Brüel & Kjær Vibro
A member of the NSK Group

SIL Safety Manual

Setpoint Machinery Protection System

Safety Manual – Rack Connection Module (RCM)

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 Rack Connection Module (RCM)**, C107578.002 / V02, en, date of issue: 25.02.2022

Table of Contents

1 About this Safety Manual

This Safety Manual documents all the information and requirements relating to VC-8000 Machinery Protection System Rack Connection Module (RCM), 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 RCM 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). RCM (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 RCM 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
S1077785	VC-8000 Machinery Protection System Datasheet
S1078950	Rack Connection Module (RCM) 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 Rack Connection Module (RCM) description and safety-relevant functionality

The Rack Connection Module (RCM) is a functional safety relevant constituent part of the VC-8000 Machinery Protection System. One RCM module MUST be installed in every VC-8000 rack.

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 vibration and temperature.

The Rack Connection Module (RCM) accepts +24 Vdc from one or two independent power sources and distributes the power along the rack backplane where it supplies all other modules including UMMs and TMMs. When redundant power sources are used, the voltages from both are distributed on the backplane; each UMM and TMM automatically and independently selects the highest in-specification voltage. As soon as one voltage is removed or drops below the other, all modules seamlessly switch to the alternate source, assuring uninterrupted operation. RCM power inputs are protected against input polarity inversion.

RCM furthermore provides connections common to the entire rack. These include the System OK relay, a local Reset (Acknowledge) pushbutton, and terminals for wiring remote contacts that invoke the rack's Trip Multiply, Inhibit, Reset and Special Alarm Inhibit features. The reset pushbutton on RCM resets the latched statuses.

RCM supplies the connections for remote contacts for the entire rack as it acquires safety-relevant discrete inputs managing inhibit, reset, trip multiply and special alarm inhibit signals.

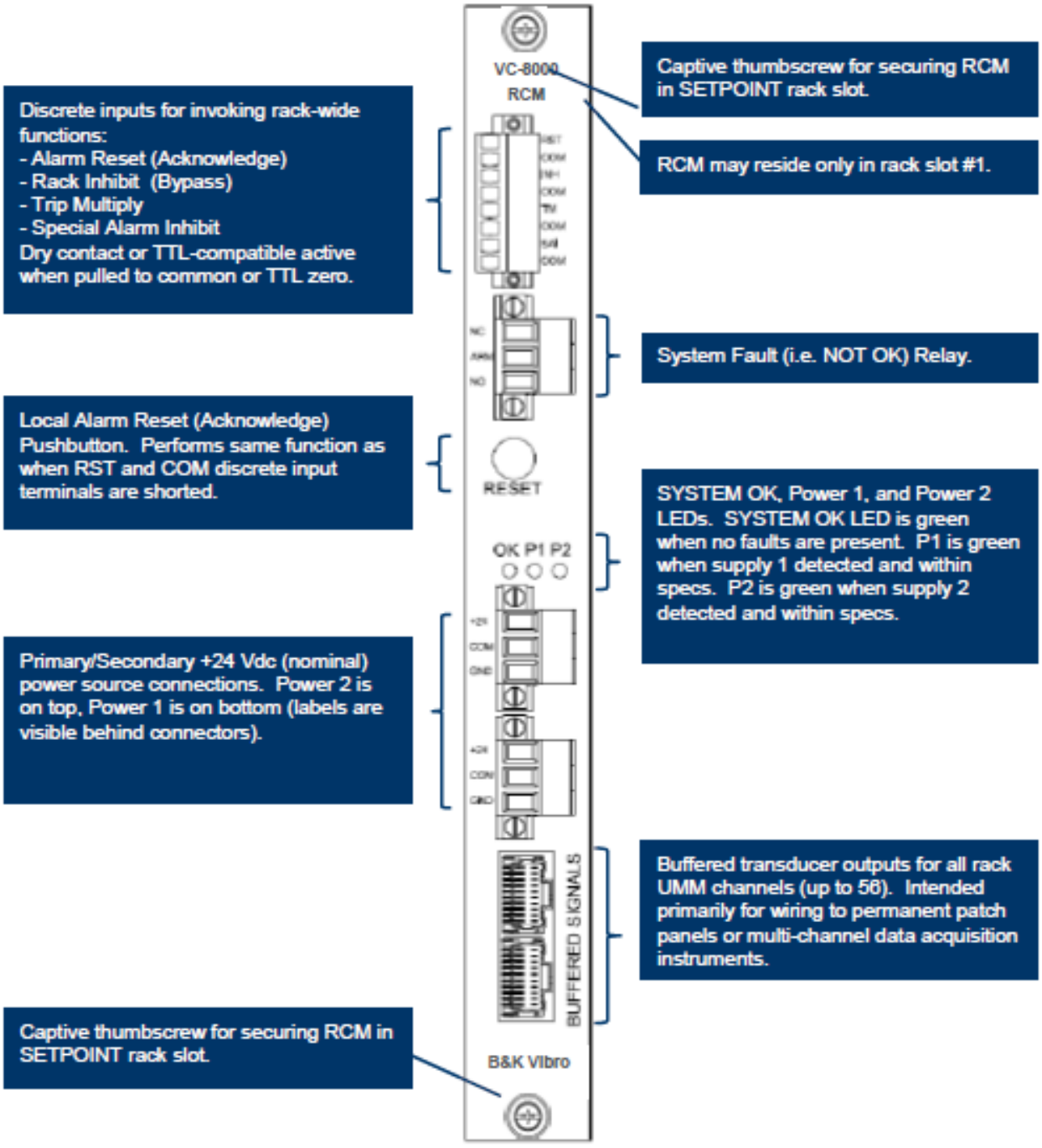
They are critical for system operation as they interfere with safety function performing, transmitted to the other boards in the rack through the backplane. As they Inhibit or bypass the safety function, these inputs are very critical for functional safety purposes, their unintended maintained activation has the potential in fact to dangerously compromise the safety functionality of the system.

RCM is also equipped with the VC-8000 rack fault relay (system NOT OK relay), important as system diagnostics as it indicates rack-wide faults. RCM board receives fault signals from any other board in the rack and in the unpowered configuration triggers system fault. Only one RCM fault relay is safety-relevant and used to indicate system faulty status, the other fault relay driven through SAM is not intended for safety applications. RCM fault relay is activated in case of faulty status of any board in the rack and is crucial for VC-8000 safety functionality.

RCM is critical for VC-8000 safety function for:

- Power supply distribution (2 independent and redundant power supply inputs);
- Transmission of inhibit, trip multiply, special alarm inhibit and reset signals from to the other boards in the rack through the backplane;
- Management of the fault status at system level through the fault relay (RCM receives fault signals due to the faulty status of any board in the rack and activates the fault relay consequently).

The following figures show RCM board and represent RCM (Rack Connection Module) layout, schematic and connections.


Captive thumbscrew for securing RCM in SETPOINT rack slot.
RCM may reside only in rack slot #1.
Discrete inputs for invoking rack-wide functions:
- Alarm Reset (Acknowledge)
- Rack Inhibit (Bypass)
- Trip Multiply
- Special Alarm Inhibit
Dry contact or TTL-compatible active when pulled to common or TTL zero.
System Fault (i.e. NOT OK) Relay.
Local Alarm Reset (Acknowledge) Pushbutton. Performs same function as when RST and COM discrete input terminals are shorted.
SYSTEM OK, Power 1, and Power 2 LEDs. SYSTEM OK LED is green when no faults are present. P1 is green when supply 1 detected and within specs. P2 is green when supply 2 detected and within specs.
Primary/Secondary +24 Vdc (nominal) power source connections. Power 2 is on top, Power 1 is on bottom (labels are visible behind connectors).
Buffered transducer outputs for all rack UMM channels (up to 56). Intended primarily for wiring to permanent patch panels or multi-channel data acquisition instruments.
Captive thumbscrew for securing RCM in SETPOINT rack slot.
VC-8000
RCM
RESET
OK P1 P2
BUFFERED SIGNALS
B&K Vibro

6.1 SIL RCM 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.

RCM SIL cards are identified as follows:

VC-8000/RCM-AA

AA=07

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

When ordering as part of a system, do not order RCM 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

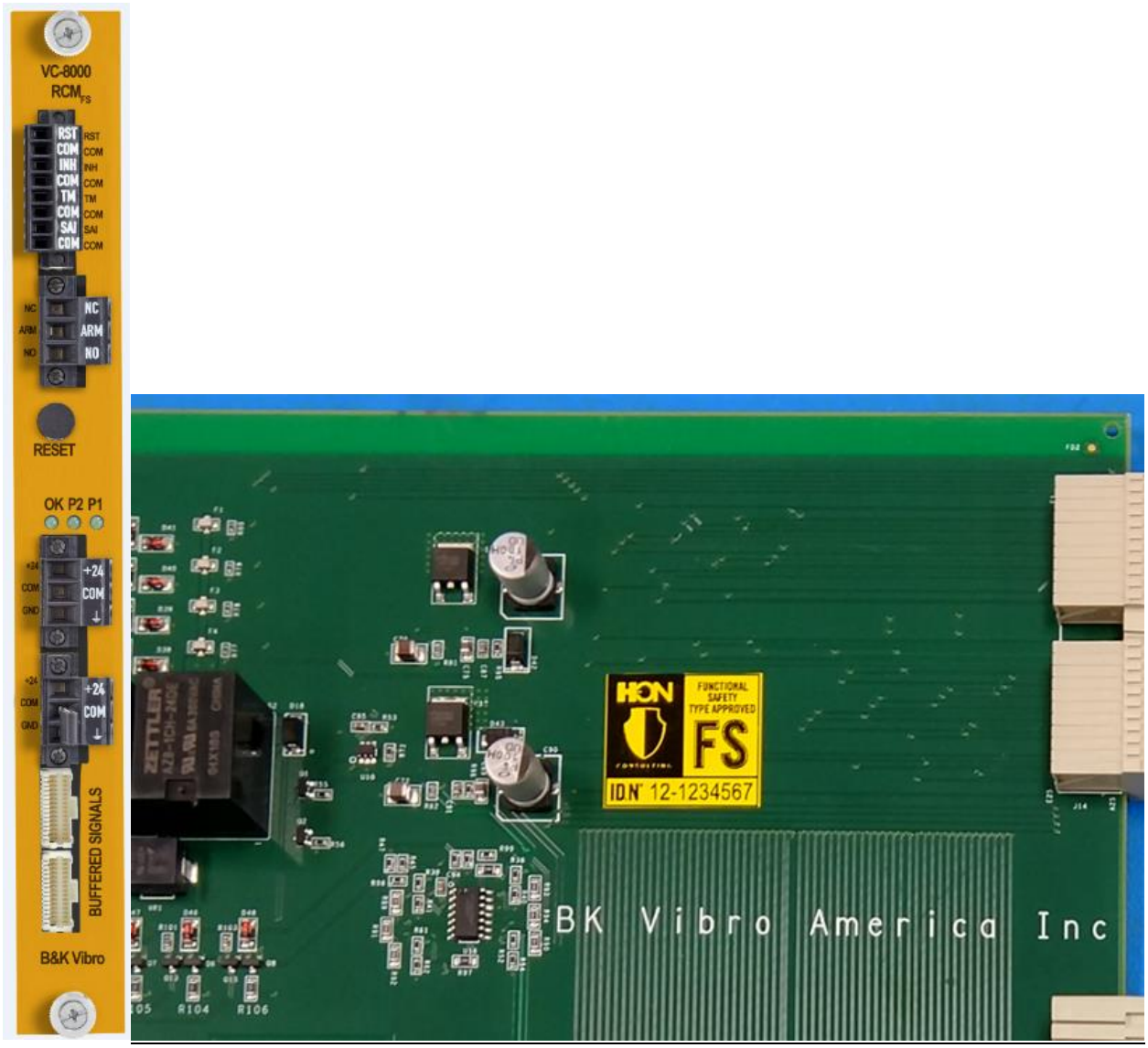
Selecting at least the followings (the other fields are selected by the end-user)

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)

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

RCM 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).


VC-8000
RCM FS
RST
COM
INH
COM
TM
COM
SAI
COM
NC
ARM
NO
RESET
OK P2 P1
+24
COM
BUFFERED SIGNALS
B&K Vibro
FUNCTIONAL SAFETY TYPE APPROVED
FS
ID.N° 12-1234567
BK Vibro America Inc

6.2 RCM Spare Parts

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

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

VC-8000/RCM-AA

AA=07

With **AA** (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 RCM hardware System installation, operation and use in safety-related applications.

7.1 RCM Hardware SIL requirements

7.1.1 RCM Discrete Inputs (TMI, SAI, RST, INH)

RCM is equipped with terminals for wiring remote contacts that invoke the rack's Trip Multiply, Inhibit, Reset and Special Alarm Inhibit features.

The Inhibit, Reset, Trip Multiply, Special Alarm Inhibit discrete inputs are allowed only through dedicated inputs from RCM for safety-related applications. The MODBUS communication of the discrete inputs to the rest of the system is inhibited.

These inputs have to be managed through discrete inputs (dry contacts) to the RCM board, working as "Closed" = "Active" (contact in closed status activates trip multiply, reset, special alarm inhibit, inhibit). Voltage inputs to these terminals are NOT allowed, these inputs have to be managed only through discrete inputs (dry contacts).

INH, TMI, SAI discrete input contacts are critical for functional safety, because their "stuck-at" failure (unintended maintained closed position) bypasses or inhibits the safety and machinery protection functionality.

7.1.2 RCM Power Supply Inputs

RCM is responsible for power supply distribution to all boards in the rack through the backplane. RCM is equipped with redundant independent power supply inputs, protected against overcurrent and reverse flow. The best solution for VC-8000 system power supply is Dedicated Power Supply, not Distributed Power Supply among the different systems.

The Power supply input voltage 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.

7.1.3 RCM Fault relay (system fault)

RCM board is equipped with two fault relays, one is used to indicate the fault status of the rack and is critical for safety applications, the other driven by SAM and is excluded from the safety critical path.

The safety critical fault relay is the rack fault, that is “activated” when any board in the rack is in a fault status.

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

- ✓ Module start up (UMM, TMM, SAM);
- ✓ SAM communication to UMM/TMM stopped;
- ✓ UMM/TMM ADC stops providing data;
- ✓ If data from the UMM/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/UMM_FS functional safety versions);
- ✓ If the -24V transducer power is out of specification (UMM_FS only functional safety version);
- ✓ Invalid Configurations (UMM/TMM);
- ✓ Invalid Personality file UMM/TMM;
- ✓ Invalid Metadata File TMM;
- ✓ SAM with mismatching or no secret inserted into rack with FS monitors;
- ✓ Any hardware failure that prevents the module from initializing/operating correctly: SAM/UMM/TMM;
- ✓ Unable to load and execute Firmware, SAM/UMM/TMM;
- ✓ 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 (e.g. vibration and monitoring on the same rack of two independent vibration control loops for NDE and DE bearings of a machine). 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 and has no issues in terms of functional safety 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 that the fault relay is common for the entire rack. 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.

7.2 Environmental and operating conditions

The RCM 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

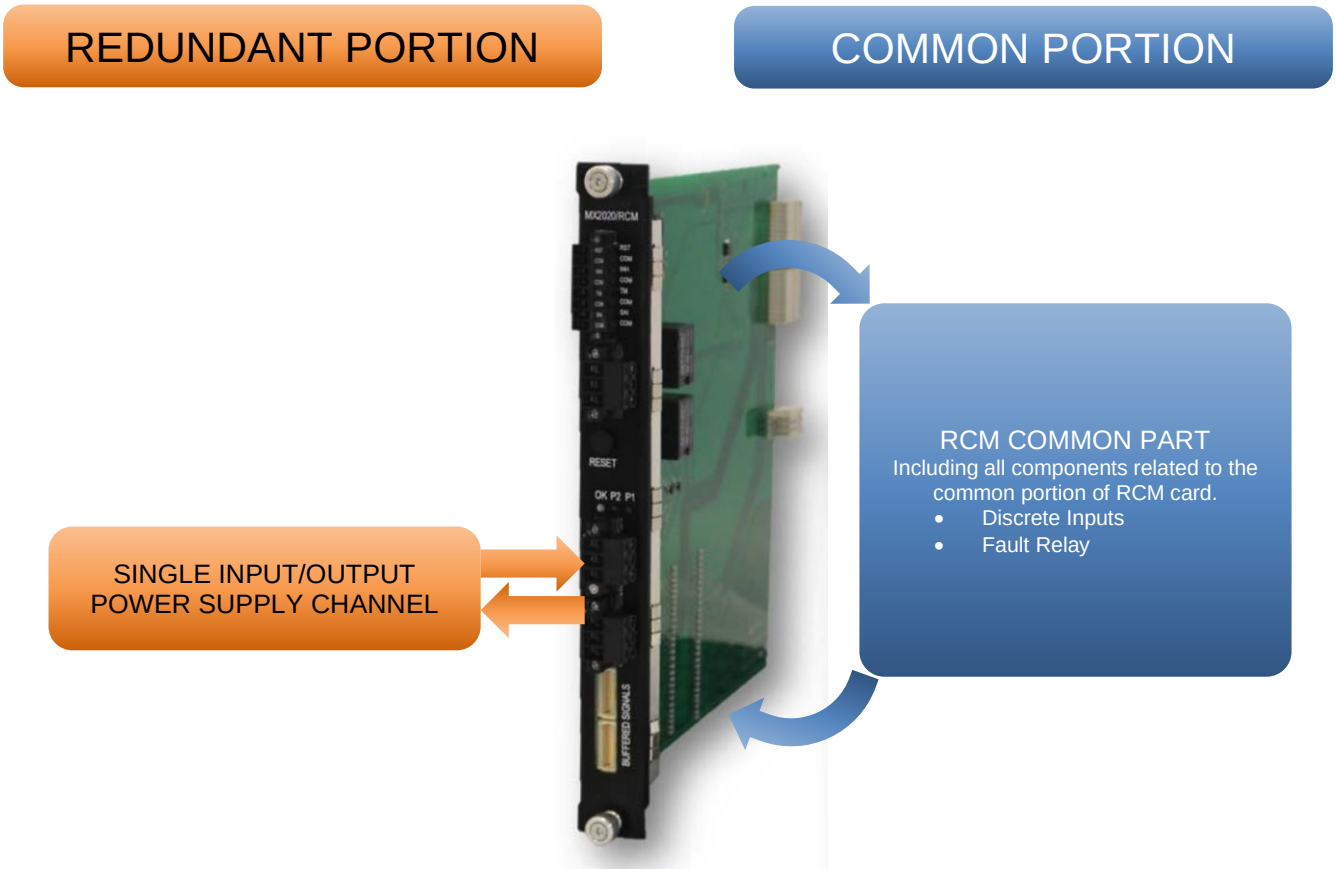
*Note 1: The continuous voltage range +22 to +30 Vdc can only be used for generic (not safety-related applications). For functional safety-related applications the admissible continuous voltage is **+23.1 to +26 Vdc.** This voltage range guarantees that all safety-related functionalities of the system 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.*

RCM is equipped with redundant and independent power supplies that transmit power supply to the whole system. 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!
RCM operation and maintenance MUST be managed by personnel having the proper training and knowledge.

8 VC-8000 RCM functional specifications

The RCM provides connections common to the entire rack. These include the System OK relay, a local Reset (Acknowledge) pushbutton, and terminals for wiring remote contacts that invoke the rack's Trip Multiply, Inhibit, Reset, and Special Alarm Inhibit features. Additionally, the RCM manages the power supply to the entire rack and provides the fault feedback that shall be used as annunciation detection of some failure modes that can affect either the whole system or a specific card. RCM card was split into common and redundant parts (according to the criteria represented in the figure below).



The RCM board is split into:

- Redundant part: consisting in the hardware components, part of the single input/output power supply channels, in redundant configuration;
- Common part: consisting in all other hardware components of RCM board that are not in redundant configuration (discrete inputs, fault relay).

The buffered signals outputs have been defined as not suitable for safety-related applications and consequently not included in the FMEDA.

The redundant channel is referred to the power supply input from the input connection located on the front side of the RCM card up to the backplane connector that provides an independent source of power supply to the entire rack.

The RCM has the main impact in the fault annunciation through a dedicated relay, and when the Trip Multiply, Inhibit, Reset, and Special Alarm Inhibit conditions shall be applied to all cards of the rack. Even if the board complexity is relatively low, these signals are critical, and their managing, in terms of diagnostic detection and redundancy, has impacted the overall board results. The power supply, modelled here to summarize the mainly impact in terms of undetectable failures, can be considered as negligible even if the power supply redundancy is not used.

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

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

8.1 RCM random hardware failures

This section is related to the random hardware failures of VC-8000 Rack Connection Module (RCM).

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

Rack Connection Module (RCM) 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 RCM failure modes, both detected and undetected by internal diagnostics are treated in detail in the FMEDA Report. For all the failure modes detected by the diagnostics the system reports the failure and the RCM fault relay is unpowered to indicate the faulty status. The failure modes that result in an unintended "activation" of the fault relay (system fault) are detected as the fault relay is the diagnostics indicator of the system. The faults that prevent fault relay activation are whereas dangerous and undetected by the internal diagnostics, as they dangerously compromise the notification of system fault. Any fault regarding RCM discrete inputs is undetectable, can be only either safe or dangerous depending on the effects on the safety function (maintained or inhibited).

8.2.2 Failure modes of the internal diagnostics

RCM fault relay that is the system diagnostics can fail in mainly two ways. All failures that determine unintended "activation" of the fault relay (the fault relay indicates system fault even if it is not present) are detected (the system fault is triggered). Whereas when the RCM fault relay does not open (e.g. welded contacts in closed position) the safety function is compromised in a dangerous way (even if a fault is present at rack level, the diagnostics is not able to trigger system fault).

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.

8.2.5 Failure rates and FMEDA Results

The RCM has the main impact in the faulty annunciation through a dedicated relay and in the acquisition of Trip Multiply, Inhibit, Reset, and Special Alarm Inhibit commands applied to all cards of the rack. Even if the board complexity is relatively low, these signals are critical, and their managing, in terms of diagnostic detection and redundancy, has impacted the overall board results. The power supply, modelled here to summarize the main impact in terms of undetectable failures, can be considered as negligible even if the power supply redundancy is not used. The following table summarized the overall RCM results:

RCM NOT REDUNDANT PART						
λS	λDU	λDD	SFF	DC	TYPE	SIL Cap.
2,28455E-07	1,62213E-07	7,95109E-08	65,50%	32,89%	A	2
REDUNDANT POWER SUPPLY CHANNEL						
λS	λDU	λDD	SFF	DC	TYPE	SIL Cap.
1,4783E-06	9E-08	0	94,26%	0,00%	A	3

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

1. RCM Not Redundant Part: all parts of RCM board circuitry apart from the redundant power supply inputs (Fault relay, discrete inputs).
2. Redundant Power Supply Channels: the TMM redundant power supply channels include the hardware circuitry of RCM power supply inputs.

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;

SIL Capability:

SIL level that can be reached by the equipment.

The whole RCM board has to be modelled in terms of reliability calculations considering always the two contributions of common and redundant parts.

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

EXAMPLE 3: Single RCM in 1oo1 configuration (@ PT (Proof Test Interval) = 1Year)

1oo1 of RCM NOT REDUNDANT PART	PDFavg	RRF
	7,1049E-04	1407,47
1oo1 of REDUNDANT POWER SUPPLY CHANNEL	PDFavg	RRF
	3,9420E-04	2536,78
RCM OVERALL RESULT	**PDFavg**	**RRF**
	1,1047E-03	**905,23**

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 RCM 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 Rack Connection Module (RCM) is suitable for SIL 2 applications, in terms of architectural constraints, because:

- RCM Not Redundant part (Type A device) is characterized by SFF of about 65%, that in 1oo1 architecture (HFT=0) is suitable for SIL 2 applications being higher than 60%;
- RCM Redundant Part (Type A device) is SIL 3 capable in terms of architectural constraints being characterized by SFF of about 90%.

As RCM module results from the combination of both common and redundant parts, the overall SIL reachable by the RCM in terms of architectural constraints is SIL 2 (limited by RCM not redundant part) and RCM is consequently SIL 2 capable.

The other safety-related parameters relevant to achieve SIL 2 (in order not to worsen architectural constraints contribution) 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;
- RCM common part characterized by Hardware Fault Tolerance (HFT) equal to 0;
- RCM redundant part (power supply inputs) is characterized by Hardware Fault Tolerance (HFT) equal to 1 if both power supply inputs are used, 0 if only one is used.

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

8.5 Common cause failures

The contribution of common cause failures is not relevant for RCM board, because the only part of the board that is in redundant configuration are the power supply inputs. RCM power supply inputs failure is mainly safe oriented, consequently dangerous failures with the potential to adversely affect the safety function due to common causes have a negligible contribution for RCM board.

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 1079330*", taking into consideration the additional RCM hardware requirements reported in paragraph 7.1.

IMPORTANT!
RCM installation, mounting and commissioning shall be carried out by properly trained personnel.

The following checks shall be carried out during RCM 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 RCM board and the populated PCB have no visible sign of damage;
- Inspect all connection/terminal boards to evaluate their integrity and to detect any broken, defective, loose etc connection;
- Ensure that the trip multiply, inhibit, special alarm inhibit and reset signals are managed as required in paragraph 7.1.1, through discrete inputs (dry contacts), no voltage inputs are allowed;
- Ensure that only the fault relay not driven by SAM is used for safety applications;
- Ensure that no visible sign of damage and moisture are present on RCM terminal boards and on the board;
- During the RCM board connection to backplane check and ensure the proper connection to ensure that it is not faulty or loose;
- During discrete inputs (mainly reset that otherwise could fail dangerously) wiring to RCM terminal board, check the proper connection of the dry contact to the board, in order to prevent any mechanical failure or improper input connection. Inspect the connector and ensure that it is not loose;
- Ensure that the fault relay output connections to the rest of the SIS are not loose;
- Verify that the fault relay is configured as Normally Energized (de-energize to trip) through Configuration Software checks, NOT OK= relay opened;
- Verify that the fault relay is activated (system fault active) at module start-up (every time the system reboots);
- Check that system configuration through MODBUS is inhibited;
- Verify that there are no unexpected events in the system events list;
- Check that the power supply is set in the admissible range for safety applications (paragraph 7.2), together with all other admissible operating conditions;

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 RCM does not have stringent proof test interval requirements, because periodical calibration on RCM 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 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 following are the periodic proof tests that shall be carried out on RCM board according to the periodicity specified. The proof test coverage that can be obtained through the implementation of the following tests is of about 95%.

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 RCM 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 mainly the reset terminal connector to ensure that it is not loose and that the reset command can be effectively transmitted to the rest of the system.

Ensure that also the output connections from the RCM fault relay to the rest of the SIS is not defective, worn, damaged or loose the ensure that the fault signal can be effectively received by RCM to activate the fault relay accordingly.

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

10.2 RCM board and populated PCB inspection

Inspect RCM board and the populated PCB to ensure that no visible sign of damage and moisture are present on RCM 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 Power supply removal test on RCM fault 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 fault relay does not de-energize. Upon disconnection of both power supply inputs whereas the fault 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 RCM fault relay contact;
- Verify that the RCM fault relay is energized evaluating ESD Simulator status;
- 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 RCM fault relay is still energized evaluating ESD Simulator status;
- 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 RCM fault relay is still energized evaluating ESD Simulator status;
- Disconnect both PWR1 and PWR2 power supply inputs to RCM;
- Verify that the RCM fault relay is de-energized evaluating ESD Simulator status;
- 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 fault relay is not de-energized. The removal of both power supply inputs shall whereas determine fault relay de-energization to announce system fault.

10.4 RCM board disconnection from the rack test

The RCM Module disconnection from VC-8000 Rack test shall be carried out to verify that in case of disconnection of the RCM Module from the Rack, RCM fault relay, is de-energized.

Test Procedure

- Connect the ESD Simulator to RCM fault relay output contact;
- Verify that the RCM fault relay is energized evaluating ESD Simulator status;
- Disconnect the RCM Module from the rack slot 1;
- Verify that the RCM fault relay is de-energized evaluating ESD Simulator status;
- Re-connect RCM Module to the rack slot 1;
- Restore the system to normal operation;
- Reset the system.

Test Results (Pass/Fail criteria)

The RCM Module disconnection from VC-8000 Rack test is passed if RCM fault relay is de-energized upon disconnection of the RCM module from the VC-8000 rack slot 1.

11 Maintenance, repair, de-commissioning and disposal

IMPORTANT!
VC-8000 RCM 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.