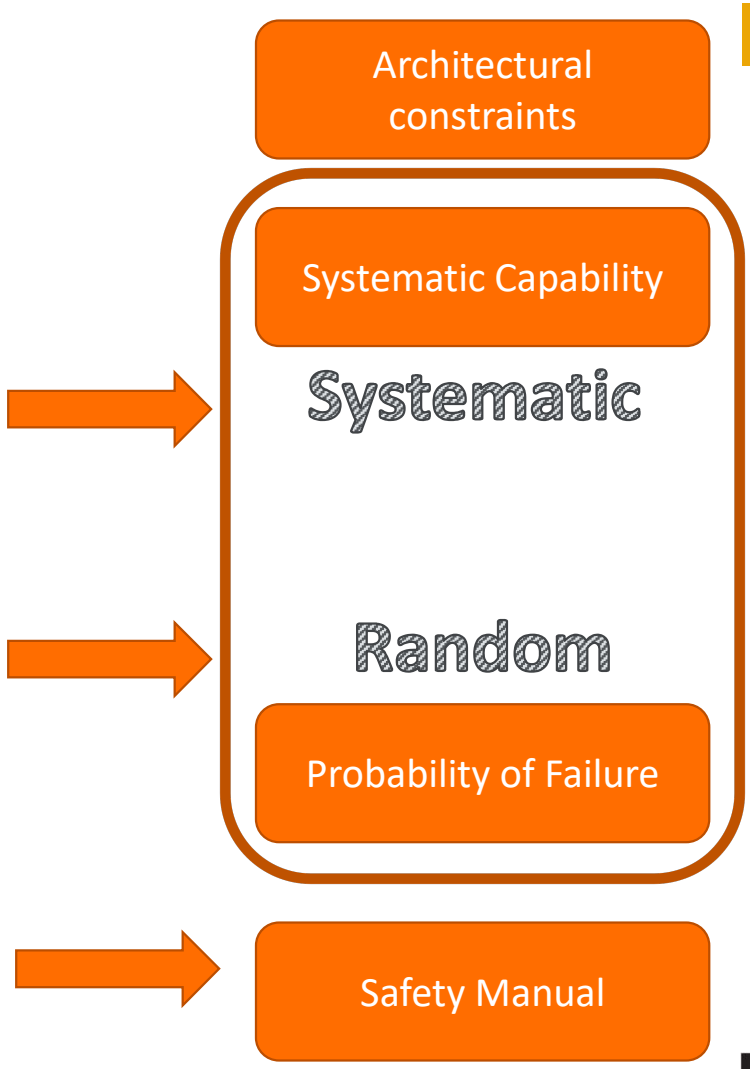
What is functional safety?

Risk reduction effectiveness?

Was the VM600 protection system well designed?
Well manufactured?
Was it properly configured and installed?

Is there a defect in the VM600 protection system?
Is one relay output stuck?

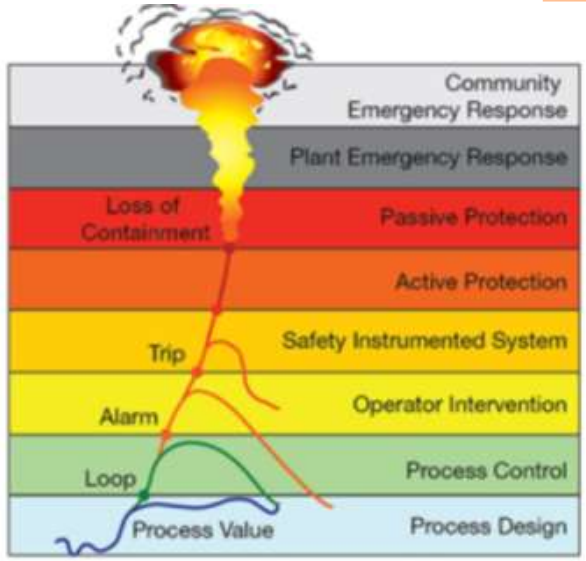
Am I using it properly?
Is it appropriated for my case?

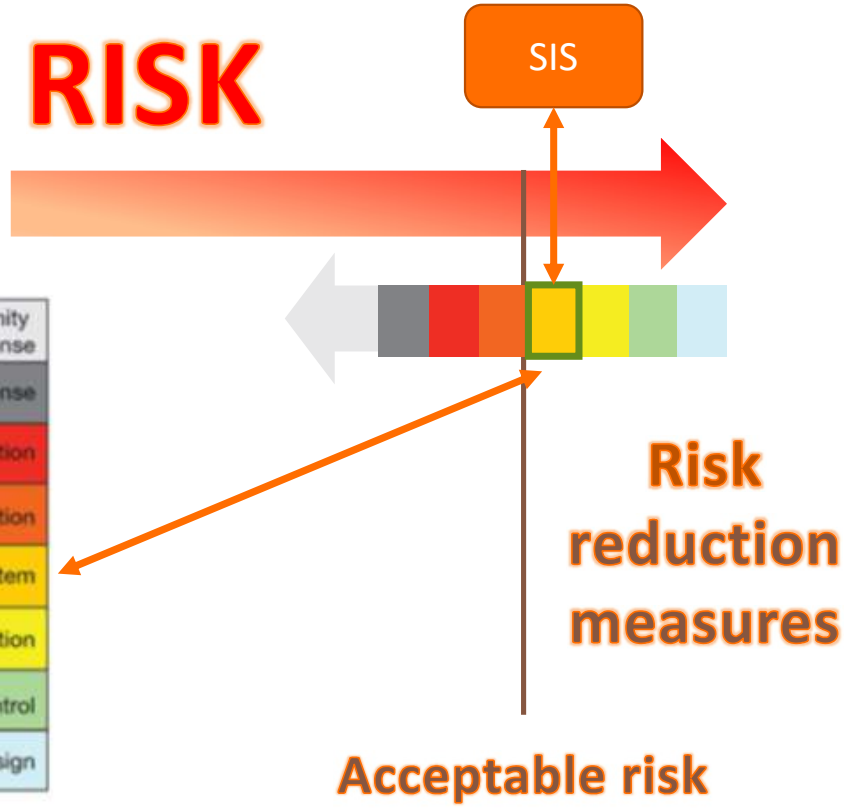


SIL Certification

Why SIL certification is important?

Risks and hazards





To what risk am I exposed?

Risk Reduction Factor	Probability of Failure on Demand	Safety Integrity Level (SIL)
10 to 100	0.1 to 0.01	SIL 1
100 to 1'000	0.01 to 0.001	SIL 2
1'000 to 10'000	0.001 to 0.0001	SIL 3
10'000 to 100'000	0.0001 to 0.00001	SIL 4

2. VM600 MK2 SIL

Presentation of VM600 Mk2 SIL and product evolution

VM600 system product evolution

Timeline summary

CPUM/CPUR
Communication

MPC4/ AMC8

XMV16

CPUM^{MK2}

MPC4^{MK2}

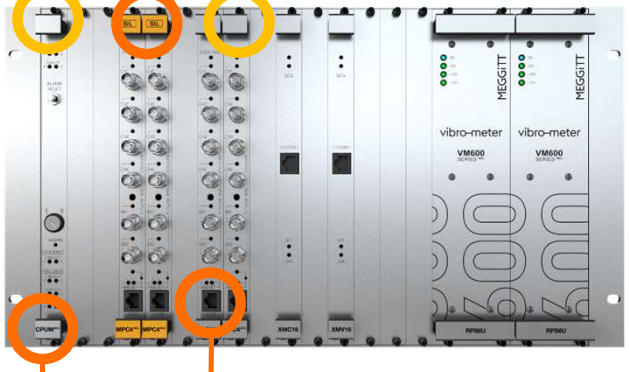
Condition
monitoring on
MPC4^{MK2}

New look

Additional
communication protocols,
ie Profinet

MPC4^{MK2} SIL

AMC10^{MK2}



Redundant
CPUM^{MK2}

Ethernet port
on the back

VM600 (1st generation) — 2000

MPC4 SIL1 — 2009

MPC4 SIL1 dedicated card — 2010

VM600 SIL2 — 2018

VM600^{MK2} new generation — 2021

VM600^{MK2} SIL2 — 2024

2025…

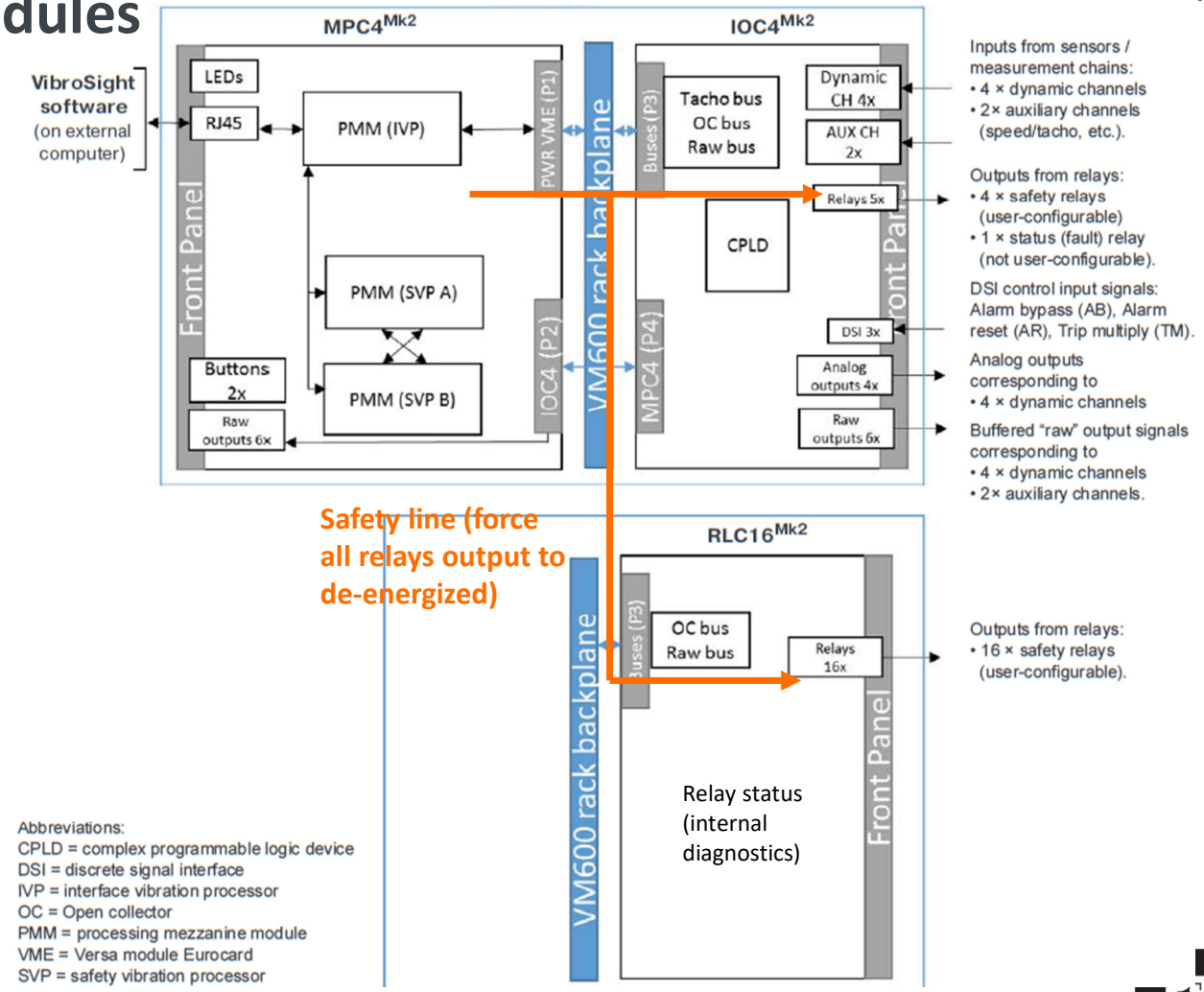
VM600 Mk2 SIL2 modules

Presentation of the concept

Each MPC4 SIL2 module has 3 processors:

- 2 dedicated for protection (SIL)
- 1 dedicated for communication and condition monitoring

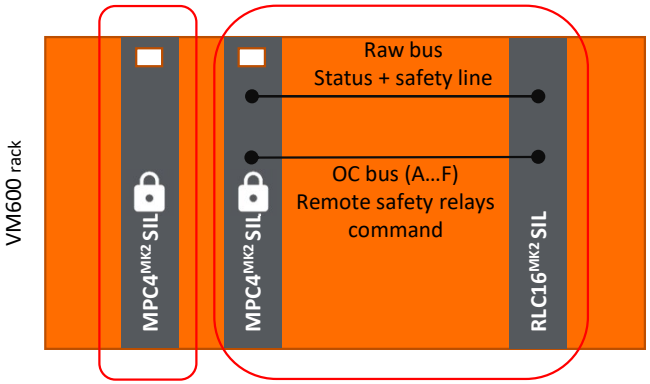
Continuous internal diagnostics to monitor state of the system
-> system goes to fail safe if detected critical problem, in this case force safe outputs, relays to de-energized



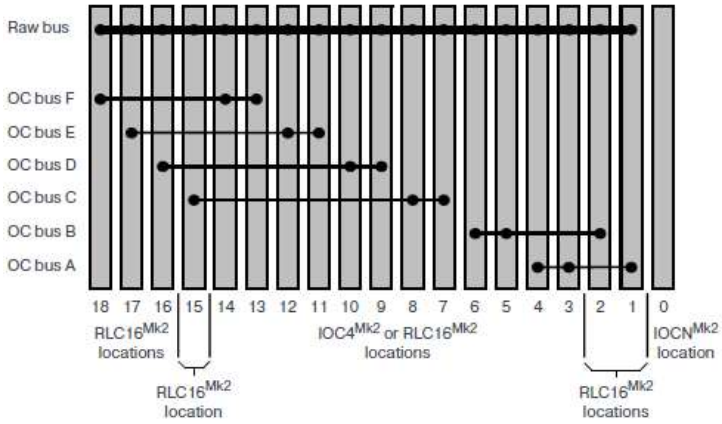
Abbreviations:
CPLD = complex programmable logic device
DSI = discrete signal interface
IVP = interface vibration processor
OC = Open collector
PMM = processing mezzanine module
VME = Versa module Eurocard
SVP = safety vibration processor

VM600 Mk2 SIL2 System

Definition of a MK2 SIL2 system and its integration within the VM600 rack

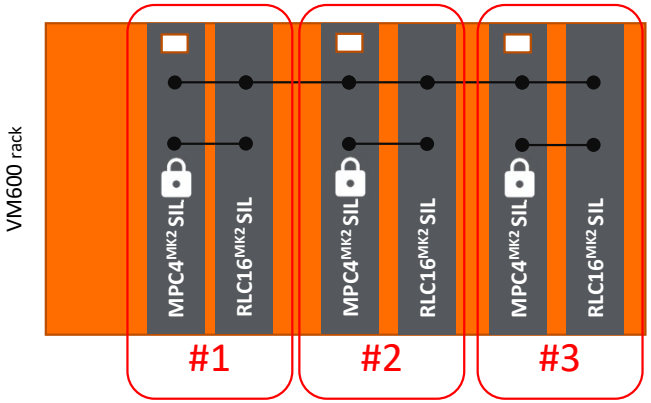


One SIL2 system is composed of MPC4 + IOC4 Mk2 SIL modules and 1 RLC16 Mk2 SIL module (optional)
Other cards non SIL can be installed in the VM600 rack



Restrictions according to the VM600 rack backplane OC bus connections

Up to 5 independant SIL2 systems with RLC16 can coexist in one VM600 rack
Example with 3 SIL2 systems:



Raw bus
3 different set of Status + safety lines

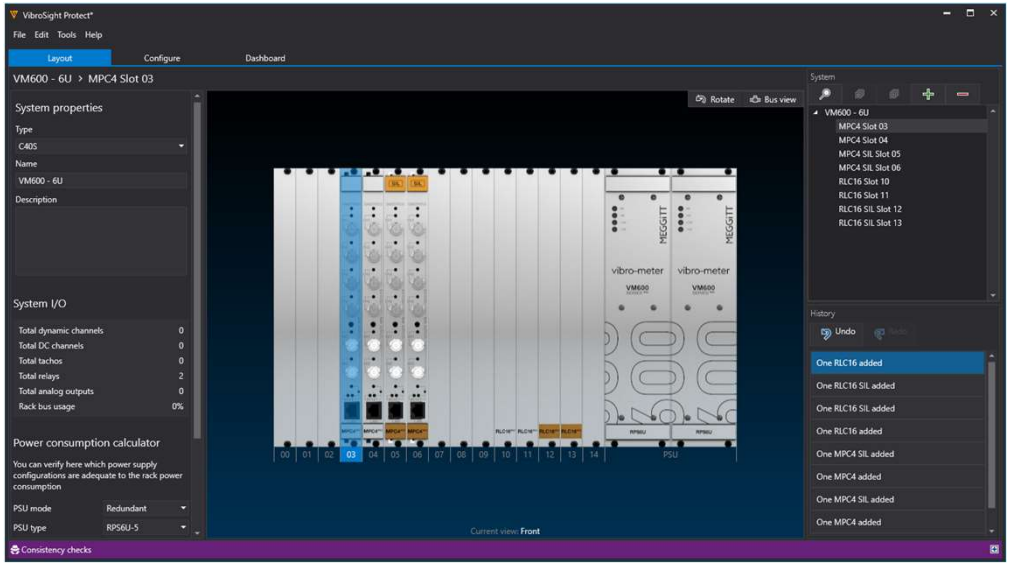
3 different OC bus used

Differences between VM600 Mk2 standard and SIL modules

Differences between Standard and SIL modules

VM600MK2 SIL machinery protection system

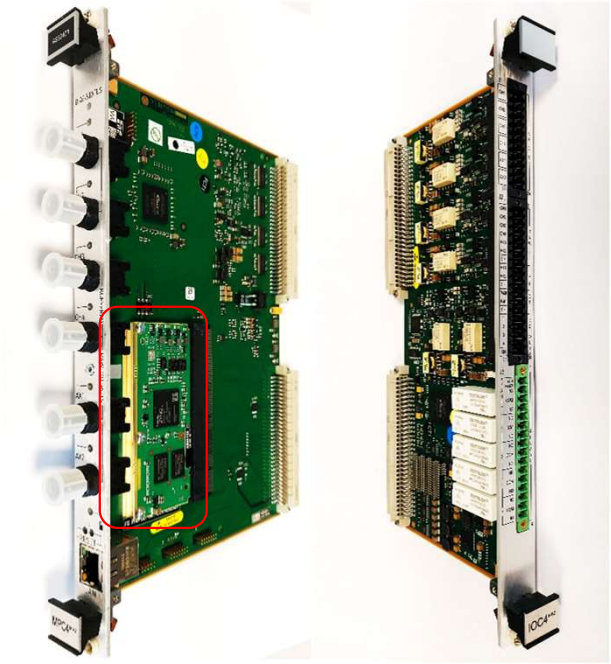
- Designed to minimize the differences of behavior between the MK2 standard and SIL modules
- Two different modules type reflected in VibroSight Protect
- Additional configuration consistency checks for SIL modules



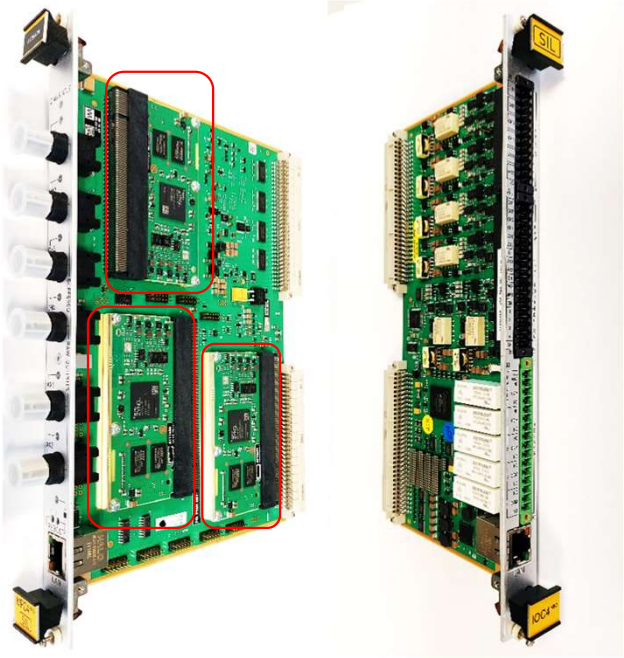
Differences between Standard and SIL modules

The looks

STD



SIL



Differences between Standard and SIL modules

Firmwares

STD

Condition monitoring firmware is optional and require a license for the MPC4 module

Proof test firmware is renamed as **Protection test** firmware to avoid confusion for SIL certification

MPC4^{Mk2} (standard) module firmware	Description
Machinery protection firmware (640-025-vvv-ppp.Mpc4g2Fw)	The machinery protection firmware runs on a MPC4^{Mk2} module in order to provide the machinery protection system (MPS) functionality required by a system. Note: All MPC4^{Mk2} module's run machinery protection firmware.
Condition monitoring firmware (640-033-vvv-ppp.VxeFw)	The condition monitoring firmware runs on a MPC4^{Mk2} module in order to provide the condition monitoring system (CMS) functionality required by a system. Note: Only MPC4^{Mk2} module's with a MPC4^{Mk2} CMS license can run condition monitoring firmware. For further information, see 4.3 VibroSight / VM600^{Mk2} MPC4^{Mk2} condition monitoring licensing.
Recovery firmware (640-031-vvv-ppp.Mpc4g2Fw)	The recovery firmware allows a MPC4^{Mk2} module to be recovered in the unlikely event of a problem with the module, such as corrupted operational firmware (machinery protection and/or condition monitoring) or a corrupted configuration. Note: It is important to note that entering the Recovery mode automatically clears the module's configuration.
Proof test firmware (640-032-vvv-ppp.VxeFw)	The proof test firmware is used to run a specific diagnostic proof test on the MPC4^{Mk2} module in order to verify the status of the module and its components (hardware and firmware). Note: Use of proof testing is primarily intended for safety-related applications.

Notes

The different MPC4^{Mk2} (standard) module firmware is identified by different part numbers (PNRs) as follows:
- The machinery protection firmware is identified by the part number (PNR): 640-025-vvv-ppp (file name 640-025-vvv-ppp and file name extension .Mpc4g2Fw).
- The condition monitoring firmware is identified by the part number (PNR): 640-033-vvv-ppp (file name 640-033-vvv-ppp and file name extension .VxeFw).
- The recovery firmware is identified by the part number (PNR): 640-031-vvv-ppp (file name 640-031-vvv-ppp and file name extension .Mpc4g2Fw).
- The proof test firmware is identified by the part number (PNR): 640-032-vvv-ppp (file name 640-032-vvv-ppp and file name extension .VxeFw).

In a MPC4^{Mk2} module firmware part number (PNR):
- vvv represents the version number of the firmware.
- ppp represents the patch number of the firmware.

For example, PNR 640-025-008-000 is the latest official release of machinery protection firmware (version 8, patch 0) for the MPC4^{Mk2} (standard) module. For further information on MPC4^{Mk2} module firmware, refer to the latest version of the *VibroSight software release notes*.

SIL

MPC4^{Mk2} SIL module firmware	Description
SIL machinery protection firmware (640-024-vvv-ppp.SafeMpc4g2Fw)	The SIL machinery protection firmware runs on a MPC4^{Mk2} module in order to provide the machinery protection system (MPS) functionality required by a system. Note: All MPC4^{Mk2} module's run machinery protection firmware.
Condition monitoring firmware (640-033-vvv-ppp.VxeFw)	The condition monitoring firmware runs on a MPC4^{Mk2} module in order to provide the condition monitoring system (CMS) functionality required by a system. Note: Only MPC4^{Mk2} module's with a MPC4^{Mk2} CMS license can run condition monitoring firmware. For further information, see 4.3 VibroSight / VM600^{Mk2} MPC4^{Mk2} condition monitoring licensing.
SIL recovery firmware (640-026-vvv-ppp.SafeMpc4g2Fw)	The SIL recovery firmware allows a MPC4^{Mk2} module to be recovered in the unlikely event of a problem with the module, such as corrupted operational firmware (machinery protection and/or condition monitoring) or a corrupted configuration. Note: It is important to note that entering the Recovery mode automatically clears the module's configuration.
Proof test firmware (640-032-vvv-ppp.VxeFw)	The proof test firmware is used to run a specific diagnostic proof test on the MPC4^{Mk2} module in order to verify the status of the module and its components (hardware and firmware). Note: Use of proof testing is primarily intended for safety-related applications.

Firmware versions

Machinery protection firmware:	640-024-001-000
SIL firmware:	640-019-001-000 (0x9434feb2)
SIL programmable logic:	640-016-102-000 (0x22d9fa8b)
Condition monitoring firmware:	640-033-005-000
Recovery firmware:	640-026-001-000
Protection test firmware:	640-032-004-000

ers (PNRs) as follows:
640-024-vvv-ppp
-033-vvv-ppp
vvv-ppp
-ppp

chinery protection firmware (version 1, test 5) for the MPC4^{Mk2} SIL module. For further information on MPC4^{Mk2} module firmware, refer to the latest version of the *VibroSight software release notes*.

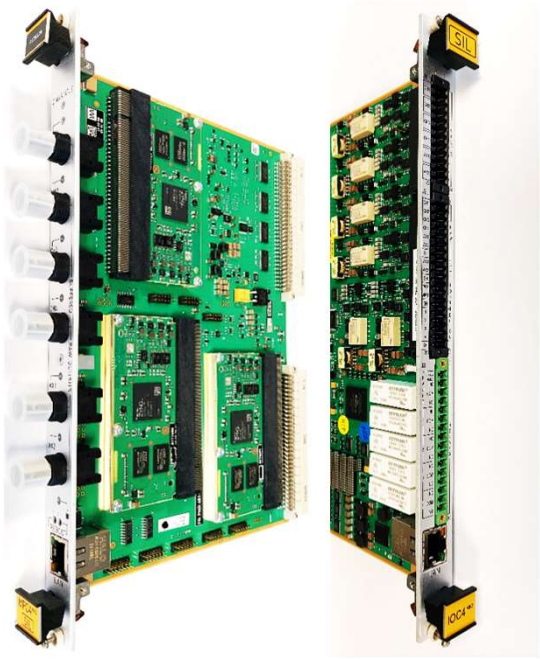
Differences between Standard and SIL modules

Input channels

MPC4 STD
Channel 1
Channel 2
Channel 3
Channel 4
Speed 1/Aux 1
Speed 2/Aux 2

No Ethernet connection on IOC4 MK2 Standard. Will be available with updated version coming in July 2024

MPC4 SIL	
Channel 1	
Channel 2	
Channel 3	
Channel 4	
Speed 1	Aux 1
	Aux 2



Only 1 speed channel – must be connected to both inputs for diagnostics reasons
Ethernet connection on IOC4 MK2 SIL

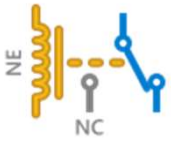
Differences between Standard and SIL modules

Relay settings

STD

Relays can be latched or unlatched and NE or NDE

SIL



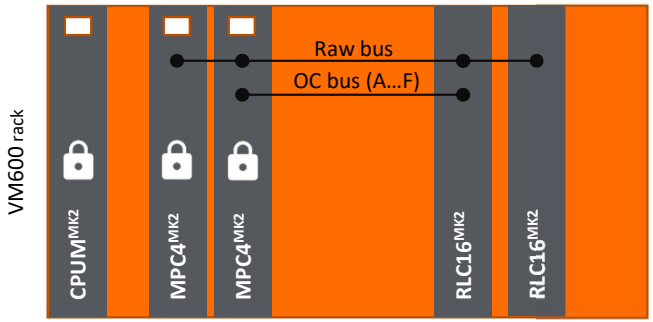
Relays can be latched or unlatched and must NE

Note: when unlatched, the relay will keep for min 500 ms its state before switching back if the alarm is intermittent

Differences between Standard and SIL modules

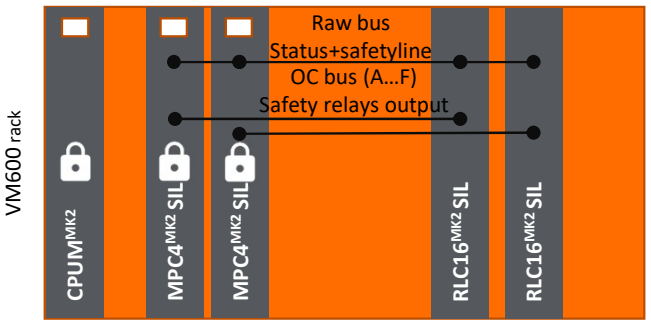
Additional relay cards

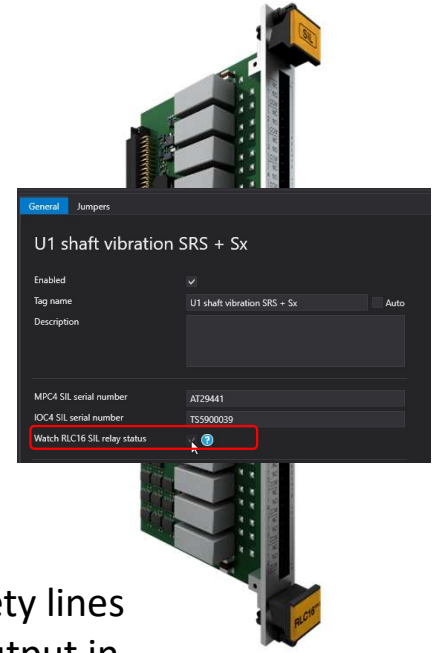
STD



Raw bus or OC bus can be used to drive external relays on RLC16 modules

SIL



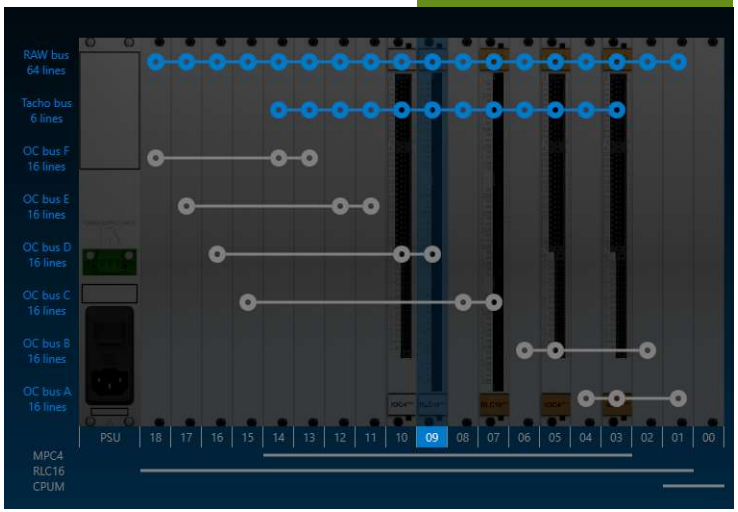


Raw bus is used for diagnostics and safety lines (force relays of RLC16 to go to “safe” output in case of problem)
OC bus only is used to drive relays on RLC16 module

Differences between Standard and SIL modules

VM600 backplane buses usage

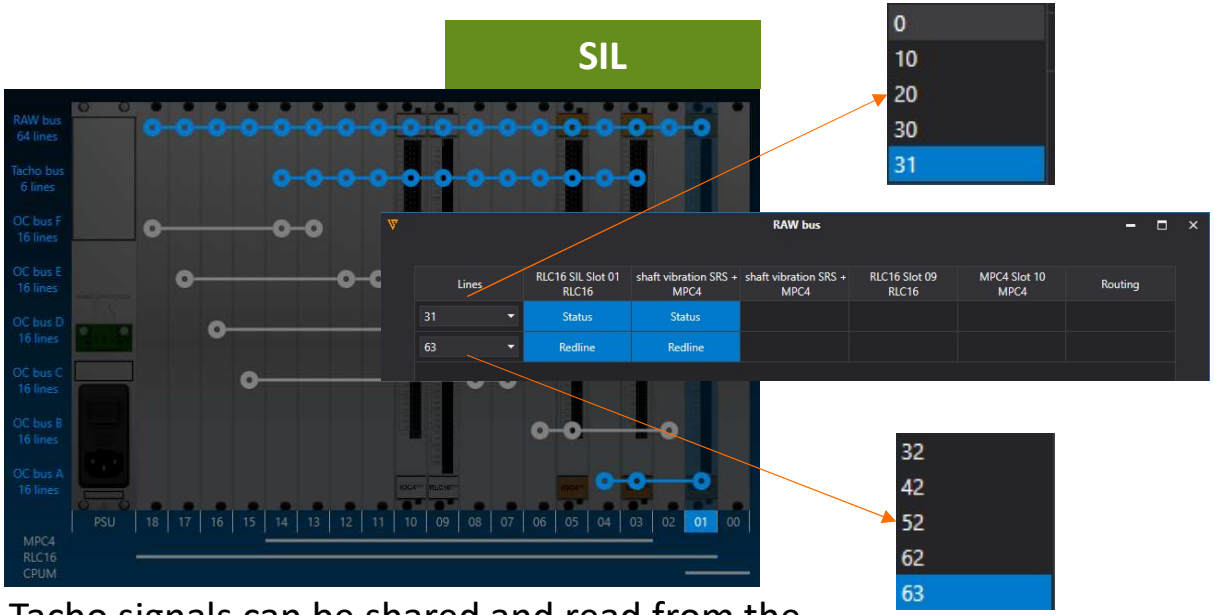
STD



Tacho signals can be shared and read from the VM600 tacho bus

RLC16 remote relays via raw bus or OC bus

SIL



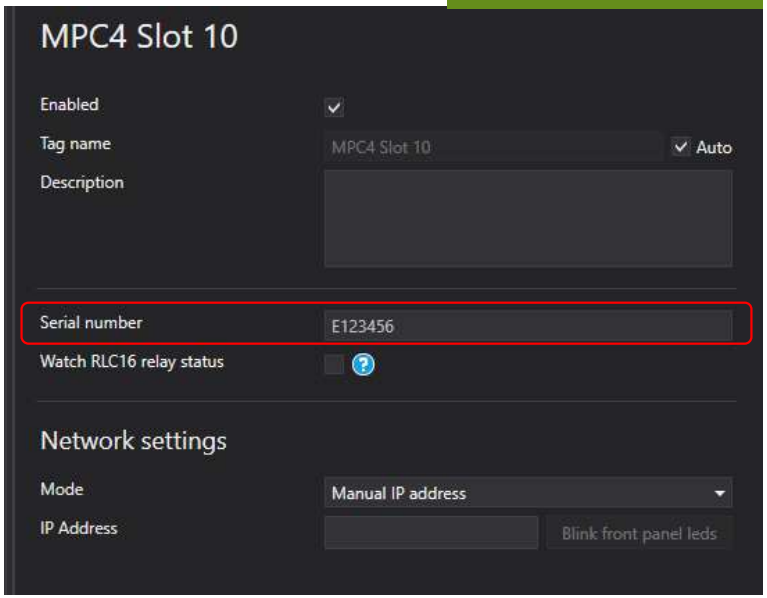
Tacho signals can be shared and read from the VM600 tacho bus but not used for safety related protection

RLC16 remote relays via OC bus only. Use of 2 raw bus lines for diagnostic feedback and safety line between MPC4 SIL and of RLC16 SIL modules

Differences between Standard and SIL modules

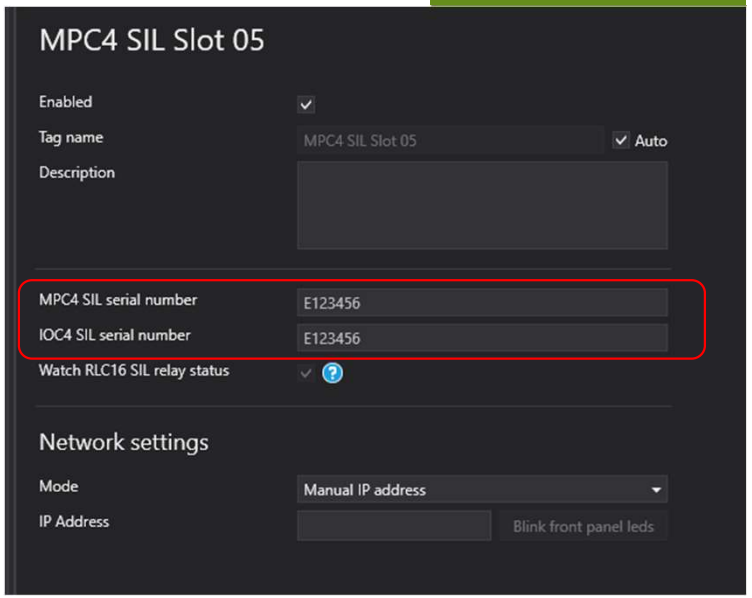
Serial number verification

STD



Verification of MPC4 serial number

SIL



Verification of MPC4 and IOC4 serial numbers

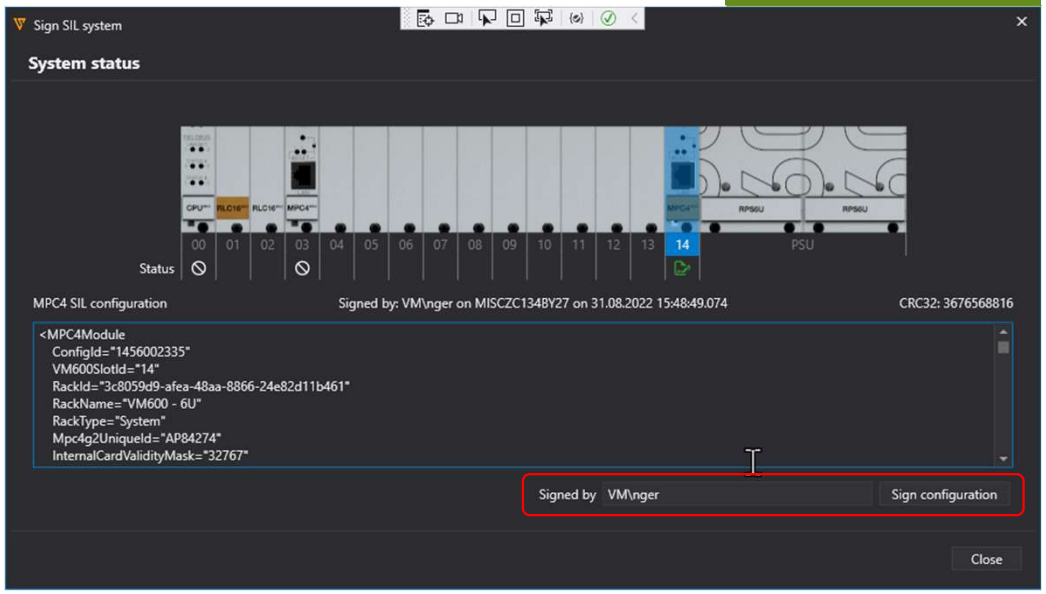
Differences between Standard and SIL modules

Protection configuration

STD

Protection configuration just must be activated

SIL



Protection configuration must be activated and then signed

Good practice for standard and mandatory for SIL is to validate by commissioning that the behavior is according to expectation by testing

Differences between Standard and SIL modules

Card lock

STD

Protects the machine either
locked or unlocked

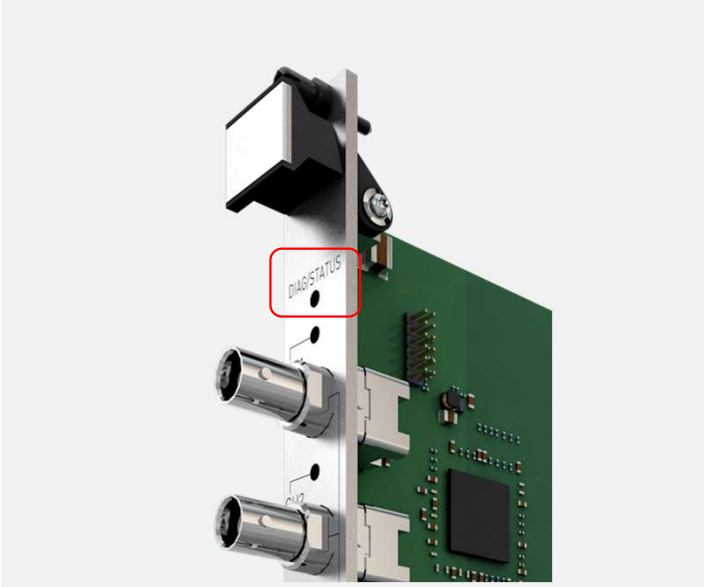
SIL

Must be locked to fulfil the SIL requirements
All diagnostics are enabled and run in “safe mode”
Card will not go to fail safe mode when unlocked

Differences between Standard and SIL modules

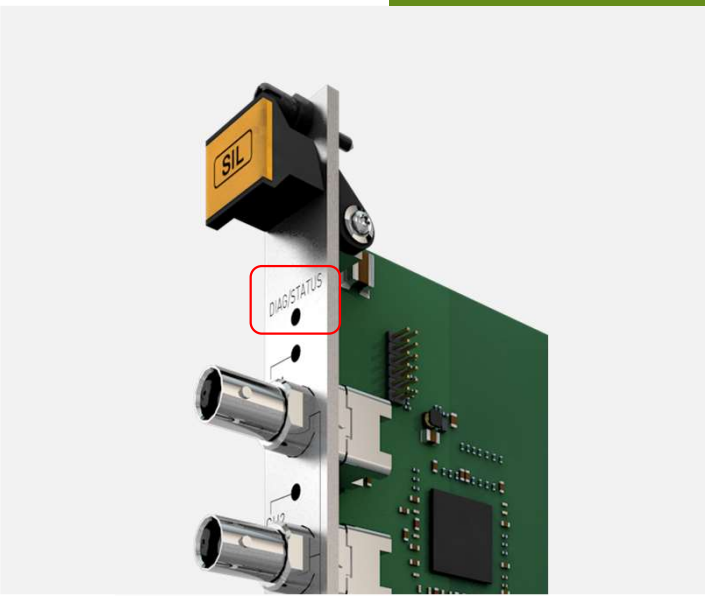
Auto-fault diagnosis

STD



Hardware fault diagnosis

SIL

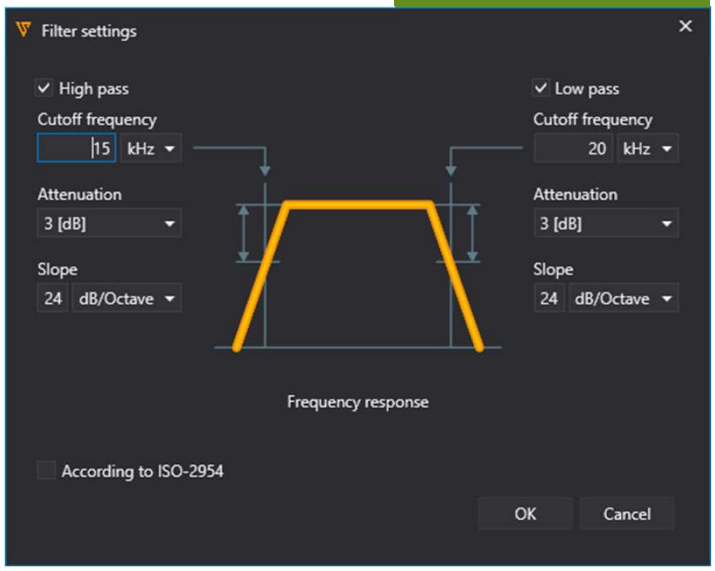


Extended hardware fault diagnosis and error correction memory for protection processors (not with condition monitoring and communication processor)

Differences between Standard and SIL modules

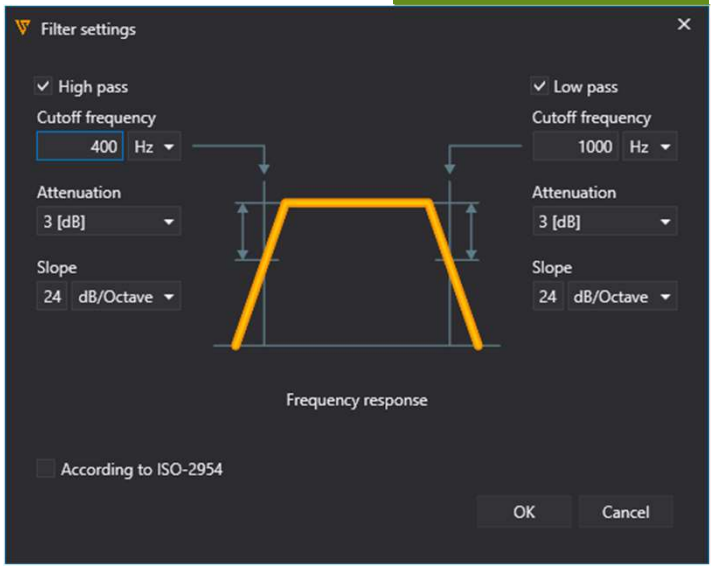
Digital high pass cutoff frequency

STD



Up to 15 kHz

SIL



Up to 400 Hz

Differences between Standard and SIL modules

MPC4 auto-configuration after card replacement (hot-swap)

STD

The replacement MPC4 it is auto-configured by the IOC4

SIL

The replacement MPC4 must be manually configured using VibroSight Protect

Differences between Standard and SIL modules

Summary table (1)

Standard versions: MPC4^{MK2} + IOC4^{MK2} and RLC16^{MK2}	SIL versions: MPC4^{MK2} + IOC4^{MK2} SIL and RLC16^{MK2}SIL
Aluminium (silver) front panels	Aluminum (silver) front panels with yellow/orange “SIL Safety” labeling
One electronics processing module on MPC4^{MK2} for all functionality (measurements, management and interfacing)	Three electronics processing modules on MPC4^{MK2} SIL: • 2 × processing modules for measurements (with measurement redundancy with cross-checking) • 1 × processing module for management and interfacing
Separation (firmware only) of machinery protection system (MPS) and condition monitoring system (CMS) functionality/processing on the MPC4^{MK2} module	Complete separation (hardware and firmware) of machinery protection system (MPS) and condition monitoring system (CMS) functionality/processing on the MPC4^{MK2} SIL module
MPC4^{MK2} + IOC4^{MK2} module only runs diagnostics	MPC4^{MK2} SIL + IOC4^{MK2} SIL module and RLC16^{MK2} SIL module both run diagnostics
Up to 2 × tachometer (speed) signals/channels per module	1 × tachometer (speed) signal per module (need to be connected to both tacho inputs)
Tachometer (speed) channel signals can be freely shared via the VM600Mk2/ VM600 rack’s Tacho bus. MPC4^{MK2} SIL + IOC4^{MK2} SIL modules can not use signals on the Tacho bus for protection (SIL), only for condition monitoring.	
Digital high-pass filter (HPF) cutoff frequency up to 15 kHz	Digital high-pass filter (HPF) cutoff frequency up to 400 Hz
Up to 4 × user-configurable relays (RL1 to RL4) and 1 × common circuit-fault relay (FAULT). Note: In standard applications, use of the FAULT relay is optional / In safety-related applications, use of the FAULT relay is mandatory.	
Up to 16 × user-configurable relays (RL1 to RL16) per additional RLC16^{MK2} / RLC16^{MK2} SIL module	
User-configurable relays can be configured as normally energized (NE) or normally de-energized (NDE)	User-configurable relays must be configured as normally energized (NE)
Alarms and relays can be configured as latched or not latched	

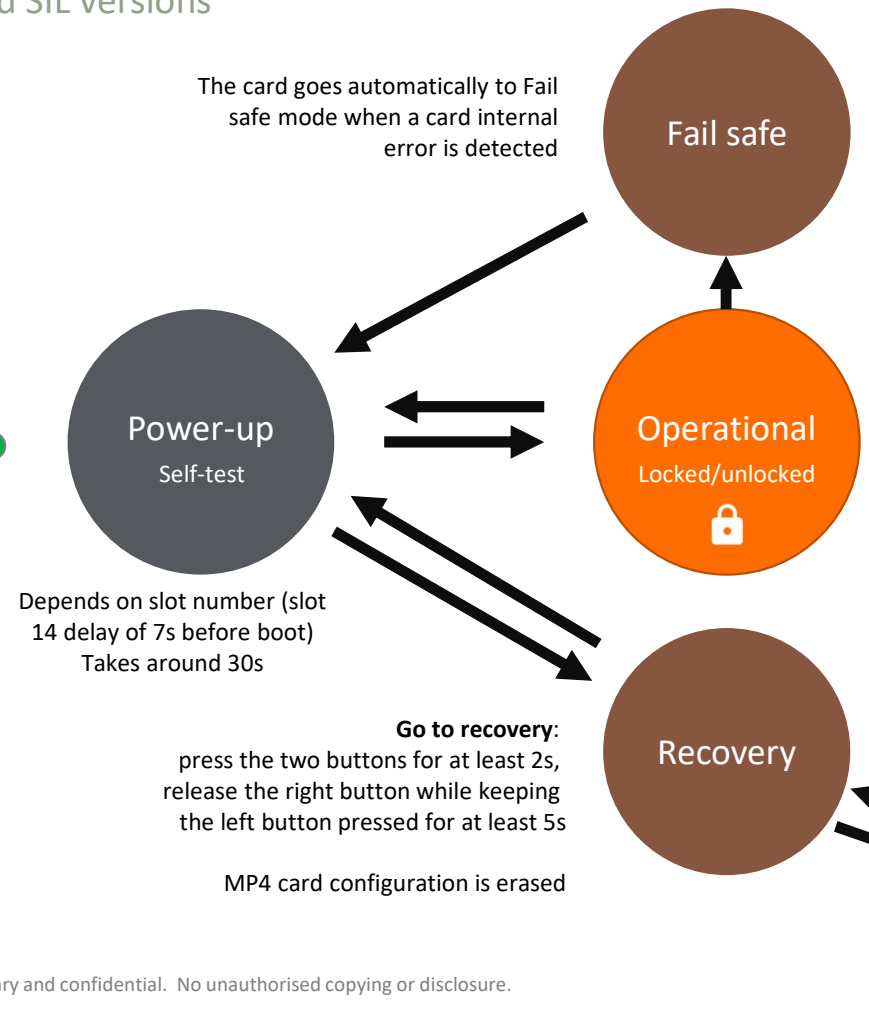
Differences between Standard and SIL modules

Summary table (2)

Standard versions: MPC4^{MK2} + IOC4^{MK2} and RLC16^{MK2}	SIL versions: MPC4^{MK2} + IOC4^{MK2} SIL and RLC16^{MK2}SIL
Machinery is protected when the MPC4^{MK2}module's main operating mode is Locked or Unlocked.	Machinery is protected only when the MPC4^{MK2} SIL module's main operating mode is Locked. Note: In safety-related applications, a MPC4^{MK2} SIL module can only run in the Locked state.
VM600^{MK2} system (MPC4^{MK2} + IOC4^{MK2}2 module and any RLC16^{MK2} modules) does not enter the safe state (fail-safe mode) if an input channel saturates	VM600^{MK2} system (MPC4^{MK2} SIL + IOC4^{MK2} SIL module and an RLC16^{MK2} SIL module) enters the safe state (fail-safe mode) if an input channel saturates for more than 1 hour
Live insertion and removal of modules (hot-swapping) is permitted with automatic reconfiguration of modules. That is, a replaced MPC4^{MK2} module will be auto-configured by its associated IOC4^{MK2} module.	Live insertion and removal of modules (hot-swapping) is permitted but automatic reconfiguration of modules is not supported. That is, a replaced MPC4^{MK2} SIL module will not be auto-configured by its associated IOC4^{MK2} SIL module.(It can only be configured manually using the VibroSight ® software.)
Verification of MPC4^{MK2} serial number by the VibroSight ® software	Verification of MPC4^{MK2} SIL and IOC4^{MK2} SIL serial numbers by the VibroSight ® software. MPC4^{MK2} SIL card will check serial number of the IOC4^{MK2} and it shall match.
Protection configuration signature not required	Protection configuration signature(SIL system signature) required. Note: Enforced by the VibroSight ® software.
Maximum altitude of 2 000 m (6 560 ft)for VM600Mk2 systems	Maximum altitude of 1600 m (5 250 ft)for VM600Mk2 SIL systems
CPUM^{MK2} module can be used for communication with both standard and SIL versions. The MPC4^{MK2} SIL module cannot accept the command AB (Alarm Bypass) from the DSI or CPUM^{MK2} command. In addition, SIL version when in fail safe can be acknowledged by the AR (Alarm Reset) command from SW or CPUM^{MK2} command (button or Modbus), however not possible from the AR DSI on the IOC4^{MK2} SIL	

MPC4 operating modes and associated status LED summary

Standard and SIL versions



The card goes automatically to Fail safe mode when a card internal error is detected

Go to operational:
- Class 1 Fatal-level: press the two buttons for at least 2s then go to Class 2 error-level
- Class 2 Error-level: press the right button for at least 1s

Status LED:
-Card fault:
--Class 1: red steady
--Class 2: blinking slowly

Unlock: press the right button 5 times within 5s

Lock: press the right button for at least 1s

Note that the card will not lock when:
- channel bypass is activated
- an internal error is detected

Status LED:
-Not configured: fast green blinking
-Configured:
--Everything OK: steady green
--Sensor NOK: steady orange
--Trip multiply: slow orange blinking

Lock LED:
-Unlocked: off / steady red (SI)
-Locked: blinking slowly green

Status LED:
Blinking slowly green

Depends on slot number (slot 14 delay of 7s before boot)
Takes around 30s

Go to recovery:
press the two buttons for at least 2s, release the right button while keeping the left button pressed for at least 5s

MP4 card configuration is erased

Go to operational:
press the two buttons for at least 2s

Status LED:
slow blinking green and red

Run the production test:
press the left button for at least 1s
The configuration backup on IOC4 card is erased

Fail-safe mode

Internal diagnostics

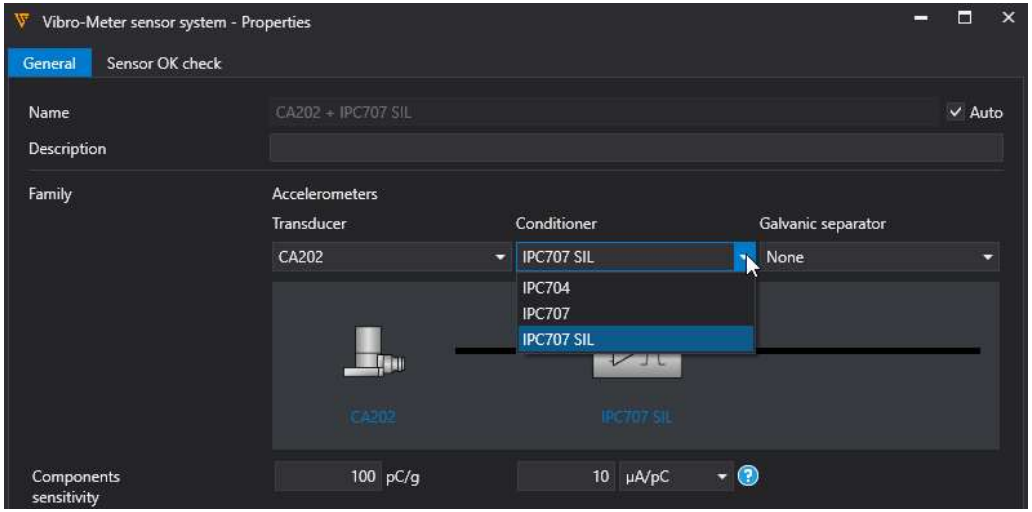
- MPC4 modules will go to fail-safe mode in case of problem detected by internal diagnostics
  - Mechanism to acknowledge the diagnostic detected problem using the buttons 1 or via the AR (Alarm Reset) command. Module will reboot to get out of the fail-safe mode
  - All relays are forced to safe state, ie. not energized state
- Diagnostics are generating fault errors classified in 3 classes :
  - Class 1 for fatal-level problems, usually hardware fault requiring to replace the module or due to incompatibility between hardware and firmware or MPC4 ad IOC4 modules. Problem must be resolved before the module can leave the fail-safe mode.
  - Class 2 for error-level problems, usually problems that will impact the normal operation of the system and need immediate attention. After fixing the problem, the error will disappear and after a reboot of the system and all self-tests are it will run back as normal.
  - Class 3 for warning-level problems, in this case the module will not go to fail safe mode and will continue to operate within the constraints of the problem detected with no immediate action required. A warning is logged and can be retrieved from VibroSight software. Usually it is configuration or input related problems that may have an impact on the operation.
  - Any problem with the sensor measurement OK chains are not considered as part of the diagnostics fault codes.
- Consult the manual for the list of diagnostics fault codes (Appendix A)

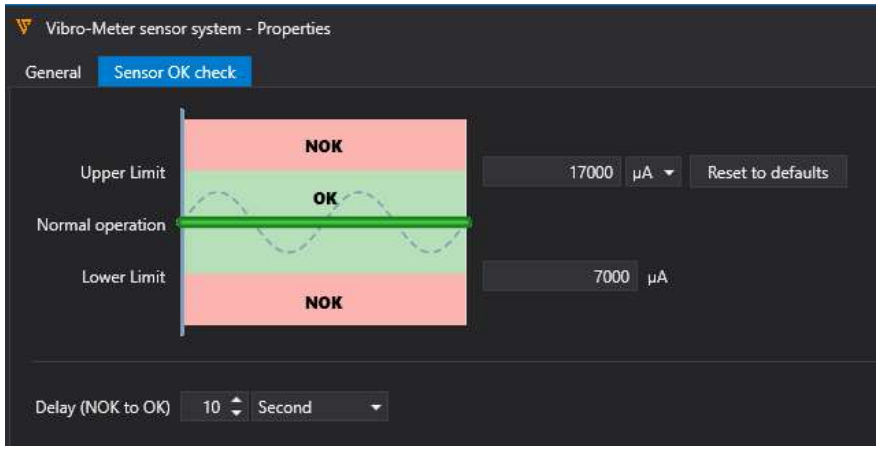
Integration with SIL2 measurement chains

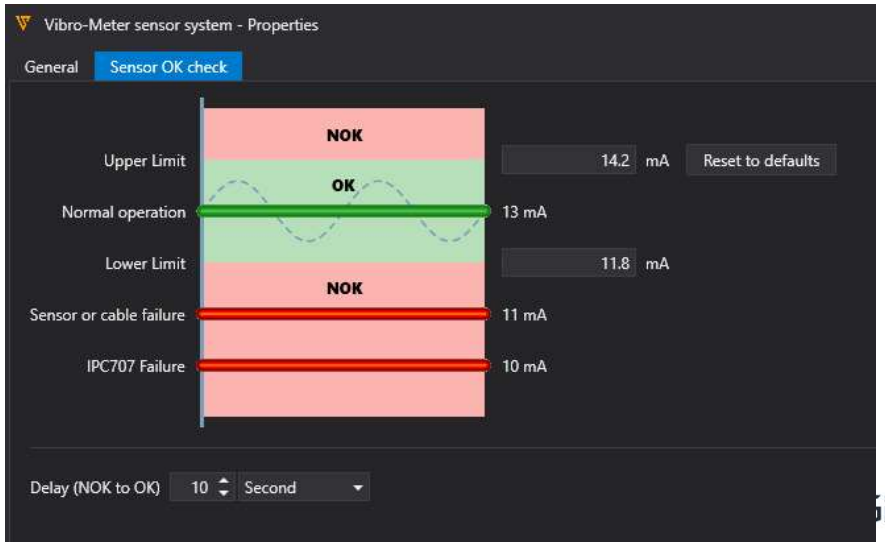
Piezoelectric accelerometer chains with IPC707

SIL2 rated chains

- Specific levels for DC bias voltage or current to indicate failure type.
- No automated interpretation of diagnostic but can be read from VibroSight Protect Dashboard to assess the failure mode.



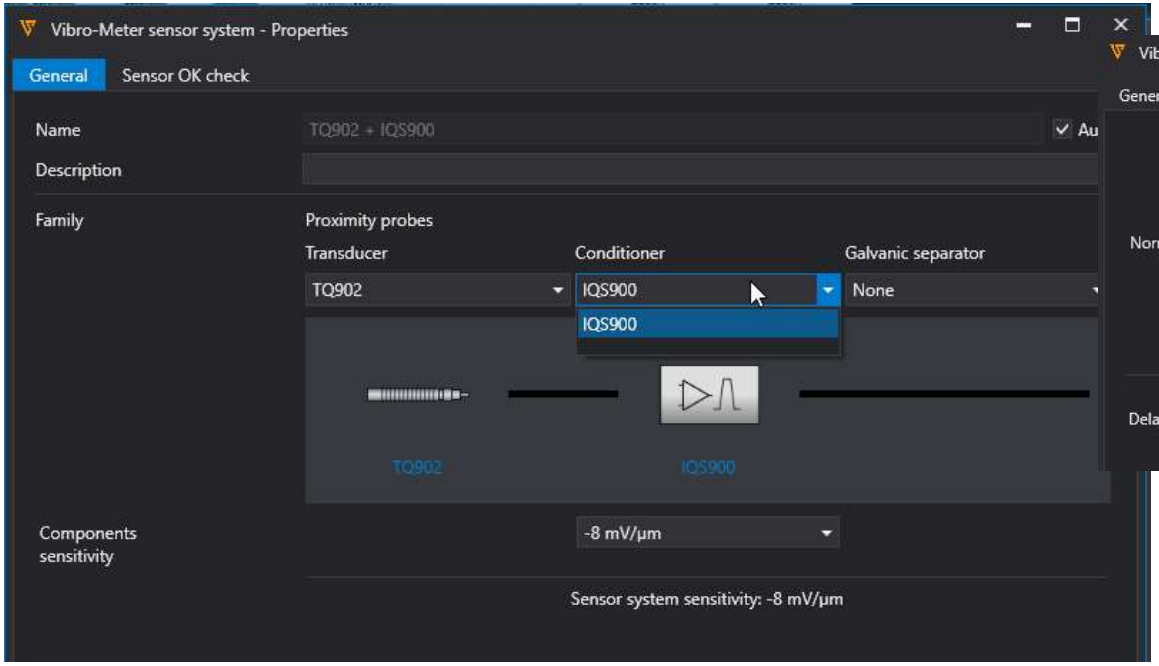


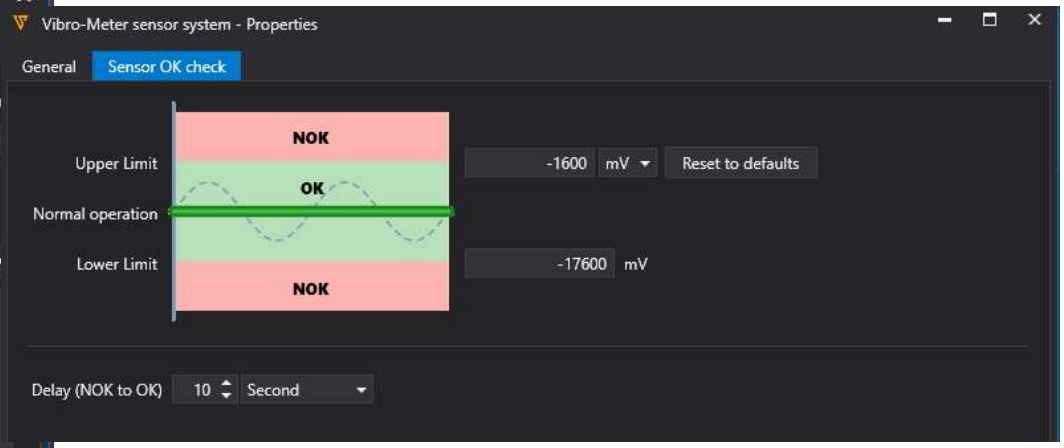


Proximity measurement chains

SIL2 rated chains

- IQS900 SIL will be added in the next release
- Outside of -1.6V to -17.6V or 15.5 to 20.5 mA indicate a problem with the measurement chain (sensor, cabling or signal conditioner)





SIL2 certificate

Certificate / Certificat
Zertifikat / 合格証

MEG 2112066 C001

exida hereby confirms that the:

VM600^{Mk2} Machine Monitoring System (MPSG2)

Meggitt SA
Fribourg, Switzerland

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-3

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type A Element

SIL 2 @ HFT=0; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
Detect limit violations by comparing measured process values with thresholds and drive relays per a user-defined configuration.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

The manufacturer may use the mark:

Revision 1.0 March 1, 2024
Surveillance Audit Due
March 1, 2027

Evaluating Assessor

Certifying Assessor

VM600^{Mk2} Machine Monitoring System

Certificate / Certificat / Zertifikat / 合格証

MEG 2112066 C001

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability:
The Product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:
The SIL limit imposed by the Architectural Constraints must be met for each element. This element meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT*

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
VM600^{Mk2} (200m**)	995	1067	13359	1971
VM600^{Mk2} (1600m**)	1081	924	40360	2315

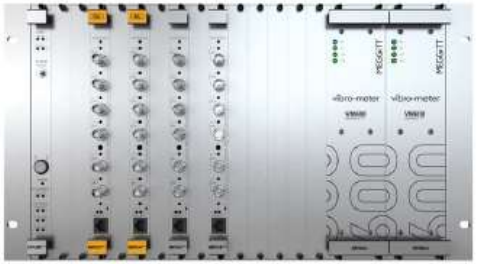
Safety property	Description / value
SIL level (IEC 61508)	SIL 2
Systematic capability (IEC 61508)	SC 2 (SIL 2 capable)
Mode of operation	Low-demand mode or high-demand mode
Type of subsystem	Type B element (random capability)
Hardware fault tolerance (HFT) See note 1	HFT=0 or HFT=1
Safe-detected failures (λ_{SD})	1081 failure rate (FIT)
Safe-undetected failures (λ_{SU}) See note 2	924 failure rate (FIT)
Dangerous-detected failures (λ_{DD})	40360 failure rate (FIT)
Dangerous-undetected failures (λ_{DU})	2315 failure rate (FIT)
No effect failures (#) See note 2	21072 failure rate (FIT)
Diagnostic coverage (DC) See note 3	95%
Proof test coverage (PTC)	74%
Process safety time (PST)	< 200 ms
Mean time to repair (MTTR)	48 hours

Safety manual

SAFETY MANUAL

vibro-meter®

VM600^{Mk2}
machinery monitoring system – IEC 61508 SIL 2



SIL Safety

This document contains important information about products that are intended for use in safety-related applications.

Document reference MAVM600MK2-FS1/E
Edition 1 – March 2024

Structure of the manual

This section gives an overview of the structure of the manual and the information contained within it. Some information has been deliberately repeated in different sections of the document to minimize cross-referencing and to facilitate understanding through reiteration.

The chapters are presented in a logical order. You should read those that are most relevant to your safety-related applications and then keep the document at hand for future reference.

The structure of the document is as follows:

Chapter 1	Introduction Explains the purpose and scope of this safety manual. Introduces the VM600^{Mk2} machinery monitoring system and system components for machinery protection system (MPS) applications.
Chapter 2	Communications Explains how to communicate with a VM600^{Mk2} machinery monitoring system, describes the VM600^{Mk2}/VM600 rack backplane and provides an overview of the VM600^{Mk2} MPC4^{Mk2} + IOC4^{Mk2} SIL module and RLC16^{Mk2} SIL module.
Chapter 3	How to use the system for safety Explains how a VM600^{Mk2} machinery monitoring system is used in safety-related applications in terms of the various safety properties. And provides safety parameters and highlights safety considerations relevant to the design, installation, configuration, use and maintenance of these systems.
Chapter 4	Configuration Provides configuration information for VM600^{Mk2} machinery monitoring systems.
Chapter 5	Installation and commissioning Provides installation and commissioning information for VM600^{Mk2} machinery monitoring systems.
Chapter 6	Operation and maintenance Provides proof test and other operation and maintenance information for VM600^{Mk2} machinery monitoring systems.
Chapter 7	Service and support Provides contact information for technical support. Includes information regarding important SIL safety product information and the procedure to follow in order to opt in and receive such SIL product communications. Includes information regarding product returns and the procedure to follow in order to report problems and return Parker Meggitt (Meggitt SA) energy products for repair.

Safety manual

Configuration / installation requirements

3.7 Hardware requirements

A VM600^{Mk2} machinery monitoring system used as a machinery protection system (MPS) in a safety-related application must meet the following hardware requirements:

- The VM600^{Mk2} ABE04x system rack shall always be installed with redundant RPS6U rack power supplies.
- When the VM600^{Mk2} system (ABE04x rack) is turned on (powered), module's can only be inserted one at a time (that is, no more than one board can be plugged in at the same time).
- The VM600^{Mk2} system (ABE04x rack) must contain at least one MPC4^{Mk2} + IOC4^{Mk2} SIL machinery protection and condition monitoring module.
- At least one relay on each MPC4^{Mk2} + IOC4^{Mk2} SIL module shall be configured for system diagnostics which shall include (but not be limited to) sensor / measurement chain input status, module status or safety level thresholds (configured alarm limits) violation.
  This relay shall be connected to an emergency shutdown system (ESD) or logic solver in order to provide a safe state when a failure is diagnosed or an alarm alert/danger is detected by the module.
- The maximum current rating used by relays (safety outputs) must be two-thirds (⅔) of the maximum operational rating.
- Relay outputs (safety outputs) must be protected by external fuses, in order to avoid welding due to transient over-currents.
- Safety loops and non-safety loops (inputs and outputs) shall not be connected in the same module, that is, they shall be provided in separate modules.
- A proof test shall be performed by trained and authorised personnel periodically in accordance with this safety manual (*VM600^{Mk2} machinery monitoring system – SIL 2 MPS safety manual*). See 6.1 Proof test.
- A complete proof test of the VM600^{Mk2} system shall be performed after removing or replacing any modules or subcomponents that are part of the critical safety path. See 6.1 Proof test.
- If VM600^{Mk2}/VM600 XMx16 + XIO16T extended condition monitoring modules are also part of the VM600^{Mk2} MPS (rack), use of the Raw bus for sharing analog signals with these modules is not allowed for safety-relevant signals. Instead, such input signals should be shared via the XIO16T module's connector (rear of rack), that is, using external cabling.

NOTE: The Raw bus must not be used to share safety-relevant signals between modules/cards.

- Use of the Alarm bypass (AB) function is not allowed.
- Use of the sensor/channel bypass (inhibit) function is not allowed.
- Upon detection of a failure by system diagnostics (that is, built-in self-test (BIST) running on MPC4^{Mk2} + IOC4^{Mk2} SIL and RLC16^{Mk2} SIL modules), the output relays or a separate alarm relay must de-energize to signal the failure.

3.8 Software requirements

A VM600^{Mk2} machinery monitoring system used as a machinery protection system (MPS) in a safety-related application must meet the following software requirements:

- The VibroSight® software shall not be permanently connected to the VM600^{Mk2} system (ABE04x rack) for either standalone or networked systems/solutions.

NOTE: Once configured, a VM600^{Mk2} machinery monitoring system used as a machinery protection system (MPS) can operate standalone, that is, without a computer permanently connected.

A "functional safety program" shall restrict overall access to the VM600^{Mk2} MPS during normal operation.

- The alarms and relays must be configured depending on the role of the VM600^{Mk2} MPS in the safety loop. See 3.1 VM600^{Mk2} in a safety-related system.
- If a safety function is performed by the VM600^{Mk2} MPS only, any safety relay corresponding to an alarm must be configured as latched and normally energized (de-energized to trip).
- If a safety function is performed by an external system using an alarm detected by a VM600 system as an input, the relay corresponding to this alarm may be configured as not latched.
  However, an analysis must be carried out at the safety-related system level to ensure that no alarm can be missed or to identify all possible impacts and acceptability of residual risks in case of a missed alarm.
- The configuration of MPC4^{Mk2} + IOC4^{Mk2} SIL modules must detect faults in the module's sensor power supply outputs.
- The system configuration must be error free and signed for (authorized by a SIL system signature) using the VibroSight Protect configuration software. See 3.9 Configuration requirements.
- The VM600^{Mk2} MPS's process manual (*VM600^{Mk2} machinery*
- Any configuration changes to safety manual (*VM600^{Mk2} mac*
- Software access to and comm with the security and cyt (see 3.14 Environmental and a

3.9 Configuration requirements

A VM600^{Mk2} machinery monitoring system used as a machinery protection system (MPS) in a safety-related application must meet the following configuration requirements:

- It is the end-user's responsibility to validate that the activated configuration performs as required within their overall safety-related system (SRS) via commissioning tests.
- By reading and interpreting the configuration (human-readable format (text-based XML)) displayed by the VibroSight Protect software when authorizing with a SIL system signature, the operator must check that the parameters are the correct ones for their specific use case (machine, speed, load, etc.) and execute a manual test.
- The end-user must approve the configuration by signing for it in the VibroSight Protect software (SIL system signature).
  This configuration verification and validation shall be formally recorded by the end-user (verification evidence).
- Live insertion and removal of modules (hot-swapping) with automatic reconfiguration is not permitted for the VM600^{Mk2} MPC4^{Mk2} + IOC4^{Mk2} SIL (see Table 1-1).

See also 4 Configuration and 4.2 Using VibroSight Protect

Next product evolution (road map)

Upcoming updated SIL2 certification

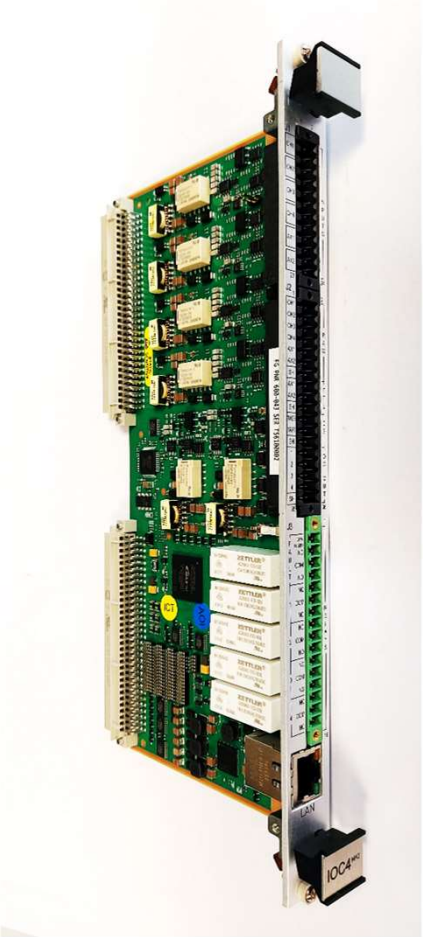
Change to come with updated SIL2 certificate expected end of 2024

- Improvement with speed processing
  - At very low speed, keep quality bit and adaptive monitoring
  - Improve low speed reliability measurement (debounce filter)
  - Speed channel saturation diagnostics to be relaxed and not lead to fail-safe mode
- Narrow band processing (order tracking) for aeroderivative market: allow lower FFT resolution to have faster reactivity of the measurement, option to configure 100, 200, 400 or 800 lines. Default as currently with 800 lines
- Lower delay option for filters with broadband especially with low high pass cut-off frequency and indication in VibroSight Protect of the filter delay
- Adaptive monitoring with 2 parameters
- Better feedback when alarm bypass or trip multiply are activated in Protect Dashboard
- Support RLC16 card without diagnostics via raw bus (configuration of redundant outputs)
- Certification – remove restriction on max altitude 1600m to align with 2000m of standard modules

Standard VM600 Mk2

Product evolution

- New version of MPC4 and IOC4 Mk2 standard card will be introduced in July 2024
  - Ethernet port on the IOC4 Mk2 Standard as it is with the SIL version
  - Need to match both version of cards
    - MPC4 MK2 standard, PNR 600-041-001-003
    - IOC4 MK2 standard, PNR 600-043-000-003
- New firmware
  - Alignment of processing, bug fix with the SIL version



THANK YOU