



Brüel & Kjær Vibro

A member of the NSK Group

BK vibro

SIL Safety Manual

Setpoint Machinery Protection System

Safety Manual – Temperature Monitoring Module (TMM)



Keep accessible for future reference

Trademarks and Copyrights

All trademarks, service marks, and/or registered trademarks used in this document belong to BK Vibro America Inc., except as noted below:

Bently Nevada, Velomitor, REBAM, and Keyphasor are marks of the General Electric Company in the United States and other countries.

Microsoft, Excel, Windows, and Outlook and their respective designs are marks of Microsoft Corporation in the United States and other countries.

Modbus® is a mark of Schneider Automation in the United States and other countries.

OSIsoft, the OSIsoft logo and logotype, Managed PI, OSIsoft Advanced Services, OSIsoft Cloud Services, OSIsoft Connected Services, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Vision, PI Data Archive, PI DataLink, PI DataLink Server, PI Developer's Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC driver, PI Manual Logger, PI Notifications, PI ODBC, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, RLINK and RtReports are all trademarks of OSIsoft, LLC.

Trademarks used herein are the property of their respective owners.

Copyright © 2022 Brüel & Kjær Vibro GmbH

All rights to this technical documentation remain reserved.

Any corporeal or incorporeal reproduction or dissemination of this technical documentation or making this document available to the public without prior written approval from Brüel & Kjær Vibro GmbH shall be prohibited. This also applies to parts of this technical documentation.

Safety Manual **VC-8000 Temperature Monitoring Module (TMM)**, C107576.002 / V02, en, date of issue: 25.02.2022

Table of Contents

1	About this Safety Manual	5
2	Related additional information	6
3	Acronyms	7
4	Terms and definitions	8
5	Applicable standards	14
6	Temperature Monitoring Module (TMM) description and safety-relevant functionality	15
6.1	SIL compliant TMM identification	18
6.2	TMM Spare Parts	20
7	SIL requirements and constraints	21
7.1	TMM Hardware SIL requirements	21
7.1.1	TMM safety-relevant inputs requirements	21
7.1.2	TMM inputs processing	24
7.1.3	TMM discrete inputs (INH, TMI, SAI, RST)	25
7.1.4	TMM Power Supply	25
7.1.5	TMM outputs requirements	25
7.1.6	TMM Fault	27
7.1.7	TMM Hardware Diagnostics	29
7.2	TMM Firmware and Configuration Software SIL requirements	29
7.3	TMM Firmware SIL compliant release identification	30
7.4	Configuration Software SIL requirements	31
7.5	Firmware SIL requirements	32
7.6	Environmental and operating conditions	33



8	VC-8000 TMM functional specifications	35
8.1	TMM random hardware failures	37
8.2	Failure modes	38
8.2.1	Failure modes detection by internal diagnostics	38
8.2.2	Failure modes of the internal diagnostics	39
8.2.3	Diagnostic test interval	39
8.2.4	System output	39
8.2.5	Failure rates and FMEDA Results	40
8.3	Systematic Capability	43
8.4	Architectural and random constraints	44
8.5	Common Cause Failures	45
9	Installation and commissioning	47
10	Proof testing	49
10.1	Connections and terminal boards inspection	49
10.2	TMM board and populated PCB inspection	50
10.3	Relay driving by input sensor disconnection	50
10.4	Fault relay activation testing	51
10.5	Safety function test	52
10.6	Power supply removal test on TMM output relay	53
10.7	TMM module disconnection from the rack test	54
10.8	Node voltage sense diagnostics test	55
10.9	Inhibit, Trip Multiply, Special Alarm Inhibit deactivation test	56
11	Maintenance, repair, de-commissioning and disposal	57
11.1	Item Modification and Retrofit Management	57
11.2	De-commissioning or disposal of the item	57

1 About this Safety Manual

This Safety Manual documents all the information and requirements relating to VC-8000 Machinery Protection System Temperature Monitoring Module (TMM), required to enable the integration into a safety-related system that performs the allocated Safety Instrumented Function (SIF). This document provides all information and constraints relevant for functional safety for the use of TMM to allow the proper operation and integration in VC-8000 Machinery Protection System for safety applications. This Safety Manual is an addendum to the SETPOINT MPS manual and shall be used in conjunction with it and provides all the functional safety-relevant information necessary for the end-user to install, verify, maintain and periodically test ensuring the respect of product safety requirements (item function, input and output interfaces etc). TMM (configured and integrated as described throughout this Safety Manual) is proven suitable for functional safety applications, as a result of a Third-Party Functional Safety Assessment (FSA) against IEC 61508 Standards requirements. The suitability of TMM for safety-related applications is declared only for the configurations, operating conditions and constraints reported in this Safety Manual. The implementation of this device in configurations or conditions other than those prescribed in the Safety Manual could impair the safety function performance under end-user responsibility. BK Vibro America Inc. has no responsibility towards changes to any of the admissible configurations and constraints declared in the Safety Manual.



2 Related additional information

Document Number	Title
S1079330	Setpoint™ Machinery Protection System Operation Manual
S1176125	Setpoint™ Condition Monitoring System Operation Manual
S1160865	Setpoint™ Hazardous Installation Manual
S1472326	Setpoint™ Calibration Interval White Paper
18-01172-002_FSA Backplane	Functional Safety Assessment
1077785	VC-8000 Machinery Protection System Datasheet
1077788	Temperature Monitoring Module (TMM) Datasheet

3 Acronyms

The followings are the acronyms used throughout this Safety Manual:

ACRONYM	DEFINITION
SIS	Safety Instrumented System
SIF	Safety Instrumented Function
λ	Failure rate (per hour) of an equipment or a sub-system
λ_D	Dangerous failure rate (per hour) of an equipment or a sub-system
λ_{DD}	Dangerous detected failure rate (per hour) of an equipment or a sub-system
λ_{DU}	Dangerous undetected failure rate (per hour) of an equipment or a sub-system
λ_S	Safety failure rate (per hour) of an equipment or a sub-system
$\lambda_N (P+F)$	Failure rate obtained through the sum of NO PART and NO EFFECT
λ_{OT}	Other failure rate
TYPE A (as Architectural Type)	Type A equipment or (sub)system: "Non –complex" (sub)system or equipment according 7.4.3.1.2 of IEC 61508-2.
TYPE B (as Architectural Type)	Type B equipment or (sub)system: "Complex" (sub)system or equipment according 7.4.3.1.3 of IEC 61508-2.
EUC	Equipment under control
DC	Diagnostic Coverage
SW	Software
HW	Hardware
FS	Functional Safety
PVST	Partial Valve Stroke Test
RRF	Risk Reduction Factor
SFF	Safety Failure Fraction
HFT	Hardware Fault Tolerance
MRT	Mean Repair Time (h)
MTTR	Mean Time To Restoration (h)
PFD_{AVG}	Average probability of dangerous failure on demand
PTI	Proof Test Interval
PTC	Proof Test Coverage



4 Terms and definitions

The followings are the terms and definitions used throughout this Safety Manual:

Architecture

Arrangement of hardware and/or software elements in a system, for example,

- (1) arrangement of safety instrumented system (SIS) subsystems;
- (2) internal structure of an SIS subsystem;
- (3) arrangement of software programs.

Architectural constraint

This reports the maximum SIL achievable based on the SIF's subsystems architecture alone. This is calculated solely on the basis of Type A or Type B device selection, redundancy (hardware fault tolerance), and the safe failure fraction (calculated or conservatively assumed if no data is provided). It does not pertain to Systematic Capability or certification. This is calculated as indicated, using respective IEC 61508 or IEC 61511 tables.

Architectural Type

Type A equipment or (sub)system: "Non –complex" (sub)system or equipment according 7.4.3.1.2 of IEC 61508-2;

Type B equipment or (sub)system: "Complex" (sub)system or equipment according 7.4.3.1.3 of IEC 61508-2.

Common Cause Failure CCF

Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel (redundant architecture) subsystem, leading to failure of a SIF.

MooN

Safety instrumented system, or part thereof, made up of "N" independent channels, which are so connected, that "M" channels are sufficient to perform the safety instrumented function.

Hardware Fault Tolerance

A hardware Fault Tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function. In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics.

Safety instrumented function (SIF)

Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

Safety instrumented system (SIS)

Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s).

Safety integrity

Probability of a SIS or its subsystem satisfactorily performing the required safety-related control functions under all stated conditions.

Safety Integrity Level (SIL)

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SIF, where safety integrity level four has the highest level of safety integrity and safety integrity level one has the lowest.

Failure

Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

Random Hardware Failure

Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.

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.



Failure Rate

Reliability parameter ($\lambda(t)$) of an entity (single components or systems) such that $\lambda(t) \cdot dt$ is the probability of failure of this entity within $[t, t+dt]$ provided that it has not failed during $[0, t]$

Safe Failure

Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

Dangerous Failure

Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or decreases the probability that the safety function operates correctly when required.

Common cause failure

Failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.

Detected, Revealed or Overt

In relation to hardware, detected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation.

EXAMPLE These adjectives are used in detected fault and detected failure.

NOTE A dangerous failure detected by diagnostic test is a revealed failure and can be considered a safe failure only if effective measures, automatic or manual, are taken.

Undetected, unrevealed or Covert

In relation to hardware, undetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation.

EXAMPLE These adjectives are used in undetected fault and undetected failure.

No Part Failure

Failure of a component that plays no part in implementing the safety function.

NOTE The no part failure is not used for SFF calculations.

No Effect Failure

Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function.

NOTE 1 The no effect failure has by definition no effect on the safety function, so it cannot contribute to the failure rate of the safety function.

NOTE 2 The no effect failure is not used for SFF calculations.

Safe Failure Fraction

Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

Diagnostic Coverage

Fraction of dangerous failures detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by total rate of dangerous failures.

Diagnostic Test Interval

Interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage.

Soft-error

Erroneous changes to data content but no changes to the physical circuit itself.

NOTE 1 When a soft error has occurred, and the data is rewritten, the circuit will be restored to its original state.

NOTE 2 Soft errors can occur in memory, digital logic, analogue circuits, and on transmission lines, etc and are dominant in semiconductor memory, including registers and latches. Data may be obtained, for example, from manufactures.

NOTE 3 Soft errors are transient and should not be confused with software programming errors.

Safe state

State of the EUC when safety is achieved.



Equipment under control (EUC)

Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

Redundancy

The existence of more than one means for performing a required function or for representing information.

Safety function

Function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.

Systematic Capability

Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

Mode of operation

Way in which a safety function operates, which may be either:

- **low demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

NOTE The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2).

- **high demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- **continuous mode:** where the safety function retains the EUC in a safe state as part of normal operation,

Fault

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

Fault tolerance

Ability of a functional unit to continue to perform a required function in the presence of faults or errors.

Probability of dangerous failure on demand (PFD)

Safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.

Average Probability of dangerous failure on demand (PFDavg)

Mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.

Functional safety assessment

Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures.

Proof test

Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition.

Safety manual for compliant items

Document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508 series.



5 Applicable standards

The following are the applicable standards to VC-8000 Machinery Protection System.

STD ID.	STANDARD CODE	STANDARD TITLE
S1	IEC 61508-1:2010-04	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
S2	IEC 61508-2:2010-04	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
S3	IEC 61508-3:2010-04	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
S4	IEC 61508-4:2010-04	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations
S7	IEC 61508-7:2010-04	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures
S8	ISO 13849-2:2012	Safety of machinery - Safety-related parts of control systems -- Part 2: Validation
S9	IEC 61164:2004	Reliability growth – Statistical test and estimation methods
S10	IEC 62308:2006	Equipment reliability – Reliability assessment methods
S11	IEC 60812:2006	Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
S12	IEC 61709:2017	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion

6 Temperature Monitoring Module (TMM) description and safety-relevant functionality

The Temperature Monitoring Module (TMM) accepts from one to six 2-, 3-, and 4-wire RTDs and/or thermocouples (both grounded and ungrounded tip) in any combination and provides six channels dedicated to temperature monitoring. It also accepts 4-20mA process variable signals. Multiple temperature channels can be grouped for differential and/or average measurements and alarming. The allowable safety-related functions implementable by TMM are only related to the temperature measurements, the 4-20mA process variable signals cannot be used for safety-related applications and are so excluded from the safety relevant inputs. The comprehensive list of input channel types and measurements suitable for safety applications is reported in the “TMM safety relevant input requirements” section 7.1.1. TMM monitor NO (Normally Open) contact of the onboard output relay(s) de-energizes the load when at least one of the input sensors reaches the configured threshold set. The output relays shall be in Normally energized (De-energize to trip) configuration, in order to guarantee the reaching of the safe state in case of either loss of power supply or in case of wiring failures, increasing the overall system reliability.





The TMM occupies a single slot in a SETPOINT® monitoring system rack and uses 24 Vdc instrument power as supplied by the SETPOINT® Rack Connection Module (RCM). TMM is not equipped with sensor power supplies. Each TMM provides all necessary power, signal conditioning, alarm comparison, and relay logic functions needed to provide six channels of continuous machinery monitoring and protection. It complies with the requirements of American Petroleum Institute Standard 670 for monitoring systems and is completely configurable using SETPOINT® configuration software. Up to 15 TMM cards can reside in a single 19" SETPOINT® rack, providing up to 90 channels of continuous machinery protection. Each module provides basic status indication for its channels as required by API 670. When used with the optional rack touchscreen, real time display of variable levels, alarm statuses, and other information is available for all channels concurrently on a single screen for "at a glance" convenience.

The considerations reported in this Safety Manual are valid for both TMM and TMMCM versions (the latter are equipped with CMS Condition Monitoring Software) and through the SAM have an additional configuration flag that allows the representation, plotting and fitting of variables and parameters.

When ordered with optional condition monitoring capabilities, the module streams high-speed (500 ms update rate) data to the rack's System Access Module (SAM) where it is available to software such as SETPOINT® CMS and/or the rack's embedded high-speed "flight recorder" on SD Card or Solid State Drive.

TMM board has the potential to acquire different inputs through configurable input channels and has onboard a dedicated acquisition and conditioning circuit to process the signals acquired. TMM is furthermore equipped with individual and fully independent SPDT electro-mechanical relays fully configurable that can be voted with other relay channels on the same boards or on other modules in the rack.

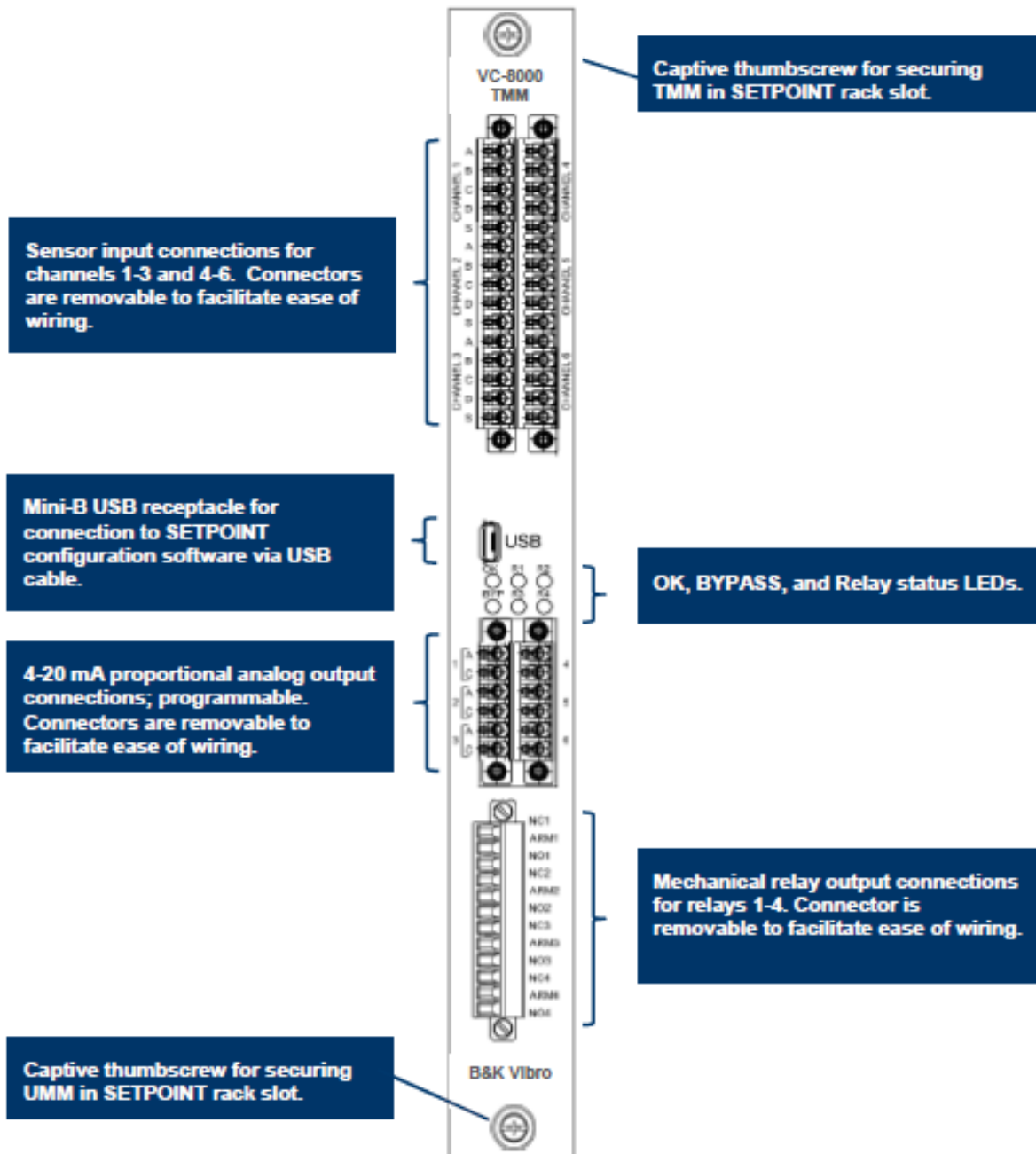
TMM is powered by RCM through backplane and is equipped with distributed power regulation functionality that improves reliability. It manages the power supply received, converts its 24Vdc power supply input to all regulated voltages needed by all devices, on-board processors and transducers, SDRAM, CPU etc. reducing the potential for rack single-point failures compared to systems that generate regulated voltages for the entire rack in a centralized power supply.

TMM firmware safety-relevant release, crucial to manage the safety-related functionality is stored in the flash memory. TMM board is configurable by the user depending on the specific application needs through Setpoint Configuration Software (e.g. channels enable, thresholds setting etc.). TMM board configuration uploading is password-protected to prevent any unintended configuration changes that could compromise the safety functionality. TMM board is configured via USB, upon completion of configuration uploading the board is rebooted. Online configuration changes, while the EUC is running are not allowed.

TMM fault conditions are managed through RCM fault relay activation via rack backplane: TMM board communicates its fault status to the rest of the rack via backplane and the RCM fault relay is subsequently triggered.

TMM board is equipped with hot swap controller functionality, that allows the replacement of the board without removing the applied voltage.

The following figure schematizes TMM layout and connections.





6.1 SIL compliant TMM identification

The VC-8000 safety relevant parts are uniquely identified and traced in respect to standard parts (for general, not-safety related items) through dedicated part numbering. In order to set up a system devoted for safety relevant applications, ONLY items having the SIL part number shall be selected.

TMM SIL cards are identified as follows:

VC-8000/TMM-AA-BB

AA=00/01/02

Selecting the TMM type as follows:

00=TMM;

01=TMM_{CM};

02= TMM_{CM} (firmware upgrade only).

BB=07

With BB (standing for Agency Approval and Certifications): 07 (SIL & Multi: ETLc, IEC, ATEX).

When ordering as part of a system, do not order TMM cards and other rack components individually. Instead order using part numbers VC-8000/RCK options AA through VV. Refer to the SETPOINT® system datasheet S1077785 to specify rack size, module types for each slot, faceplate, touchscreen, mounting style and other options.

The VC-8000 rack suitable for SIL applications shall be selected according to the following part number criteria:

VC-8000/RCK-AA-BB-CC-DD-EE-FF-GG-HH-JJ-KK-LL-MM-NN-PP-RR-SS-TT-UU-VV

Selecting at least the followings (the other fields are selected by the end-user)

DD= 06 (SIL option) or **07** (SIL & Multi: ETLc, IEC, ATEX);

EE: selected according to the configuration implemented on the combination of slot 1 (where RCM resides and slot 2)

The other fields shall be selected depending on the configuration to be implemented and on the slot where TMM is required to reside.

SIL compliant TMM are visibly identifiable by the end-user because they are yellow (instead of black like the standard boards) and are labelled as TMM FS (functional safety compliant), as shown in the figure below:

TMM board is furthermore characterized by the presence of a label with the identification number of the SIL compliant item (see the example reported in the figure below).





6.2 TMM Spare Parts

When ordering spare TMM cards not ordered as part of a VC-8000 system, the following part number shall be used.

TMM spare parts suitable for functional safety applications are identified as follows:

VC-8000/TMM-AA-BB

AA=00/01/02

Selecting the TMM type as follows:

00=TMM; **01**=TMM_{CM}; **02**= TMM_{CM} (firmware upgrade only).

BB=07

With **BB** (standing for Agency Approval and Certifications): **07** (SIL & Multi: ETLc, IEC, ATEX).

7 SIL requirements and constraints

This section treats the functional safety relevant requirements for TMM hardware, System installation, operation and use in safety-related applications.

7.1 TMM Hardware SIL requirements

7.1.1 TMM safety-relevant inputs requirements

TMM board is equipped with acquisition and conditioning circuits for different types of sensors/transducers, among all of them, only those detailed in the table below are suitable for safety-related applications.

The following tables contain all safety relevant measurements that can be managed by the TMM card and that can be used in safety-related applications. All other measurements that are not listed below are not suitable to realize a Safety Instrumented Function (SIF).

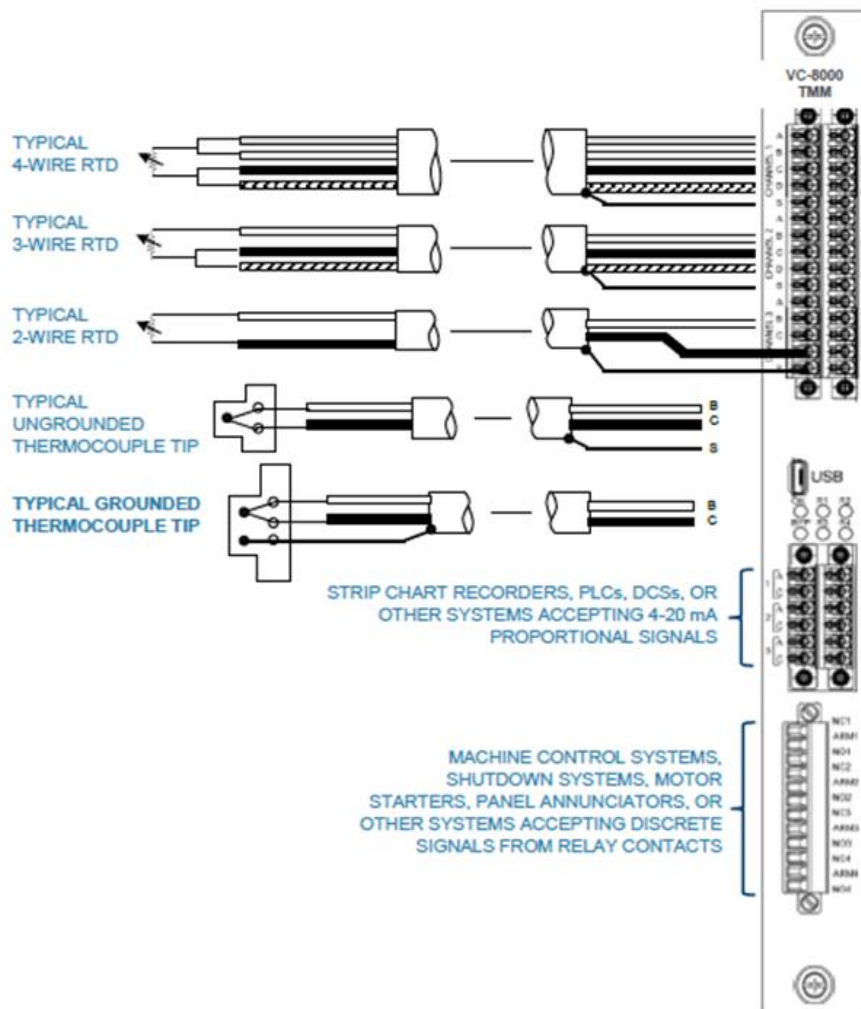
The highlighted measurements in the following table are applicable to Safety Instrumented Systems.

**IMPORTANT!**

This Safety Manual provides to the end user and SIS integrator **ONLY** the requirements for the selection of input sensors suitable for safety-related applications. The selection of the sensors together with of any barriers or input interfaces resides under the **SOLELY** responsibility of the SIS integrator. The use of input typologies that are not listed in the following table is forbidden for safety applications.

Channel Type	Typical Uses	Measurements	Measurement Description	Safety measurement	Type
Temperature	Thermocouple or RTD temperature measurements	Direct (primary)	Temperature	YES	X
		Difference	Difference between two temperature sensors or between a temperature sensor and an average.	NO	Add

The following figures show the input connections to the TMM board. Inputs shall be connected to the TMM board according to the instructions reported in the Datasheet and in VC-8000 Manual.



- Only single channel components have been included in safety-related applications (multi-channel such as differential measurements, are not safety-relevant);
- Slow measurements for low speed machines are not safety-relevant due to the long alarm response time;
- Grounded tip thermocouples **MUST NOT** be used in safety-related applications, **ONLY** ungrounded tip thermocouples are suitable as Safety Instrumented Function (SIF) input;

TMM has the potential to acquire different type of sensors based on the user configuration. After the configuration, the firmware will automatically set the proper signal conditioning, including for example the temperature compensation, specific for the sensor type to be connected. TMM is characterized by an acquisition and signal conditioning circuitry of the input signals. Input signals are filtered in order to remove the noise through EMI high frequency filters, that cut-off the signals having a frequency lower than a set value. TMM is characterized by the presence of a conditioning circuitry, that in case of thermocouples includes a cold joint compensation circuitry that avoids measurements alterations and errors and increases the confidence in measurements reliability.

Any interfaces on input channels, such as isolating and Zener barriers, out of BK Vibro America Inc. scope of supply, are not treated in this Safety Manual. Barriers selection, evaluation and integration in the overall system depending on the foreseen application, sensors acquired etc. is in customer scope and resides under SIS integrator responsibility. When an input interface, such as a barrier is installed on TMM input channel line, the SIS integrator and system end-user shall be aware that the diagnostics implemented on TMM inputs would not “read” the status of the sensor itself, but of the interposing isolator. TMM sensors and any barriers, interfaces and isolators part of the SIS having a specific allocated SIL target shall be selected by the SIS integrator to guarantee the achievement of the target Safety Integrity Level. Sensors and any barriers, interfaces etc. part of the safety loop shall be capable to reach a safety integrity level at least equal to the target. The overall SIL reached by the loop is in fact limited by the lowest SIL among all components involved in the loop. This selection resides under end user/system integrator responsibility.

TMM six input channels are identical in terms of hardware circuitry and independent three by three. The first and the second group, both formed of three channels are wired to two distinct analog-to-digital (ADC) converters. Full redundancy between input channels can be effectively implemented only between channels belonging to the first group (channel 1, channel 2 and channel 4) and channels belonging to the second group (channel 2, channel 5 and channel 6). Being the two groups acquired by different ADCs, this guarantee that the input paths are fully independent, and that full redundancy can be implemented. Redundancy between input channels is recommended for safety applications, as it increases the overall reliability.

TMM is characterized by default setpoint limits, within the limits of the sensors. Overvoltage and undervoltage conditions can be indicators of an incorrect setting of probe distance. Setpoint default limits are changeable by the user, under the solely end-user responsibility.

TMM board measurements are characterized by the following **OK/in specs ranges**:

Sensor	Minimum °C	Maximum °C
100Ω Pt RTD (0.385)	-200	1000
10Ω Copper RTD	-105	265
120Ω Nickel RTD	-85	265
100Ω Pt RTD (0.932)	-205	705
100Ω Copper RTD	-100	260
Type E TC	-105	1005
Type J TC	-5	765
Type T TC	-165	405
Type K TC	-5	1375

All measurements that exceed these limits, depending on the probe type selected, indicate an unintended operating condition or faulty status from TMM inputs side and therefore determines the depowering of the board output relay(s).



7.1.2 TMM inputs processing

TMM board is equipped with a processor counter, for the processing of the inputs acquired. The processor counter evaluates if the temperature signal measured is properly maintained in the subsequent time samples, in order to ensure that the reading acquired is correct and that is not affected by measurements errors. The processor counter is characterized by a certain time delay, that evaluates that the measurement is maintained and thus valid and realistic. This functionality avoids spurious trips that prevents the EUC from being tripped due to only one measurement acquired beyond dangerous threshold caused by measurements disturbances and errors. This functionality avoids the EUC tripping for a single value affected by disturbances. Processor counter is crucial for both system availability avoiding spurious trips and for safety applications because it could fail dangerously preventing the EUC from being tripped, in case of dangerous scenario.

The minimum reacting time for the TMM board is **0.6 seconds**, due to the fact that the TMM acquires 3 samples for each measurement and performs a comparison to verify the correctness of the values.

7.1.3 TMM discrete inputs (INH, TMI, SAI, RST)

TMM board receives reset, trip multiply, special alarm inhibit and inhibit signals from backplane. Those signals are in fact transmitted from RCM through the backplane to all boards in the rack. They are critical for the safety-related functionality as they have the potential to inhibit or bypass the safety function with dangerous consequences. These commands shall be managed via dry contacts (discrete inputs) transmitted from backplane to TMM board.

7.1.4 TMM Power Supply

TMM is powered by RCM through backplane and is equipped with distributed power regulation functionality that improves reliability. It manages the power supply received, converts its 24Vdc power supply input to all regulated voltages needed by all devices (USB, SDRAM, CPU etc.), on-board processors and transducers, reducing the potential for rack single-point failures compared to systems that generate regulated voltages for the entire rack in a centralized power supply.

Power supply input from RCM shall comply with the following characteristics:

- Nominal: +24 Vdc;
- Continuous for generic applications, not safety-related: +22 to +30 Vdc;
- **Continuous for functional safety related applications: +23.1 to +26 Vdc;**
- Transient (<1 sec): +18 to +36 Vdc
- Ripple: <100mV pk to pk

The continuous voltage range +22 to +30 Vdc can only be used for generic (not safety-related applications). For functional safety-related applications the admissible continuous voltage is +23.1 to +26 Vdc. This voltage range guarantees that all safety-related functionalities of the system are effectively guaranteed: the system is able to carry out properly the allocated safety function, the node voltage sense diagnostics works properly (relay sense line proper distinction and no unintended system fault due to supply voltage values) and the system reboots correctly, when required.

7.1.5 TMM outputs requirements

TMM analog outputs MUST not be used for safety-related applications, all analog outputs are not safety relevant. TMM outputs relevant for safety applications are relay outputs. TMM is equipped with individual and fully independent SPDT electro-mechanical relays fully configurable that can be voted with other relay channels on the same boards or on other modules. TMM relay outputs are protected against overvoltage and transient voltage peaks through dedicated varistors installed on relay contacts.

TMM relay outputs can be managed independently from the TMM inputs (there is not a 1oo1 correspondence between TMM input and output channel), but are fully configurable. Through the Setpoint Configuration Software, it is possible to configure each output relay independently, driven by inputs on the same boards or on different boards with a user-defined voting logic between inputs triggering relay trip.



TMM monitor NO (Normally Open) contact of the onboard output relay(s) de-energizes the load when at least one of the input sensors reaches the configured threshold set. The output relays **MUST** be configured in Normally energized (De-energize to trip) configuration, in order to guarantee the reaching of the safe state in case of either loss of power supply or in case of wiring failures, increasing the overall system reliability (fail-safe operating principle). The relays **MUST** be configured as NOT OK= relay opened; any NOT OK condition determines relay output contact opening.

TMM output relays response depends on the logic of the inputs driving the relay itself set by the SIS integrator. If the relay is driven by only one input (1oo1), the removal/loss of the input shall determine relay de-energization (contact opening). Whereas if the relay is driven by more than one input, the response depends on the logic set between inputs, the relays follow the configuration defined. If for example the relay is driven to trip by two probes in 2oo2, the loss of both of them is necessary to trigger relay trip (the loss of only one probe does not de-energize the relay). This behavior has to be evaluated by the SIS integrator depending on the specific application.

TMM output relays are all identical and fully independent, consequently it is possible for the user to implement full redundancy between any of relay output channels to increase system reliability.

TMM output relays are tripped (de-energized) due to the following conditions:

- ✓ Configuration uploading via USB;
- ✓ Inputs readings over the set threshold, following the logic configured;
- ✓ Removal of both power supply inputs from RCM (if redundant power supply is present), otherwise single power supply input removal;
- ✓ TMM module disconnection from the VC-8000 rack;
- ✓ RCM module disconnection from VC-8000 rack;
- ✓ Probe(s) disconnection driving the output relay, following the logic implemented between inputs via Setpoint Configuration Software;
- ✓ Out of Specs (Out of OK range) (ref. to paragraph 7.1.1 for the OK ranges of different sensor types) input value readings.

TMM relay outputs can be driven either by the inputs on the same TMM board, or by inputs on different boards of VC-8000 rack, when properly configured through Setpoint Configuration Software.

When safety function inhibit command is activated, the TMM output relays are not tripped even when the dangerous threshold is reached (safety function inhibition).

One issue that could be relevant for the end-user, having no impact for system reliability, but only in terms of availability for the end-user is the trip of the same output relays by safety inputs and non-safety inputs. Tripping the same output relay(s), driven by both safety inputs and not safety measurements, would not compromise the reliability of the system, but would only worsen the availability. This would in fact increase the spurious trip rate, defined as the false trips triggered by not safety inputs, because the machinery would be driven in safe state even when no safety issue (trip threshold reached by not safety-relevant inputs) is present. In order to allow the end-user not to compromise the availability of the system, based on the previous considerations, the suggestion is to configuring the system so that the safety-relevant inputs are voted to trip dedicated output relay(s), that are not the same tripped in case of not safety inputs. In this way, if the alarm threshold is reached by not safety inputs, the relative output relay could be used to trigger only alarm and not trip of the machinery. This solution maintains the reliability unchanged; but improves the availability of the system.

7.1.6 TMM Fault

TMM fault status is managed through the transmission of the fault signal to the backplane. TMM fault status diagnostics by the system is performed through the triggering of the RCM fault relay (that indicates rack fault status).

The RCM fault relay is “activated” to indicate rack fault in the following conditions:

- ✓ Module start up;
- ✓ SAM communication to TMM stopped;
- ✓ TMM ADC stops providing data;
- ✓ If data from the TMM ADC suffers from a stuck bit;
- ✓ If any sensor or measurement has a NotOK status;
- ✓ If Relays are not in expected state (only for TMM_FS functional safety versions);
- ✓ Invalid TMM Configurations;
- ✓ Invalid TMM Personality file;
- ✓ Invalid TMM metadata file;
- ✓ Any hardware failure that prevents the module from initializing/operating correctly for TMM;
- ✓ Unable to load and execute TMM Firmware;
- ✓ The loss (disconnection) of any board input “activates” the fault status, the fault status is automatically deactivated upon reconnection of the input.

The fault relay is one for the entire rack and managed by RCM card, since a rack can be equipped with several modules that potentially can be used to managed different safety functions. This fault relay shall be used by the end-user as an annunciation of any fault able to affect the entire rack and all the safety functions with it. As required by the application standard of IEC 61508 (e.g. IEC 61511) the end-user is responsible for the implementation of the proper fault management to protect the EUC when the SIS is not able to perform safety functions, by the implementation of other safety features (not SIFs), having the same capability in terms of risk reduction, for the entire time while the SIS is unavailable or, when this is not feasible, force the machine into the safe state.



The fault relay for safety applications **MUST** be configured in De-Energize to Trip (normally energized mode) in compliance with fail-safe operating principle. Based on this assumption, power supply loss is also to be considered a fault condition, as the loss of power supply “activates” the fault status. In case of fault activation, the fault relay contact is opened (NOT OK condition = relay opened).

The fault relay activation condition, indicating a rack fault status has to be managed by the SIS integrator depending on the specific application. No mandatory prescription is in place regarding the necessity to trip the machinery, based on the fault relay activation conditions the end-user shall evaluate how to manage the fault status in terms of effects on the EUC.

As there is only one safety-relevant fault relay that indicates the faulty status at rack level, if the rack is composed of safety-relevant inputs and standard (not safety) inputs, the fault relay would be “activated” by both inputs. This does not worsen system reliability but has potential impacts for the availability of the system. In this case in fact the fault status activated by non-safety inputs would impair the overall availability of the system, being the fault relay unique. A possible solution to avoid availability degradation that the SIS integrator could implement, if needed, is a configuration of the relay logic combining the evaluation of the status of the SIL board output relay and of the fault relay e.g for the evaluation of channel status. The evaluation and comparison of the status of the SIL board output relay and of the fault relay to trip the machinery could be a possible solution to avoid degradation in availability due to non-safety inputs.

7.1.7 TMM Hardware Diagnostics

TMM is equipped with diagnostics implemented at hardware level, capable of detecting potentially dangerous failure modes of the system.

TMM has internal diagnostic capabilities able to monitor critical voltage values in the different parts of the circuitry and to compare them with the expected values. For all voltages defined as critical, node voltage sense diagnostics reads the value and is able to detect overvoltage, undervoltage and no voltage conditions. In case of voltage values out of the acceptable range or null, the system is rebooted. The described principle is acceptable for voltage references assuming that the fault relay is de-energized during system rebooting. This routine is implemented mainly for temperature reasons, in order to avoid false trips arising from temperature peaks. Node voltage sense diagnostics is furthermore able to detect mismatch between the microprocessor command provided to the relay(s) and the relay status feedback from node voltage sense. In case of mismatch, the system is driven in fault condition.

During boot sequence, all the relays are set in not powered state; node voltage sense reboots the system in case of mismatch between the read relay status and the expected one. During board runtime, in case of mismatch detection between the real and expected status of the relay, the system fault is triggered.

Node voltage sense consists in one voltage value checked every cycle. The complete check of all voltages by node voltage sense for fault detection is carried out every 400ms: the overall time duration necessary to complete all checks carried out by node voltage sense.

When a mismatch is detected in background, during the next Runtime cycle the module manages it and sets accordingly the fault relay. The overall diagnostics timing includes the background phase duration and the runtime time necessary to set the fault relay upon mismatch detection.

TMM hardware is characterized by a watchdog, external to the microprocessor that is able to detect problems at microprocessor level, such as infinite loops and reset the microprocessor subsequently (e.g. loss of communication between microprocessor and memories).

Hardware diagnostics is of crucial importance for the capability of the system to carry out properly the safety functionality, any dangerous failure of the diagnostics has the potential to dangerously impair the safety function.

7.2 TMM Firmware and Configuration Software SIL requirements

This section treats the functional safety relevant requirements for TMM firmware and configuration software in safety-related applications.



7.3 TMM Firmware SIL compliant release identification

The SIL firmware is unambiguously identified in respect to standard firmware, not safety-related through different release numbers.



IMPORTANT!

For each board required to be SIL compliant during the set-up of the system, the end-user shall check and ensure that the safety-relevant firmware is correctly uploaded on the board (TMM SIL firmware release).

7.4 Configuration Software SIL requirements

Setpoint Configuration Software is the tool allowing the end-user to set and configure the system according to the needs based on the specific applications.

The configuration shall be uploaded by the end-user via USB connector.

The allowable configurations of VC-8000 system, suitable for functional safety are implemented as checks at configuration software level. The configuration software has a pre-created list of inputs relevant for safety-applications and is characterized by warnings to the user in case of attempts of configuring the system in a way that is not suitable for safety-relevant applications (e.g. in terms of admissible inputs, relay configuration etc.). The configuration software clearly indicates the admissible TMM safety-relevant measures, to avoid misuse and configuration mistakes by the end-user.

The aim is to prevent unintended use and configuration of the system to perform safety functions. The configuration software is password protected to guarantee the safety and security of the system. The aim is to prevent unintended or malevolent modifications of the configuration with the potential to compromise dangerously the safety function (e.g. dangerous increase of the thresholds that cause the loss of protection of the EUC from the risk scenario).

The Configuration Software performs checks on the system in order to ensure that wrong configurations, not suitable for safety applications are not used:

- ✓ The Configuration Software checks that MODBUS communication between SAM and the other cards is inhibited. MODBUS control is not allowed to manage safety functions. For this reason, System Access Module (SAM), that manages through MODBUS communication system configuration and inhibit, trip multiply etc signals transmission is excluded from the VC-8000 safety-relevant parts. A SAM module safety related configuration is implemented, not able to transmit INH, TMI etc. signals through MODBUS communication for these reasons. The Configuration Software, through periodic checks ensures that these features, that could have potential critical impacts on functional safety, are inhibited.
- ✓ The Configuration Software prevents that any safety-relevant board can be set with the output relay in Energize to Trip Mode in order to ensure the proper relay configuration (Normally energized, de-energize to trip).
- ✓ The Configuration Software carries out a check channel by channel to allow the proper distinction between safety-relevant and non-safety relevant inputs;
- ✓ The Configuration Software has a dedicated Maintenance Section where all events and faults at rack level are recorded;
- ✓ The new configuration is uploaded via USB, upon completion of configuration uploading the system reboots. No configuration change is allowed online, when the EUC is running. The unintended disconnection of USB plug during configuration uploading (not yet finalized) on the board does not alter the existing configuration.



7.5 Firmware SIL requirements

TMM SIL firmware is unambiguously identified from the standard firmware, not for safety applications through part number and release number. The firmware is stored in the Flash Memory.

The relays are closed in the normal configuration upgrade (relay bypassed). When uploading the firmware, the system is not performing the safety function (relays are closed). Firmware upgrading takes about 4 seconds. When uploading the firmware, the protection of the system is not lost, safety is maintained. During the uploading of the configuration the relays remain in the same state, the system continues to perform the safety function and never loses the protection. Once the configuration uploading is completed the system reboots. When the system is rebooted all relays are opened.

The safety relevant firmware has a crucial importance for the VC-8000 system safety function as it is responsible for relevant diagnostic functionalities implemented through routines.

- ✓ The firmware is of crucial importance combined with voltages hardware diagnostics, because a firmware routine is responsible for the acquisition of the value sampled by node voltage sense and for the comparison with the expected value to detect undervoltage, overvoltage and no voltage conditions. A dedicated firmware routine is also responsible for the mismatch detection of the command provided by the microprocessor to the relay(s) and the relay(s) status feedback.
- ✓ A time-out routine is present for loss of data/invalid data from analog-to-digital converter (ADC) to microprocessor that in case of loss of data detection drives the system in fault condition;
- ✓ A firmware routine is present in order to detect out of specs (out of OK range) input readings, comparing the inputs acquired with the admissible range depending on sensor type (according to the OK range reported in paragraph 7.1.1 for each sensor type);
- ✓ A firmware routine is present able to detect data stuck-at for a certain time interval.
- ✓ Channel cycling and overload recovery is not possible. Only single cycle settings are implemented, gains and rates are not changed.

7.6 Environmental and operating conditions

The TMM shall be installed and operated respecting the following environmental and operating conditions, that guarantee that the system performs the allocated safety function in compliance with its safety integrity requirements. The use of the system changing any of the following environmental and operating conditions out of the admissible range has the potential to impair the safety functionality of the system under end-user responsibility. All considerations and assessment results reported throughout this document are based on these assumptions.

The following characteristics are applicable to the whole MPS VC-8000, taking into consideration the 16 Slot Rack configuration unless otherwise noted.

Characteristics	Characteristics
Operating Temperature	-20°C to +65°C
Storage Temperature	-40°C to +85°C
Humidity	5% to 95%, non-condensing
Power supply input voltage	Nominal: +24 Vdc Continuous for generic applications, not safety-related: +22 to +30 Vdc. (see note 1) Continuous for functional safety related applications: +23.1 to +26 Vdc (see note 1) Transient (<1 sec): +18 to +36 Vdc Ripple: <100mV pk to pk
Power fuse rating	10A
Maximum allowable power consumption	≤ 160W, <8A when input power voltage is 22 to 26 Vdc. - NOTE: Assumes fully loaded 16-position rack with display, redundant SAMs, all relays energized, all 4-20 mA outputs at full scale, and maximum transducer power requirements.
Mounting Orientation	Vertical
Shock	15 g for 11 ms (acc. to IEC 68-2-27, Ea)
Vibration	10 – 55 Hz, 0.75 mm / 55 - 500 Hz, 2 g (acc. to IEC 68-2-6)
Weight	Up to 9,3 kg
EMC Compliance	According to IEC 61326-1



*Note 1: The continuous voltage range +22 to +30 Vdc can only be used for generic (not safety-related applications). For functional safety-related applications the admissible continuous voltage is **+23.1 to +26 Vdc**. This voltage range guarantees that all safety-related functionalities of the system are effectively guaranteed: the system is able to carry out properly the allocated safety function, the node voltage sense diagnostics works properly (relay sense line proper distinction and no unintended system fault due to supply voltage values) and the system reboots correctly, when required.*



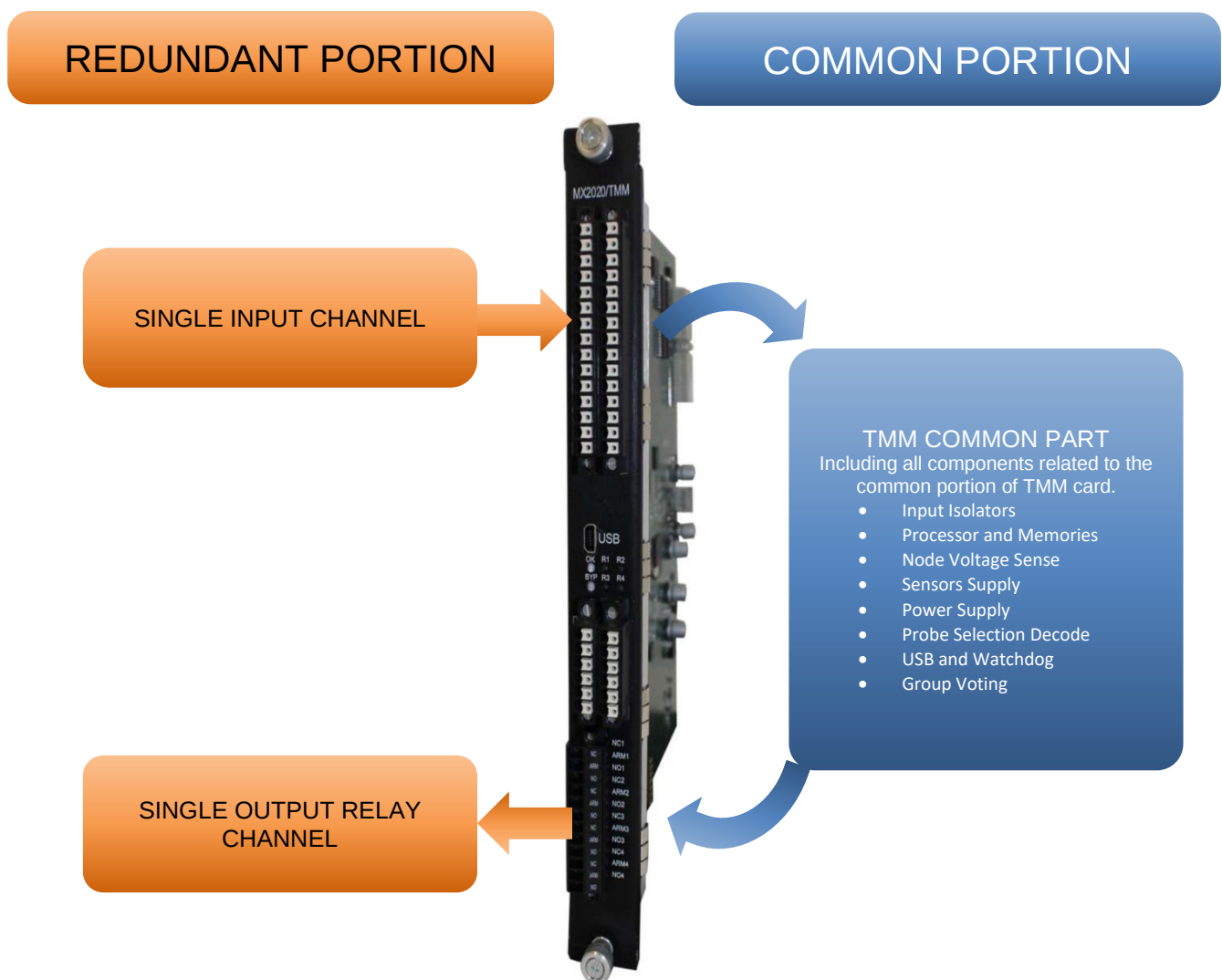
IMPORTANT!

TMM operation and maintenance **MUST** be managed by personnel having the proper training and knowledge.

8 VC-8000 TMM functional specifications

The Temperature Monitoring Module (TMM) has been assessed independently in respect to the other cards and components of the MPS-VC8000 rack in order to allow BK Vibro America to arrange the rack as per customer needs based on the specific application.

TMM board has 6 input channels and 4 output relays that can be configured independently, the FMEDA analysis has been carried out taking into consideration the following main subsystems split in redundant and common portions:





The TMM redundant part is split into:

- Input redundant part: consisting in the hardware components, part of the input subsystem, in redundant configuration;
- Output redundant part: consisting in the hardware components, part of the output subsystem, in redundant configuration;

The TMM common part consists in all other parts of the board that are not in redundant configuration (ADC, Processor and Memories, Node Voltage Sense, USB and Watchdog etc.).

As the six input channels are equipped with two identical ADCs in order to arrange the system in a proper way and to allow full independency and redundancy between input paths, the redundancy cannot be realized using any one of the inputs of the same board. The channels 1, 2, and 4 cannot be used together to make a redundancy, but they shall be used with one of the other channels (3, 5 and 6), being the two groups of channels wired to two distinct ADCs.

The analogue outputs have been excluded from the analysis since they are not safety-relevant part of TMM.

The output relays can be set in redundant configuration using two of any available relays on the TMM board.

The Functional safety analysis, based on the FMEDA, has produced results that are split in the previously reported categories (Input redundant part, Output redundant part and Common part).

TMM is in fact characterized by a common part to the whole board, redundant input channel having completely independent paths and redundant output channels having completely independent paths.

The resulting failure rates have been apportioned following these criteria. The overall calculation for the whole TMM board has to comprehend all previous contributions, with voting logics of redundant parts based on the specific architecture.

8.1 TMM random hardware failures

This section is related to the random hardware failures of VC-8000 Temperature Monitoring Module (TMM).

A systematic FMEDA analysis, extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis, was carried out to estimate failure rates, the failure modes and their distributions.

The resulting failure rates are based on the following assumptions:

- Failure modes distribution and failure rates are based on Quanterion Solutions Incorporated database, that is a part of Reliability Information Analysis Center (RIAC);
- Electronic Parts Reliability Data (EPRD-2014) is used as the reference database for electronic components;
- Failure Mode/Mechanism Distributions FMD-2016 is used as the reference failure modes and distribution database;
- Failure rates are constant, wear-out or infant mortality contributions are not included;
- All the internal failures of any parts of a board under analysis resulting in the depowering of the faulty relay, have been considered as dangerous detected. This means that the fault relay cannot necessarily be used to drive the EUC into the expected safe state;
- The failure rates are expressed in Failures in Time (FIT):

$$FIT = 10^{-9} \frac{1}{h}$$

- The response time is relevant for the safety purpose, the reacting time for the expected safety function has not been assessed during the FMEDA. Failure modes having an impact on the equipment response time have been anyway evaluated and classified as dangerous;
- Propagation of failures is not relevant, unless otherwise noted;
- All components that are not part of the safety function and cannot influence the safety function are excluded from the analysis;
- All devices assessed have been designed to manage the expected safety function in fail-safe orientation;
- The failures that have the potential to affect the functionality of a whole card, if detected, have generally the effect to drive the faulty relay in the "not powered" condition;
- The power supply section of the whole system has been analyzed only on the RCM board that contains the main power supply protection devices able to fail in a dangerous undetectable way;
- Sensors, including the eventually interposing devices, such as Zener barriers or isolators, are excluded from this analysis;
- Materials are compatible with process conditions, and environmental condition expected during the design phase;
- Failure of the metal case of the rack, including defects in fabrication have been considered as negligible;



- The device is installed and used as per manufacturer's instructions;
- All boards have been developed/manufactured/designed in compliance all applicable IEC standards, including the IEC 61326-1

8.2 Failure modes

Temperature Monitoring Module (TMM) failure modes are treated in detail in the FMEDA Report, whose results are included in the Third-Party Functional Safety Assessment Report.

8.2.1 Failure modes detection by internal diagnostics

All TMM failure modes, both detected and undetected by internal diagnostics are treated in detail in the FMEDA Report. The macro categories of modes of failure detectable by the internal diagnostics that can arise from different kinds of failures of different components in the circuitry are those that result in:

- Loss or invalid data from ADC to microprocessor;
- Input readings out of specs (out of OK admissible range);
- Wrong voltages in different parts of the circuit;
- Mismatch in relay status in respect to microprocessor command;
- Infinite processor loops;
- Loss of communication between microprocessor and memories;
- Sensor or measurement in NotOK status;
- Invalid TMM Configurations;
- Invalid UMM Personality file;
- Invalid TMM metadata file;
- Any hardware failure that prevents the module from initializing/operating correctly;
- Unable to load and execute TMM Firmware;
- The loss (disconnection) of any board input "activates" the fault status, the fault status is automatically deactivated upon reconnection of the input.

The main undetectable failures that can dangerously compromise the safety function are those that result in changing the system response within specs, within the acceptable range: the system responds providing an output in the admissible range but is affected by faults that alter the response, that is consequently not reliable. All failures of the diagnostics are dangerous and undetectable for the system as they compromise the diagnostic capabilities of potentially dangerous faults.

8.2.2 Failure modes of the internal diagnostics

The failure modes of the internal diagnostics can be either safe or dangerous oriented. The safe oriented ones are those that allow the diagnostics to detect a faulty status even if the system is not in fault condition (unintended activation of system fault). The potentially dangerous failure modes of the diagnostics hardware components are whereas those that compromise the diagnostic capabilities and that make the diagnostics either not available or malfunctioning. Node voltage sense fault would compromise the system capability to detect wrong voltages in different parts of the circuitry or relay status following microprocessor command. Watchdog fault would instead impair the capability of the system to detect infinite processor loop and loss of communication between microprocessor and memories, compromising critically the safety function.

8.2.3 Diagnostic test interval

Diagnostic test interval of the diagnostics for dangerous detected failures, defined as the interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage, is fixed less than one minute.

8.2.4 System output

When the internal diagnostics reveals a fault, the RCM fault (NOT OK) relay is unpowered to indicate system fault, when any of the conditions reported in paragraph 7.1.6 happens. TMM output relay(s) are also tripped (de-energized) when any of the conditions reported in paragraph 7.1.5 is verified.



8.2.5 Failure rates and FMEDA Results

The FMEDA analysis of the TMM has produced the following overall results, split in to three categories in order to allow a proper modelling, during system integration taking into account the specific architecture.

The following table summarizes the results of the Functional safety assessment conducted on the TMM board by a Third-Party.

In this specific case, the hardware used for all inputs is identical independently from the sensor type, consequently, the values resulting from the analysis can be used for any channel type. In order to simplify the system assessment, the negligible differences between the failure rates of the input channel obtained considering the different typology of temperature sensors, have not been considered in the resulting channel listed below. The following data represent the worst-case scenario.

TMM NOT REDUNDANT PART						
λ_S	λ_{DU}	λ_{DD}	SFF	DC	TYPE	SIL Cap.
6,63212E-07	2,68003E-07	1,05439E-07	74,15%	28,23%	B	1
REDUNDANT INPUT CHANNEL (COMMON)						
λ_S	λ_{DU}	λ_{DD}	SFF	DC	TYPE	SIL Cap.
1,23743E-07	7,57079E-08	5,0229E-08	69,68%	39,88%	B	1
REDUNDANT OUTPUT CHANNEL (OUTPUT RELAY)						
λ_S	λ_{DU}	λ_{DD}	SFF	DC	TYPE	SIL Cap.
5,97277E-08	3,27085E-08	2,40947E-09	65,51%	6,86%	A	2

As indicated in the previous table, TMM board failure rates data are apportioned into:

1. TMM Not Redundant Part: all parts of TMM board circuitry apart from the redundant parts of the input and output channels (ADC, Memories, Microprocessor etc.).
2. Redundant Input Channels: the TMM redundant input channels include the hardware circuitry of TMM inputs, independently from the sensor type. The analysis is not split in this case in the different sensor typologies, but the worst-case scenario is considered, being the differences in TMM inputs negligible as a function of sensor type.
3. Redundant Output Channels: the redundant part of TMM output channels. The hardware of all output relays is identical, consequently the FMEDA results evaluated on one channel do not vary for the other channels. TMM single relay output was analyzed and the considerations remain the same for the others, being fully identical and independent.

The parameters reported in the previous table are the followings:

λ_s = safe failure rates: failure of elements or subsystems that play a part in implementing the safety function, as they result in the spurious operation of the safety function or in the increase of the probability of spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state;

λ_{DU} = dangerous undetected failure rates: failure of elements or subsystems that play a part in implementing the safety function that prevent a safety function from operating when required (demand mode) such that the EUC is put into a hazard or potential hazardous state and that decrease the probability that the safety function operates correctly when required. The dangerous undetected failure rates are not detected by diagnostic tests.

λ_{DD} = dangerous detected failure rates: failure of elements or subsystems that play a part in implementing the safety function that prevent a safety function from operating when required (demand mode) such that the EUC is put into a hazard or potential hazardous state and that decrease the probability that the safety function operates correctly when required. The dangerous detected failure rates are detected by diagnostic tests.

SFF=ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

$$SFF = (\sum \lambda_{s\ avg} + \sum \lambda_{DD\ avg}) / (\sum \lambda_{s\ avg} + \sum \lambda_{DD\ avg} + \sum \lambda_{DU\ avg})$$

DC=fraction of dangerous failures detected by automatic online diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total range of dangerous failure.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D\ total}}$$

TYPE: Complexity level of the backplane, evaluated against the requirement of IEC 61508 section (type A simple device);

**SIL Capability:**

SIL level that can be reached by the equipment.

The whole TMM board has to be modelled in terms of reliability calculations considering always all these three contributions. The calculation performed on the redundant input and output parts vary depending on the architecture implemented (number of channels used and voting logic between channels).

The following table shows a reliability calculation example performed on VC-8000 TMM.

EXAMPLE 2: Single TMM equipped with a single input in 1oo1 configuration (@ PTI (Proof Test Interval) = 1Year)

1oo1 of UMM NOT REDUNDANT PART	PDFavg	RRF
	1,1739E-03	851,89
1oo1 of REDUNDANT INPUT CHANNEL (COMMON)	PDFavg	RRF
	3,3160E-04	3015,68
1oo1 of REDUNDANT OUTPUT CHANNEL (OUTPUT RELAY)	PDFavg	RRF
	1,4326E-04	6980,16
TMM OVERALL RESULT	PDFavg	RRF
	1,6487E-03	606,53

The parameters calculated in the example reported in the table above are:

Probability of dangerous failure on demand (PFD) = safety unavailability of the safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.

Risk reduction factor (RRF) = the inverse of the probability of dangerous failure on demand (PFD).

The reliability data reported above shall be used to calculate VC-8000 TMM contribution, to be added to those of the other VC-8000 safety relevant parts.

The integration in the SIS, the whole SIS validation, and the PFD_{avg} calculation of the whole safety loop implementing the SIF is under end-user responsibility, together with the verification of the compliance with the allocated target SIL.

8.3 Systematic Capability

The systematic capability was assessed in order to evaluate the techniques and measures implemented to control and avoid systematic failures during the different phases of the safety lifecycle in accordance with the **IEC 61508-2, Route 1s**.

MPS VC-8000 was subject to a Third-Party Functional Safety Assessment that resulted in a systematic capability of SIL 2. The systematic capability provides a quantitative estimation of the robustness of the system against systematic failures resulting from project management, documentation quality and control requirements, structured design etc managed through all lifecycle phases, to prevent the system to fail in a systematic manner.

The declared systematic capability level is guaranteed only with the respect of requirements and limitations reported in this Safety Manual, in case of violation of the same the declared systematic capability can be totally or partially invalid. The use of the system by the end-user e-g in operating conditions or architectures others than those admissible as per this Safety Manual could impair the systematic capability and lead the system to fail dangerously and systematically.



8.4 Architectural and random constraints

VC-8000 Temperature Monitoring Module (TMM) is suitable for SIL 1 applications, in terms of architectural constraints, when configured in 1oo1 (HFT=0) simplex architecture because:

- TMM Not Redundant part (Type B device) is characterized by SFF of 74% (between 60% and 90%) and limits the reachable SIL to 1;
- TMM Input Channel (Redundant): is type B device characterized by SFF higher than 60% and are SIL 1 capable in terms of architectural constraints contribution;
- TMM Output Channel Redundant: is type A component, characterized by SFF higher than 60% and is SIL 2 capable in terms of architectural constraints contribution.

As TMM module results from the combination of all previous parts, the overall SIL reachable by the TMM in terms of architectural constraints is SIL 1 (limited by TMM not redundant part), in simplex (1oo1) architecture: single TMM input channel and single TMM output channel.

The other safety-related parameters relevant to achieve SIL 1 (in order not to worsen architectural constraints contribution) are:

- Average probability of dangerous Failure on Demand (PFD) < 10⁻¹
- Low demand model of operation;
- Hardware safety integrity evaluated through Route 1H;
- Systematic safety integrity evaluated through Route 1s;
- 10 years lifetime;
- TMM common part characterized by Hardware Fault Tolerance (HFT) equal to 0;
- TMM redundant part (both of inputs and outputs) characterized by Hardware Fault Tolerance (HFT) equal to 0;

A redundant architecture SIL 2 capable shall be composed of:

- Two TMM modules;
- Two redundant input channels wired to the two different TMMs (HFT=1);
- Two redundant output channels wired to the two different TMMs (HFT=1).

Depending on the specific configuration and application implemented, the end-user and SIS integrator shall evaluate the overall PFD_{avg}, considering all SIS contributions.

8.5 Common Cause Failures

Common cause failure rates estimation of the redundant parts, channels or subsystems composing the overall equipment under analysis, was carried out through the calculation of a value for β factor for each of them. Common cause failures result from a single shared cause and have the potential to affect more than one channel or more than one component of the overall equipment.

These may result from a systematic fault (e.g. a design or specification mistake), or environmental stress (e.g. excessive temperatures, electromagnetic interferences etc.) leading to an early random hardware failure, project systematic failures (e.g. due to the complexity of the product or due to the lack of experience with the new technology); no spatial separation between channels, human errors during maintenance and repair. Because common cause failures are likely to affect more than one redundant part or components of the overall equipment, the probability of common cause failures is likely to be dominant factor in determining the overall probability of failure, in order to provide a realistic estimate of the safety integrity level of the combined architecture

The β -factor model, treated in IEC 61508-6 Annex D and adopted for the analysis, is a widely used and realistic way to deal with multi-channel or redundant architectures typically up to four dependent elements, that allows to estimate and derive the probability of common cause failures limited to hardware. The β -factor model in fact relates the probability of common cause failure to the probability of random hardware failure; this methodology is not used to obtain an overall failure rate which takes into account the probability of software-related failures. The probability of common cause failures which involve the system as a whole depends on the complexity of the system (possibly dominated by the user software) and not on the hardware alone. Clearly, any calculations based on the probability of random hardware failure cannot take into account the complexity of the software. Reporting of common cause failures is generally limited to hardware failures, that are of most concern to the manufacturers of the hardware, systematic failures such as software failures are not considered practicable to model.

The estimated factors for common cause failures quantification are β and β_D , where β is the common cause failure factor for undetectable dangerous faults (which is equal to the overall β -factor that would be applicable in the absence of diagnostic testing) and β_D is the common cause for undetectable dangerous faults.

Upon identification of parts/components forming voted groups of the whole equipment, the first step of the approach is to establish which measures lead to an efficient defense against common cause failures occurrence (e.g. separation/segregation), diversity, complexity/experience/maturity of the project, analysis/assessment and feedback of data, procedures/human interface, competency/training/safety culture, environmental control, environmental testing). Each measure is associated to a value, a score based on engineering judgement, representing the contribution in the reduction of common cause failures. As extensive diagnostic tests may be incorporated into programmable electronic systems, allowing the detection of non-simultaneous common cause failures, the diagnostics contribution is included by dividing the overall contribution in two sets of values, X and Y. For each measure, the X:Y ratio represents the extent to which the measure's contribution against common cause failures can be improved by diagnostic testing.



The following common cause failure factors are those related to the TMM parts and subcomponents that can be arranged in redundant architecture:

Equipment redundant components	β	βD
Board input channels	2,00%	1,00%
Board output channels	2,00%	1,00%
Diverse TMM boards	2,00%	1,00%
UMM and TMM boards (inputs on one board driving the output of the other)	1,00%	0,50%

The data reported in the table were estimated for the 1oo2 architecture. The β and βD values can be calculated for different voting logics as follows (IEC 61508-6 Annex D Table D.5):

MooN		N			
		2	3	4	5
M	1	β_{int}	$0,5 \beta_{int}$	$0,3 \beta_{int}$	$0,2 \beta_{int}$
	2	-	$1,5 \beta_{int}$	$0,6 \beta_{int}$	$0,4 \beta_{int}$
	3	-	-	$1,75 \beta_{int}$	$0,8 \beta_{int}$
	4	-	-	-	$2 \beta_{int}$

Maintainers shall be trained (with training documentation) to understand the cause and consequences of common cause failures.

9 Installation and commissioning

VC-8000 MPS Machinery Protection System shall be mounted and installed in the commissioning phase following the instructions reported in the “*Setpoint Machinery Protection System – Operation and Maintenance S1079330*”, taking into consideration the additional TMM hardware requirements reported in paragraph 7.1.

**IMPORTANT!**

TMM installation, mounting and commissioning shall be carried out by properly trained personnel.

DURING START-UP PHASE, THE SIS INTEGRATOR MUST CHECK AND ENSURE THAT THE SAFETY-RELEVANT FIRMWARE IS UPLOADED ON THE BOARD (SIL FIRMWARE RELEASE).

The following checks shall be carried out during TMM commissioning phase, to ensure that the system carries out properly the expected allocated safety functionality:

- Check that the board has the functional safety label stamped on, containing the item ID certified for functional safety;
- Verify that the TMM board and the populated PCB have no visible sign of damage;
- Inspect all connection/terminal boards to backplane, to input sensors and output relays, to evaluate their integrity and to detect any broken, defective, loose etc connection;
- Ensure that the input sensor(s) to be installed are those allowed for safety-relevant applications, listed in paragraph 7.1.1 of this Safety Manual;
- Ensure that input sensor(s) redundancy is implemented according to the criteria and constraints reported in paragraph 7.1.1;
- Ensure that output relay(s) redundancy is implemented according to the criteria and constraints reported in paragraph 7.1.5;
- Ensure that no visible sign of damage and moisture are present on TMM terminal boards and on the board;
- During the TMM board connection to backplane check and ensure the proper connection to ensure that it is not faulty or loose;
- During input sensor(s) wiring to TMM terminal board, check the proper connection (through solder screw flange connections) of the probe to the terminal board, in order to prevent any mechanical failure or improper input connection. Inspect all connectors and ensure that they are not loose;
- Check the connections to TMM terminal board, in order to prevent any mechanical failure or improper input connection. Inspect all connectors and ensure that they are not loose;
- Ensure that the output relay(s) connections to the rest of the SIS are not loose;
- Plug in the USB connector to upload the configuration and verify that the system reboots after successful completion of configuration uploading;



- Ensure that the password protection against unintended or malevolent configuration changes is active;
- During boot sequence, check that all the relays are set in powered state (24Vdc);
- Verify that the fault relay is activated (system fault active) at module start-up (every time the system reboots);
- Configure and check the dangerous threshold limits (minimum and maximum of the admissible range) and the configuration (number of inputs, voting logic etc) of TMM inputs and outputs;
- Check that system configuration through MODBUS is inhibited;
- Verify that there are no unexpected events in the system events list;
- Verify that the sensor(s) type(s) are allowed as safety-relevant inputs through Configuration Software checks (that indicate whether a sensor type is suitable or not for safety applications);
- Verify that all relays configured to be used for functional safety applications are configured in normally energized (de-energize to trip configuration) and in Not Ok status equivalent to relay open through Configuration Software checks;
- Check that the power supply is set in the admissible range for safety applications (paragraph 7.6), together with all other admissible operating conditions;
- Check that the safety-relevant firmware (SIL firmware release identified in paragraph 7.3) is uploaded on the board.

10 Proof testing

The proof test interval shall be chosen according to the calculations carried out by the SIS integrator in accordance to the required safety integrity level allocated to the Safety Instrumented Function (SIF). VC-8000 TMM does not have stringent proof test interval requirements, because periodical calibration on TMM is not required and there are no critical components subject to degradation over time. There are no critical requirements in terms of calibration and components degradation, imposing the need of periodic proof testing. more frequent than every 5 years unless otherwise indicated in the specific test procedure.

Proof test interval could be reduced, increasing the frequency on testing, under SIS integrator responsibility based on the target SIL allocated to the Safety Instrumented Function (SIF) and the results of reliability calculations. Proof testing interval higher than 5 years is not recommended by BK Vibro America Inc.

Refer to Section 5 of manual S1079330 for further reference.



IMPORTANT!

The VC-8000 Machinery Protection System rack proof testing shall be carried out by properly trained and suitably qualified personnel.

The following are the periodic proof tests that shall be carried out on TMM board according to the periodicity specified. The proof test coverage that can be obtained through the implementation of the following tests is about 90%.

10.1 Connections and terminal boards inspection

The aim of the test is to carry out a visual inspection of all boards and connections of TMM board in order to ensure that all of them are integer, not damaged or worn and not loose.

All connectors and terminal boards shall be thoroughly inspected in order to verify their integrity and connection stability. Ensure that the connections are not defective, worn, damaged or loose

Check terminal board where the input probes are connected, inspect all connectors (solder screw flange connections) for integrity, to detect any damages, wear effects and looseness and ensure that the probes are stably connected to the terminal board.



Ensure the connection integrity and stability of the board output relay(s) to the rest of the SIS, inspect all connectors for integrity, to detect any damages, wear effects and looseness and ensure that the connections are stable and not loose.

In case of non-conformances arising from the inspection, proceed to proper maintenance and repair, in order to guarantee connection stability.

10.2 TMM board and populated PCB inspection

Inspect TMM board and the populated PCB to ensure that no visible sign of damage and moisture are present on TMM terminal boards and on the board. Verify that any board connectors have no visible sign of damage or moisture. In case of any non-conformity detection, the board shall be sent for maintenance and repair.

10.3 Relay driving by input sensor disconnection

The aim of the test is to evaluate that the system properly responds to the disconnection of the probe from the input channel (board relay output de-energization).

Testing procedure

- Configure the system so that one input channel drives one output relay in 1oo1;
- Connect the TMM relay outputs to an ESD simulator to verify the status of the output relay;
- Verify that the TMM relay output is energized evaluating ESD Simulator status;
- Disconnect the sensor from the input channel;
- Verify that TMM relay output is de-energized evaluating ESD Simulator status;
- Reconnect the sensor to the input channel;
- Reset the system;
- Configure the system so that two input channels in 2oo2 (HFT=0) drive the output relay (the disconnection of both triggers output relay trip);
- Verify that the TMM relay output is energized evaluating ESD Simulator status;
- Disconnect one input sensor;
- Verify that the output relay is energized through ESD Simulator status;
- Disconnect the second sensor;
- Verify that the output relay is de energized through ESD Simulator status;
- Reset the system.

Test Results (Pass/Fail Criteria):

The TMM probe disconnection from the input channel test is passed if when the sensor is disconnected from TMM, the configured TMM output relay is de-energized, according to the configuration logic implemented.

10.4 Fault relay activation testing

The aim of the test is to evaluate the proper activation (depowering to indicate system fault) of the fault relay upon disconnection of any input sensor.

Testing procedure

- Connect the RCM fault relay output to an ESD simulator to verify the status of the relay;
- Verify that RCM fault relay output is energized evaluating ESD Simulator status;
- Disconnect the sensor from the input channel;
- Verify that RCM fault relay output is de-energized evaluating ESD Simulator status;
- Reset the system;
- If the RCM fault relay is not de-energized, a crosscheck shall be carried out in order to identify where the problem is: disconnect an input sensor connected to another board in the rack and evaluate the activation (depowering) of the RCM fault relay to indicate system fault;
- If the fault relay is de-energized upon disconnection of the second probe, the problem/fault is in the fault signal path of the first board. Otherwise, if the fault relay does not de-energize in any case, the relay itself is in faulty status (e.g. welded contacts).
- Reset the system.

Test Results (Pass/Fail Criteria):

The fault relay activation test is passed if the RCM fault relay is de-energized (system fault activation) upon disconnection of any input. The cross-check test is aimed at identifying where the fault status is, either at board fault signal transmission path or at fault relay level.



10.5 Safety function test

The aim of the test is to verify that the safety function is carried out properly, upon reaching of the set dangerous threshold the output relay is de-energized.

Testing procedure

- Connect the TMM relay output to an ESD simulator to verify the status of the relay;
- Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Simulate an increase in temperature readings above dangerous threshold/temperature limits;
- Verify that the TMM relay output is de-energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NC);
- Decrease the temperature readings below dangerous threshold;
- Reset the system;

Test Results (Pass/Fail Criteria):

The safety function test is passed if the TMM output relay is de-energized when the input readings acquired by the sensor are above the dangerous threshold.

10.6 Power supply removal test on TMM output relay

The aim of the test is to verify that upon removal of a single power supply input (in case of redundant power supply) the system continues to operate normally, and the output relay does not de-energize. Upon disconnection of both power supply inputs whereas the TMM output relay shall de-energize. This test allows to detect any faults at board output relay level (e.g. welded contacts).

Testing procedure

- Connect the ESD Simulator to TMM relay output;
- Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Disconnect only PWR1 power supply input from RCM, maintaining PWR2 connected;
- Verify that the led P1 is off indicating a power 1 line fault and that the Maintenance Software indicates the PWR1 power supply fault event;
- Verify that the TMM output relay is still energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Reconnect PWR1 power supply input and then disconnect PWR2 power supply input from RCM;
- Verify that the led P2 is off indicating a power 2 line fault and that the Maintenance Software indicates the PWR2 power supply fault event;
- Verify that the UMM output relay is still energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Disconnect both PWR1 and PWR2 power supply inputs from RCM;
- Verify that the led P2 is off indicating a power 2 line fault and that the Maintenance Software indicates the PWR2 power supply fault event;
- Verify that the TMM relay output is de-energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NC);
- Re-connect PWR1 and PWR2 power supply inputs to RCM;
- Reset the system.

Test Results (Pass/Fail Criteria):

The test is passed if upon disconnection of only one power supply input (in case of redundant power supply), the system continues to operate normally, and the output relay is not de-energized. The removal of both power supply inputs shall whereas determine relay de-energization, trip.



10.7 TMM module disconnection from the rack test

The aim of the test is to verify that upon disconnection of TMM card from the rack the output relay is tripped, de-energized.

Testing procedure

- Connect the ESD Simulator to TMM relay output;
- Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Verify the status of the RCM fault relay (powered/unpowered);
- Disconnect the TMM Module from the rack;
- Verify that the Maintenance Software indicates the event (card disconnection);
- Verify that the TMM relay output is de-energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NC);
- Verify the status of the RCM fault relay (powered/unpowered);
- Re-connect TMM Module to the rack;
- Verify the status of the RCM fault relay (powered/unpowered);
- Restore the system to normal operation;
- Reset the system.

Test Results (Pass/Fail Criteria):

The test is passed if upon disconnection of TMM board from the rack, the TMM output relay is de-energized.

10.8 Node voltage sense diagnostics test

The node voltage sense diagnostics test is aimed at verifying that node voltage sense diagnostics is able to properly detect wrong input voltage values and that upon detection of wrong voltages, the system is subsequently rebooted.

Testing procedure

- Connect the ESD Simulator to TMM relay output;
- Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- Verify the status of the RCM fault relay (powered/unpowered);
- Increase the power supply voltage beyond the maximum operation limit, in order to trigger node voltage sense detection of wrong voltages in the different parts of the circuitry;
- Verify that upon detection of wrong voltages the system is rebooted;
- Verify that the Maintenance Software indicates the event;
- Verify that the TMM relay output is de-energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NC);
- Verify the status of the RCM fault relay (powered/unpowered), that shall indicate system fault;
- Re-connect TMM Module to the rack;
- Reset the system;
- Repeat the same steps decreasing the power supply voltage below minimum operation limit.

Test Results (Pass/Fail Criteria):

The test is passed if when a wrong voltage value is detected in the various sampling points of the TMM circuitry, the system is rebooted (the board relay is de-energized, and the system fault is triggered through the RCM fault relay).



10.9 Inhibit, Trip Multiply, Special Alarm Inhibit deactivation test

This test is aimed at verifying that the TMM is able to successfully deactivate Inhibit, Trip Multiply, Special Alarm Inhibit restoring the safety function. This test is crucial in order to detect any “stuck at” fault of these commands that maintained activated can compromise dangerously the safety function.

Testing procedure

- ✓ Connect the TMM relay output to an ESD simulator to verify the status of the relay;
- ✓ Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- ✓ Activate Trip Multiply command;
- ✓ Verify that the TMM relay output is energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NO);
- ✓ Deactivate trip multiply command;
- ✓ Verify that the TMM relay output is de-energized evaluating ESD Simulator status and performing continuity measurements between relay contacts using the multimeter (electrical continuity between ARM and NC);
- ✓ Decrease the temperature readings below dangerous threshold;
- ✓ Reset the system;
- ✓ Repeat the same procedure for inhibit and special alarm inhibit commands.

Test Results (Pass/Fail Criteria):

The test is passed if when the inhibit, trip multiply, special alarm inhibit are deactivated the safety function is correctly restored (the output relay trips upon reaching of the dangerous threshold by TMM input readings).

11 Maintenance, repair, de-commissioning and disposal



IMPORTANT!

VC-8000 TMM maintenance and repair shall be carried out by properly trained and qualified personnel.

All maintenance and repair activities shall be carried out by qualified personnel or in qualified repair centers.

In order not to worsen system availability and to minimize the potential for common cause failures, maintenance activities on redundant legs shall be carried out by different people at different times.

Procedures shall be in place to ensure that maintenance (including adjustment or calibration) of any part of the independent legs / channels shall be staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests shall be allowed to run satisfactorily between the completion of maintenance on one leg / channel and the start of maintenance on another.

All repaired items shall go through a full pre-installation testing, before start-up.

All parts of redundant systems (for example cables, etc) intended to be independent of each other, are not to be relocated, during maintenance and repair activities.

VC-8000 MPS Machinery Protection maintenance and repair shall be carried out following the instructions reported in the “*Setpoint Machinery Protection System – Operation and Maintenance S1079330*”.

11.1 Item Modification and Retrofit Management

Any modification request on VC-8000 by end user shall be subject to BK Vibro America Inc approval.

Any field returns (safety performance below target, deviations in the expected safety function etc.) shall be communicated to BK Vibro America Inc. Service Department in order to conduct an impact analysis of the proposed modification or retrofit activity.

11.2 De-commissioning or disposal of the item

VC-8000 Machinery Protection System de-commissioning and disposal activities shall be carried out by the Customers and end-users.

Customers and end-user are the sole responsible for the decommissioning and disposal of the product at the end of its useful lifetime. All applicable federal, state, local or international laws shall be observed. BK Vibro America Inc. has no responsibility connected with the disposal of the item at the end of its lifetime.

Contact