Brüel & Kjær Vibro
A member of the NSK Group

SIL Safety Manual

Setpoint Machinery Protection System

Safety Manual - VC-8000 Backplane and System Integration requirements

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.

Safety Manual **VC-8000 Backplane and Rack**, C107579.002 / V02, en, date of issue: 25.02.2022

Brüel & Kjær Vibro GmbH
Leydheckerstrasse 10
64293 Darmstadt
Germany

Phone: +49 6151 428 0
Fax: +49 6151 428 1000

Brüel & Kjær Vibro A/S
Lyngby Hovedgade 94, 5 sal
2800 Lyngby
Denmark

Phone: +45 69 89 03 00
Fax: +45 45 80 29 37

BK Vibro America Inc
1100 Mark Circle
Gardnerville NV 89410
USA

Phone: +1 (775) 552 3110

Hotline

Phone: +49 6151 428 1400
E-Mail: support@bkvibro.com

Homepage

www.bkvibro.com

Corporate E-Mail

info@bkvibro.com

Table of Contents

1 About this Safety Manual

This Safety Manual documents all the information and requirements relating to VC-8000 Machinery Protection System backplane and rack, required to enable their integration into a safety-related system that performs the allocated Safety Instrumented Function (SIF). This Safety Manual furthermore provides all constraints relevant for the integration of all VC-8000 Machinery Protection System safety-relevant parts in order to guarantee the performing of the allocated safety function, respecting the associated safety integrity requirements. The specific functional safety related requirements of the other VC-8000 safety-relevant parts are treated in detail throughout the dedicated Safety Manuals. This Safety Manual is an addendum to the SETPOINT MPS manual and shall be used in conjunction with it and provides all the information necessary for the end-user, relevant to integrate the device in a Safety Instrumented System (SIS), to install, verify, maintain and periodically test ensuring the respect of product safety requirements (item function, input and output interfaces etc). VC-8000 Machinery Protection System (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 VC-8000 Machinery Protection System for safety-related applications is declared only for the configurations, operating conditions and constraints reported in this Safety Manual and in dedicated Safety Manuals of the other VC-8000 safety-relevant parts. 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 product 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
S1077785.002	VC-8000 Machinery Protection System 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
λD	Dangerous failure rate (per hour) of an equipment or a sub-system
λDD	Dangerous detected failure rate (per hour) of an equipment or a sub-system
λDU	Dangerous undetected failure rate (per hour) of an equipment or a sub-system
λS	Safety failure rate (per hour) of an equipment or a sub-system
λN (P+F)	Failure rate obtained through the sum of NO PART and NO EFFECT
λOT	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 (λ(t)) of an entity (single components or systems) such that λ(t). 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 of 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 VC-8000 Machinery Protection System integration requirements

The Machinery Protection System (MPS) VC-8000 is a rack-based continuous machinery monitoring platform designed to fully comply with American Petroleum Institute Standard (API) 670 for machinery protection systems. The MPS VC-8000 monitors up to 60 vibration/position/speed channels or 90 temperature/process variable channels and displays in a single 19” rack. The system measures and alarms on a wide variety of vibration, position, speed, temperature and process variables inputs and provides monitoring functionality through the combination of basic modules types. The condition monitoring platform provides information to assess and protect rotating and reciprocating machinery from mechanical issues, through the continuous monitoring of parameters, mainly vibrations and temperature.

VC-8000 Machinery Protection System is designed to perform the safety functions reported in the table below, to mitigate the correspondent risk scenario described. The effectiveness of the risk reduction achievable has to be assessed by the end user for each specific EUC depending on the whole Safety Instrumented System (SIS) implemented to carry out the allocated Safety Instrumented Function (SIF) allocated

List of Expected Safety Instrumented Functions		
SIF n°	Expected Hazardous Scenario	Overall Safety Instrumented Function
SIF 1	Uncontained projection of machine parts due to an unexpected failure of its rotating parts.	Vibration monitoring of critical machine motion parts in order to activate the EUC shutdown prior it reaches a potentially dangerous condition.
SIF 2	Coupling mechanical uncontained failure causing projection of its parts due to an excessive coupling compression by the machine shafts.	Axial displacement monitoring on each critical machine shaft-end in order to activate the EUC shutdown prior it reaches a potentially dangerous condition.
SIF 3	Motion parts enclosed into machine casing or crankshaft housing that could be hit or introduce excessive vibrations due to an unexpected failure with consequent risks of projection of parts.	Machine casing acceleration monitoring or detection of mechanical looseness on reciprocation machine in order to activate the EUC shutdown prior it reaches a potentially dangerous condition.
SIF 4	An excessive temperature of bearings (radial or thrust) due to a lubrication system failure or unexpected bearings wear.	Temperature monitoring on each critical machine bearings (radial or thrust) in order to activate the EUC shutdown prior it reaches a potentially dangerous condition.

The MPS VC-8000 safety-relevant modules, involved in the system safety function, are listed below:

- VC-8000/UMM (Universal Monitoring Module) including $UMM_{CM;}$
- VC-8000/TMM Temperature Monitoring Module including TMM_{CM};
- VC-8000/RCM Rack Connection Module;
- 4 to 16 slots rack chassis (including the rack backplane);

Instead, the following components are excluded from VC8000 safety-critical path:

- VC-8000/SAM (System Access Module);
- VC-8000/PCM (Power Connection Module);
- VC-8000/RDP (Remote Display Panel);
- Integral Backlit Touchscreen Display;
- VC-8000/CMS (Condition Monitoring Software): the software is relevant for functional safety only regarding the fault reduction due to configuration check and limitations that the software implements prior to allowing a new configuration uploading to a card.

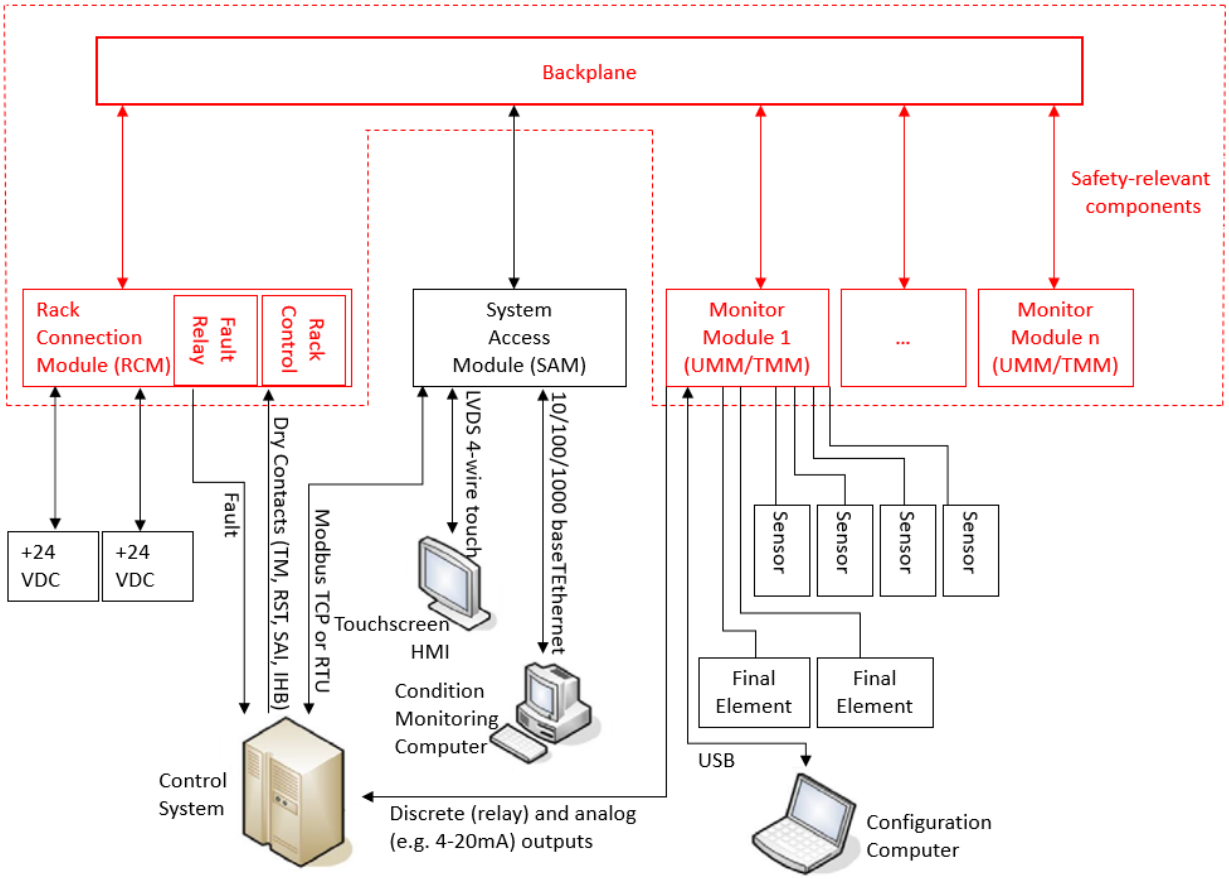
MPS VC-8000 safety function consists in the activation of the expected safety state of the EUC upon detection of over the threshold several safety-related parameters, continuously monitored and controlled. The activation of the safe state, that will be detailed by the end-user during a SIL allocation, will be managed by the output relay(s) of UMM and TMM cards. The fault relay is one for the entire rack and is managed through the Rack Connection Module (RCM). Since a rack can be equipped with several modules that potentially can be used to manage different safety functions (e.g. vibration and temperature monitoring on the same rack or two independent vibration control loops for NDE and DE bearings of a machine), RCM fault relay has to be used by the end-used as annunciation of faults 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 will be responsible to implement the proper fault management to protect the EUC when the Safety Instrumented System (SIS) is not able to perform safety functions, by the implementation of other safety features (not Safety Instrumented Functions SIFs), having the same capability in terms of risk reduction, for the entire time while the SIS in unavailable or, when this is not feasible, force the machine into the safe state.

Further details regarding each VC-8000 part relevant for safety applications are reported in the dedicated Safety Manuals.

The following figure shows the overall VC-8000 rack fully assembled.

The following diagram schematizes VC-8000 Machinery Protection System and identifies the safety-relevant parts (in red) distinct from the parts excluded from the safety-critical path (in black).



IMPORTANT!

This Safety Manual covers only for VC-8000 Machinery Protection System and provides the integration requirements in the overall Safety Instrumented System (SIS). The overall SIS is out of the scope of this Safety Manual, as it does not reside under BK Vibro America Inc. responsibility. BK Vibro America Inc. provides through this Safety Manual only requirements and constraints for the future system integration but is not responsible for validation of the overall SIS, where VC-8000 is to be integrated.

Elements such as sensors, final elements and power supply are reported for completeness in the schematic to represent the device scope, they are in fact out of BK Vibro America Inc. scope and supply. Their selection and installation reside under end-user responsibility. All functional safety relevant constraints and requirements reported in BK Vibro Safety Manuals MUST be respected in order not to impair system safety integrity. Any deviation from the expected safety behavior and safety integrity due to misuse by end-user is not under BK Vibro America Inc. responsibility.

The selection of sensors and final elements is in Customer Scope of Supply.

Any isolating and Zener barriers are out of the scope of supply, the evaluation and integration of any barrier in the system is under Customer Scope.

The VC-8000 Machinery Protection System is able to carry out the allocated safety function if composed **AT LEAST** by the following minimum set of modules:

- RCM (Rack Connection Module): 1 RCM must be installed in each VC-8000 rack in slot 1;
- Backplane and rack;
- At least 1 monitor module (TMM or UMM) depending on the safety function to be performed.

The monitor modules (TMM or UMM) in a standalone mode CANNOT carry out on their own the allocated safety function. In order to allow the system to carry out the expected safety functionality, MPS VC-8000 MUST be composed, at least, by the minimum set of modules previously listed.

Provided that the previous minimum architecture requirements are fulfilled, the configuration of the system to be selected and implemented has to be evaluated by the end-user/Safety Instrumented System (SIS) integrator depending on the specific requirements, foreseen application and risk scenario to be mitigated. The configuration, that MUST comply with the requirements and constraints imposed in the Safety Manual has to be evaluated in every case by the SIS integrator according to the machinery and to its potential risks for which the SIFs are conceived.

The main functionalities of the MPS VC-8000 safety-relevant components are reported below:

- Monitoring Module (TMM or UMM): modules designed to acquire field sensors measuring the physical variable to be monitored (vibration or temperature) that de-energize the load (through the opening of relay outputs contacts) when at least one of the input sensors (depending on the configuration and logic implemented) reaches the dangerous threshold set.
- Rack Connection Module (RCM): module equipped with redundant power supplies and responsible for power supply distribution to all boards in the rack. RCM furthermore acquires discrete inputs relevant for functional safety managing inhibit, reset, trip multiply and special alarm inhibit that are critical for system operation as they interfere with safety function performing. They are transmitted to the other boards in the rack through the backplane. RCM has also the rack fault relay onboard, that is the diagnostics of any fault in the rack. RCM receives fault signals from the other modules in the rack and triggers the system fault through the fault relay.
- Backplane and Rack Chassis: support and communication module that manages power supply and signals transmission between the different boards in the rack.

The VC-8000 MPS supports fully redundant and independent power supply inputs to the RCM boards.

The VC-8000 system operates in low demand mode.

This Safety Manual treats in detail the safety-related aspects of VC-8000 backplane and rack, the other safety-relevant modules are treated in detail in their dedicated Safety Manuals.

6.1 VC-8000 Safety relevant parts 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.

VC-8000 rack and backplane shall be ordered 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.

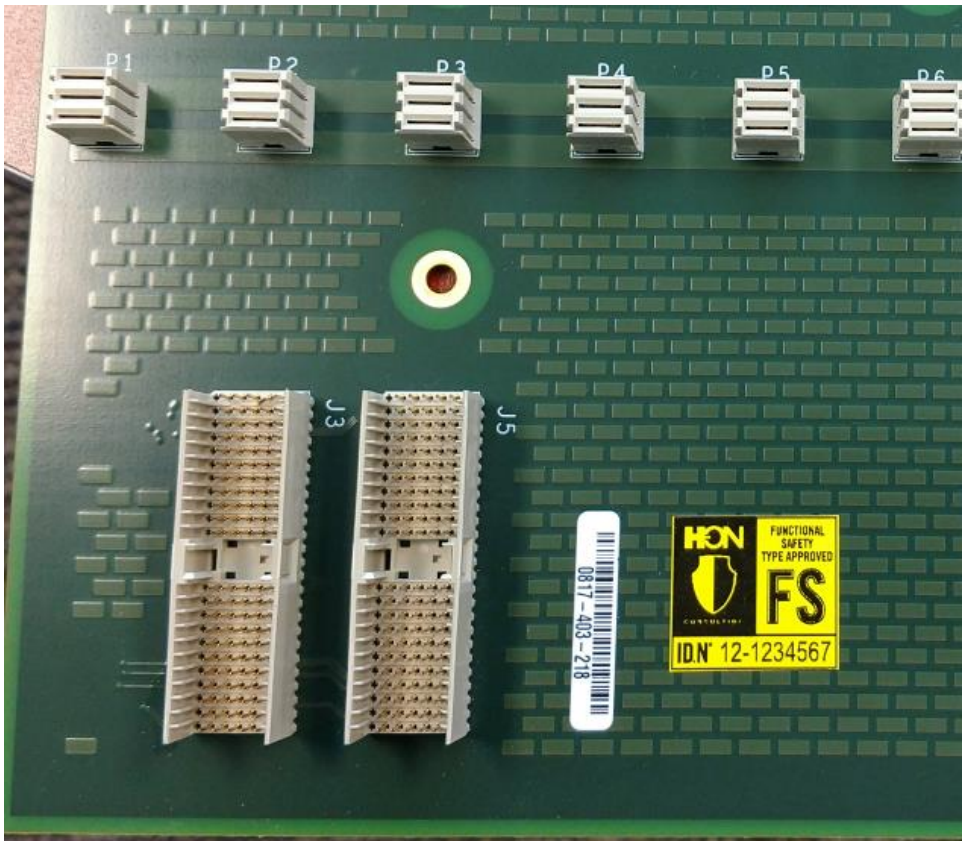
The VC-8000 rack suitable for SIL applications shall be selected according to the following part number criteria:

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 following (the other fields are selected by the end-user)

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

The identification criteria of all other SIL boards forming the VC-8000 system are detailed in their dedicated Safety Manual.



6.2 Basic Safety-related system architectures

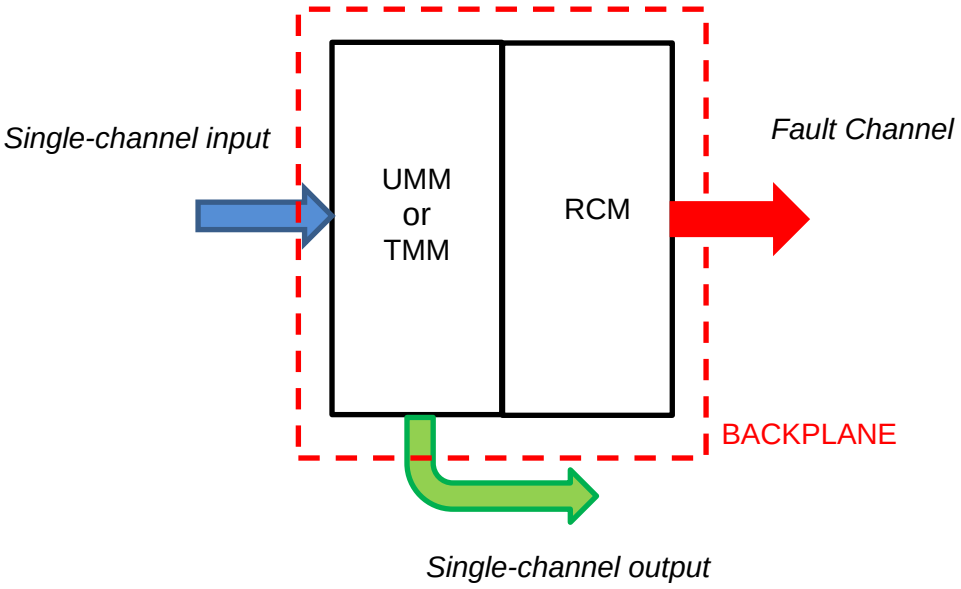
The MPS-VC8000 is a system characterized by the possibility to be arranged according to customer needs in many ways. A single rack can also be used to manage more than a safety function in parallel, also different in nature (different measurement type e.g. vibration and temperature). However, this flexibility involves some prescriptions that in terms of functional safety shall be taken into consideration when a rack has been arranged. The following system configurations are selected taking into consideration the most common VC-8000 applications. The suitable VC-8000 Machinery Protection System configuration has to be defined by the Safety Instrumented System (SIS) integrator depending on the specific application, ensuring the fulfilment of all constraints and requirements provided by BK Vibro America Inc in the Safety Manual. Below the basic configurations of the system and their architecture are described: Simple and Redundant configurations.

6.2.1 Simplex Configuration

The below diagram shows the minimum architecture usable to realize a safety function, based on MPS-VC8000 in a simplex configuration (HFT=0).

The simplex configuration of VC-8000 MPS is schematized in the figure below and consists of the following safety-relevant parts:

- Monitoring module (UMM or TMM) single channel input;
- Monitoring module (UMM or TMM) single channel output;
- Backplane and Rack Chassis;
- Rack Connection Module (RCM).



This architecture is characterized by the presence of a single card to acquire a single sensor through any one of the available input channels, in order to drive a single relay of the same board to the "unpowered" condition when a threshold limit is reached.

The single relay output shall be used to drive the EUC in the expected safe state.

In case a failure, that able to affect the whole system and not only the single channel in use, has been detected, the fault relay on the RCM board is driven in the “unpowered” condition in order to provide a feedback to a SIS.

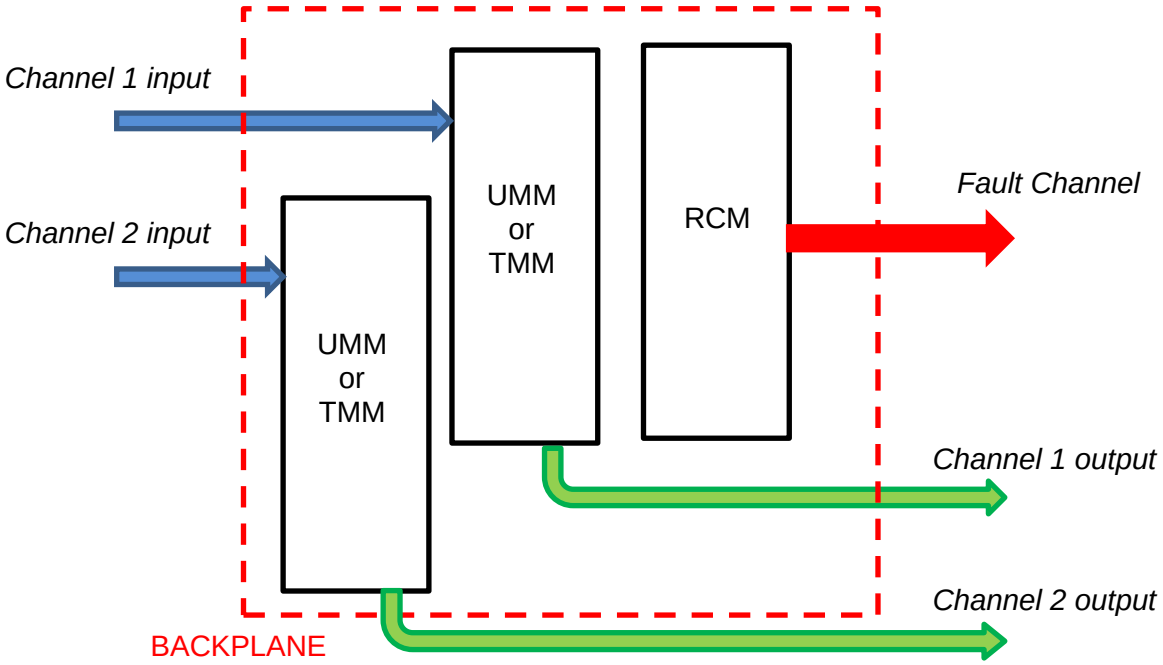
This simplex configuration can be used indifferently with UMM and TMM boards, depending on the specific application and on the physical variable to be monitored. The contribution of the redundant part of RCM, mainly related to the power supply and the relative protection devices, can be used either with or without the second power supply line connected.

The simplex architecture allows to meet the requirements for SIL 1 using a single monitor input and a single monitor output to carry out the safety function.

6.2.2 Redundant Configuration

The below diagram shows the minimum architecture usable to realize a safety function using the MPS-VC8000 in a redundant configuration (HFT=1).

- The redundant configuration (HFT=1) of VC-8000 MPS consists of the following safety-relevant parts:
- Redundant monitoring modules (UMM or TMM) with 2 input channels wired to distinct modules;
- Redundant monitoring modules (UMM or TMM) with 2 output channels wired to distinct modules;
- Backplane and Rack Chassis;
- Rack Connection Module (RCM).



This architecture is characterized by the use of two different cards to acquire two independent signals coming from two sensors installed so as to measure the same process variable, in order to realize a redundancy of the measurement. The effectiveness of the redundancy in terms of measurement is under the end-user responsibility such as the correct selection of all devices not included in the MPS-VC8000.

Both cards will be able to detect the over-the-threshold condition of their respective input signal and drive an output relay in the "unpowered" status. The reaching of the unpowered status of any one of the two output relays will be enough to drive the EUC in the expected safe state.

In case a failure, that is able to affect the system and not only the single channel in use, has been detected, the fault relay on the RCM board is driven in the “unpowered” condition in order to provide a feedback to the SIS.

The redundancy shall be made outside the MPS-VC8000 connections, for example, through the connection in series of the two NO contacts coming from the output relays, or through a proper management in a 1oo2 logic via safety PLC.

This redundant configuration can be used indifferently with UMM and TMM modules. The contribution of the redundant part of RCM, mainly related to the power supply and the relative protection devices, can be used either with or without the second power supply line connected.

Even if this architecture can be used to realize, through a management in a 2oo2 logic of the output relays, a duplex configuration, suitable for increasing the availability of an application, it is not recommended for safety-related application since the overall reliability of the MPS-VC8000 will be drastically reduced. However, the proper architecture selection is under the end-user responsibility. An architecture usable to optimize the performance of the MPS-VC8000 for reliability and availability could be the 2oo3.

The redundant architecture is SIL 2 capable using two monitors acquiring two distinct sensors and two independent relay output channels.

7 SIL requirements and constraints

This section treats the functional safety relevant requirements for VC-8000 Machinery Protection System operation such as environmental conditions for the use in safety-related applications.

7.1 Environmental and operating conditions

The whole VC-8000 MPS Machinery Protection System 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 is 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.*

The VC-8000 system is equipped with redundant and independent power supplies (inputs on RCM), the failure of one power supply input guarantees the operation continuity of the system. The power supply is fail-safe, the failure of both power supply inputs leads the system to the safe state, as it trips the EUC.

IMPORTANT!

The VC-8000 Machinery Protection System rack operation and maintenance MUST be managed by personnel having the proper training and knowledge.

8 VC-8000 Backplane and Rack chassis functional specifications

VC-8000 Backplane and Rack chassis is a subsystem part of a vibration monitoring system (rack based) for rotating machine or equipment in general, including reciprocating compressors, for the potential risks connected to an excessive motion of its rotating and moving parts.

MPS VC-8000 rack chassis, available in 16-slot, 8-slot and 4-slot sizes, have no safety function specifically allocated. It represents a support and communication structure that performs two main functions:

- Transmission;
- Communication.

VC-8000 backplane is relevant for functional safety as it allows power supply distribution from RCM to the other boards of the rack and the transmission/communication of signals exchanged between the boards installed in the rack (UMM, TMM, RCM), such as:

- Fault signal from any faulty board in the rack to RCM (Rack Connection Module);
- Synchronization signals;
- Inhibit (INH), Trip Multiply (TMI), Special Alarm Inhibit (SAI), Reset (RST) from RCM to the other boards in the rack.

Furthermore, being that the VC-8000 rack/chassis is made of an aluminum alloy (4 by 4 plates), it guarantees the mechanical protection of the whole system against any possible mechanical failures and provides to the system high mechanical resistance of the structure to mechanical strains, such as impact and bending. Based on these considerations, the mechanical failure due to the previous causes can be considered negligible for the whole system.

8.1 Backplane and rack chassis random hardware failures

This section is related to the estimation of random hardware failures for VC-8000 backplane and rack chassis.

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;
- 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.
- 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

The Rack Chassis has been assessed since it provides two fundamental functions, the mechanical protection of the cards, not equipped with covers or enclosures by themselves, and contains the backplane rail used to connect all cards together. Through the backplane, the Trip Multiply, Inhibit, Reset, and Special Alarm Inhibit signals are provided from the RCM to each other card while they control the RCM single fault relay.

The only assumption made for the backplane is related to the redundancy of power supply tracks on the PCB that has not been considered mainly due to the negligible contribution of this redundancy in comparison to the failure rates that affect the whole backplane.

8.1.1 Failure modes

VC-8000 Backplane and rack chassis failure modes are treated in detail in the FMEDA Report, whose results are included in the Third-Party Functional Safety Assessment Report.

8.1.2 Failure modes detection by diagnostics

VC-8000 Backplane and rack chassis failure modes are either safe, in case of unintended reaching of the safe state and of maintaining of the safety functionality or dangerous, when the safety function is unintendedly bypassed or inhibited. In particular, the most dangerous modes of failures are the failure of fault transmission from the other boards in the rack to the RCM and the failure in reset command from RCM to the other boards. Those failures are not detected by the diagnostics., the resulting diagnostic coverage is 0% All failure modes are treated in detail in the FMEDA Report. For all these failure modes the system does not report the failure and the RCM fault relay is not unpowered to indicate the faulty status.

8.1.3 Failure rates and FMEDA Results

The Rack Chassis provides two fundamental functions, the mechanical protection of the cards, not equipped with covers or enclosures by themselves, and contains the backplane rail used to connect all cards together. The backplane has the main functionality to allow the communication between the cards of a rack. Through the backplane, the Trip Multiply, Inhibit, Reset, and Special Alarm Inhibit signals are provided from the RCM to each other cards and the fault signals are transmitted from any card in the rack to the RCM to trigger system fault. The only assumption made for the backplane is related to the redundancy of power supply tracks on the PCB that has not been considered mainly due to the negligible contribution of this redundancy in comparison to the failure rates that affect the whole backplane. The impact of the backplane in the reliability assessment is negligible due to the extreme simplicity of its hardware architecture. However, the assessment of the MPS-VC8000 rack shall takes into consideration also the contribution of this part. This extreme low level of complexity has been used to simplify the assessment that has been performed only for the worst-case scenario, related to the 16-slot rack.

BACKPLANE						
λS	λDU	λDD	SFF	DC	TYPE	SIL Cap.
1,61559E-08	3,58412E-09	0	81,84%	0,00%	A	2

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 in case of backplane);

SIL Capability:

SIL level that can be reached by the equipment.

The following table shows a reliability calculation example performed on VC-8000 rack and backplane. The negligible contribution, in terms of dangerous undetectable failure rates, is evident in the following calculation example.

EXAMPLE 4: Backplane (@ PTI (Proof Test Interval) = 1Year)

BACKPLANE	PDFavg	RRF
	1,5698E-05	63700,62
BACKPLANE OVERALL RESULT	**PDFavg**	**RRF**
	1,5698E-05	**63700,62**

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 rack and backplane 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.

8.2 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.

8.3 Architectural and random constraints

The whole VC-8000 MPS Machinery Protection System is suitable for SIL 1 applications in the simplex configuration described in paragraph 6.2.1 (1oo1 architecture: one input channel and one output channel) and is SIL 2 capable in redundant configuration (e.g. redundant monitors with 2 independent input channels and 2 independent output channels as reported in paragraph 6.2.2).

The safety-related parameters relevant to achieve the targeted SIL 1 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;
- Simplex (1oo1) input channel configuration (HFT=0);
- Simplex (1oo1) output channel configuration (HFT=0).
- The safety-related parameters relevant to achieve the targeted SIL 2 are:
- Average probability of dangerous Failure on Demand (PFD) < 10-2
- Low demand model of operation;
- Hardware safety integrity evaluated through Route 1H;
- Systematic safety integrity evaluated through Route 1s;
- 10 years lifetime;
- Redundant (1oo2) input channel configuration (HFT=1);
- Redundant (1oo2) output channel configuration (HFT=1).

Different configurations in terms of inputs and outputs voting logic in respect to those previously listed have to be evaluated and validated through calculations by the end-user/SIS integrator based on the specific application.

In terms of architectural constraints, the following considerations are valid for VC-8000 backplane and rack chassis:

- Backplane and rack chassis SFF < 60% being a type A element (backplane and rack chassis SFF calculated higher than 80%, suitable for SIL 2 in terms of SFF contributions);
- Backplane and rack chassis are characterized by Hardware Fault Tolerance (HFT) equal to 0 as they are not characterized by redundant architecture.

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

8.4 Common cause failures

VC-8000 backplane and rack chassis is not characterized by redundant parts or subsystems, for this reason common cause failures calculation is not applicable.

9 Backplane 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 1079330*".

IMPORTANT!
The VC-8000 Machinery Protection System rack MUST be mounted with VERTICAL ORIENTATION, to allow the effective heat dissipation and to prevent overheating, allowing airflow and heat dissipation. Being a fanless system, a different mounting would compromise the airflow for heat dissipation and would determine temperature increasing beyond environmental limits for the foreseen application, with potentially dangerous impacts on the safety functionality.

The appropriate system grounding is another crucial aspect to guarantee that the whole VC-8000 Machinery Protection System operates as expected in terms of functional safety. The proper system grounding in fact guarantees that the measurements are not affected and subsequently unreliable in respect to the physical variable measured due to the improper grounding consequences.

IMPORTANT!
The VC-8000 Machinery Protection System rack MUST be properly grounded during system commissioning phase to operate correctly. When using existing power supplies be sure to adhere to proper grounding practices, providing single point ground and avoiding ground loops. Use a 24V to 24V isolator if necessary. The system is equipped with grounding, isolation between the system and the chassis, separated but can be connected through a jumper to prevent potential differences between masses.

IMPORTANT!
The VC-8000 Machinery Protection System rack installation, mounting and commissioning shall be carried out by properly trained personnel.

During the commissioning of the VC-8000 system the followings shall be verified:

- Check the mechanical integrity of the rack in order to prove that the mechanical protection of the boards located inside is ensured;
- Check that all backplane connectors are not damaged, stable and not loose;
- Verify the proper system grounding as previously indicated;
- Verify the proper vertical mounting of the rack to allow proper heat dissipation.

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 Backplane and Rack does not have stringent proof test interval requirements, because there are no critical components subject to degradation over time. There are no critical requirements in terms of 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 of 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 1079330 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 followings are the periodic proof tests that shall be carried out on the VC-8000 Backplane and Rack according to the periodicity specified. The proof test coverage that can be obtained through the implementation of the following tests is about 100%, due to the extreme simplicity of the equipment under analysis.

10.1 Connections and terminal boards inspection

The aim of the test is to carry out a visual inspection of connectors on backplane 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

For functional safety purposes, the connectors of most interest are those where the SIL boards are connected. The loss or the loose communication between the boards and the backplane could in fact compromise the communication with the rest of the rack. Most of all reset and fault are particularly critical, their loss could have dangerous drawbacks on the safety function.

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

10.2 Backplane and rack inspection

Inspect backplane and rack connectors to ensure that no visible sign of damage and moisture are present on connectors surface. In case of any non-conformity detection, the board shall be sent for maintenance and repair. Check the mechanical integrity of the rack chassis and send it for repair in case of relevant damages detection that could compromise the mechanical protection function.

11 Maintenance, repair, de-commissioning and disposal

IMPORTANT!
The VC-8000 Machinery Protection System rack 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 1079330*".

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 t 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.

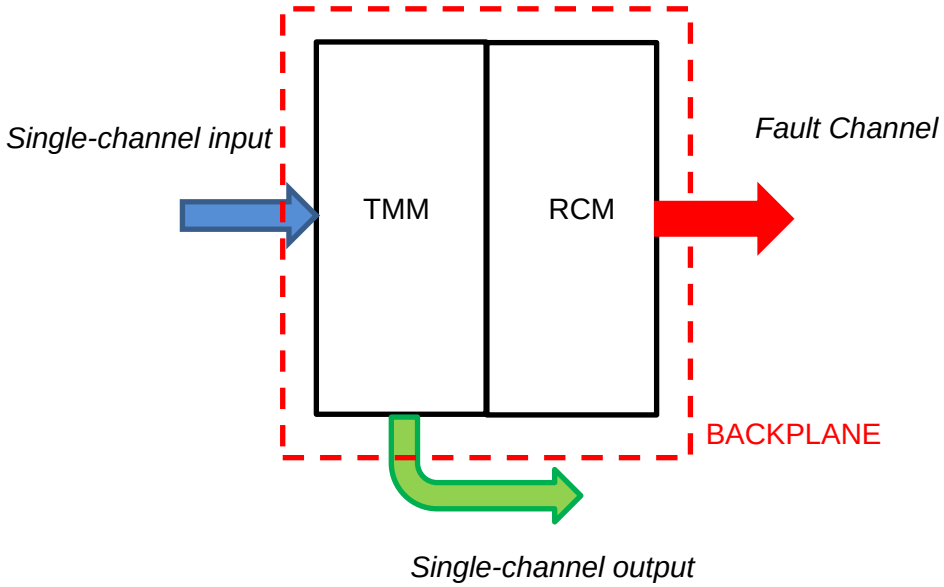
Customers and end-user are the sole responsible for the decommissioning and disposal of the product at the end of its useful lifetime. All applicable federal, state, local or international laws shall be observed. BK Vibro America Inc. has no responsibility connected with the disposal of the item at the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

ANNEX 1 Example of PFDavg calculation on the VC-8000 overall system

The following is an example of a PFDavg calculation performed on a VC-8000 system, to be integrated in the overall SIS for temperature monitoring in simplex architecture. The VC-8000 system is composed as follows:

- VC-8000 Rack Backplane;
- Rack Connection Module (RCM);
- Temperature Monitoring Module (TMM) board in simplex architecture: 1 input channel (1oo1) and 1 output channel (1oo1).

VC-8000 in this configuration can be modeled as follows. The approach in case of vibration measurements (UMM board) is the same, TMM board modeling and data shall be replaced in this case with UMM. This is only an example to show the end user how to manage the data of the whole VC-8000 system, customized configurations shall be developed and calculated by the SIS integrator depending on the specific applications (e.g. different voting logic between inputs and outputs).



The overall PFDavg of the VC-8000 system shall be calculated for this specific configuration as:

PFDavg TOT = PFDavg (TMM) + PFDavg (RCM) + PFDavg (Rack and Backplane)

The single contributions shall be evaluated according to the following criteria. The overall PFDavg of each board is calculated considering the addition of the PFDavg contributions of the board parts, according to the modeling criteria reported in the dedicated Safety Manual. The failure rates to be used for the calculation are also detailed in the board Safety Manual.

The PFDavg of the TMM board results from the contributions of the common and redundant parts:

PFDavg (TMM) = PFDavg (TMM Common) + PFDavg (TMM Input Redundant) + PFDavg (TMM Output Redundant)

The PFDavg of the RCM board consists in the sum of the common and redundant parts contributions:

PFDavg (RCM) = PFDavg (Common Part) + PFDavg (Redundant Part)

The PFDavg of the backplane and rack chassis is instead calculation considering the whole backplane as not redundant using the reliability data reported in this Safety Manual.

The overall PFDavg calculated is related to the solely VC-8000 system in this specific configuration. In order to estimate the overall PFDavg of the SIS the SIS integrator shall evaluate all others SIS contributions to realize the safety function. The SIS integrator shall reevaluate the PFDavg of VC-8000 depending on the specific configuration implemented (e.g.UMM/TMM board, voting logic between inputs and outputs etc.)

Contact

Brüel & Kjær Vibro GmbH
Leydheckerstrasse 10
64293 Darmstadt
Germany

Phone: +49 6151 428 0
Fax: +49 6151 428 1000

Brüel & Kjær Vibro A/S
Lyngby Hovedgade 94, 5 sal
2800 Lyngby
Denmark

Phone: +45 69 89 03 00
Fax: +45 69 89 03 01

BK Vibro America Inc
1100 Mark Circle
Gardnerville NV 89410
USA

Phone: +1 (775) 552 3110

Corporate E-Mail: info@bkvibro.com

Homepage: www.bkvibro.com

VC-8000 Backplane and Rack ● © Brüel & Kjaer Vibro ● 02/2022 ● C107579.002 / V02 ●