Functional Safety Assessment

SETPOINT™ MX2020/RCK Machinery Protection System

SETPOINT Vibration
2243 Park Place Suite A
Minden, NV 89423, USA
info@setpointvibration.com
www.setpointvibration.com

Document Number: 1354794
Revision: B (Feb 2016)

SETPOINT™

Functional Safety Assessment

SETPOINT™ MX2020/RCK Machinery Protection System

Trademarks and Copyrights

All trademarks, service marks, and/or registered trademarks used in this document belong to SETPOINT Vibration, a division of Compressor Controls Corporation, except as noted below:

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

Document Number: 1354794
Revision: B (Feb 2016)

SETPOINT™

Table of Contents

1 About this Document

This document summarizes the results of the MX2020/RCK Machine Protection System reliability assessment according to IEC 61508 for Safety Integrity Level (SIL) calculation.

The assessment was performed by SETPOINT™ Vibration (the manufacturer) via a Failure Modes, Effects and Diagnostics Analysis (FMEDA) to determine the MX2020/RCK failure modes, the effect of the failure on the machinery protection function, and the ability to detect and annunciate the failure via Fault relay contact, front panel display, or other means.

Failure rates were calculated by T-Cubed Systems, Inc. (http://www.t-cubed.com/consulting.htm), an independent third party.

2 Abbreviations and Definitions

Abbreviation	Definition
Beta	Common Cause Failure percentage
DC	Diagnostic Coverage ($\sum\lambda_{dd}$ / $\sum\lambda_{d}$)
HFT	Hardware Fault Tolerance. A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
λ_d	Total dangerous failures $\lambda_d = (\lambda_{du} + \lambda_{dd})$
λ_{du}	Probability of Dangerous Undetected Failure
λ_{dd}	Probability of Dangerous Detected Failure
λ_s	Total safe failures $\lambda_s = (\lambda_{su} + \lambda_{sd})$
λ_{su}	Probability of Safe Undetected Failure
λ_{sd}	Probability of Safe Detected Failure
FIT	Failure in Time. The number of failures per billion (10^9) hours.
PFD	Probability of Failure on Demand
PFD_{avg}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction $(\sum\lambda_s + \sum\lambda_{dd})$ / $(\sum\lambda_s + \sum\lambda_d)$

3 Analysis Results

The SETPOINT MX2020/RCK Machinery Protection System is suitable for SIL 1 and 2 applications in simplex configurations. It is suitable for SIL 1, 2, and 3 applications in redundant configurations. Table 1 on the following page summarizes each system arrangement reviewed herein and its corresponding SFF and PFD_{avg} for the MX2020/RCK alone and as part of a system (rack, sensors, and final elements) where allocations have been made for sensors and final elements. Sections 6-8 of this document provide the supporting methodology, analysis, and data used to generate Table 1.

Table 1: Summary Data for SETPOINT SIL Evaluation

Refer to Section	Redundancy Configuration				SETPOINT Calculated Values				
	Sensors[2]	Final Elements	Monitors[1]		Monitors Only (MX2020/RCK)			Full System (Monitors, Sensors, Final Elements)	
	Qty	Qty	Qty	HFT	SFF	PFD_{avg}	SIL	PFD_{avg}	SIL
8.1.5	Simplex	Simplex[4] w/ SFF = 50%	Simplex	0	95%	2.22×10^{-4}	2	3.25×10^{-3}	1
		Simplex[3] w/ SFF > 60%							2
8.1.6	Duplex (1oo2D)	Simplex[4] w/ SFF = 50%	Simplex	0	94%	2.49×10^{-4}	2	1.74×10^{-3}	1
		Simplex[3] w/ SFF > 60%							2
8.1.7	Simplex	Simplex[3] w/ SFF > 60%	Duplex (1oo2D)	1	94.8%	5.03×10^{-5}	3	3.03×10^{-3}	2
8.1.8	Triplex	Triplex	Triplex (1oo3)	1	95%	3.45×10^{-5}	3	9.49×10^{-5}	3
8.1.9	Duplex	Simplex w/ SFF > 60%	Triplex (2oo3)	1	91.8%	2.87×10^{-5}	2	1.23×10^{-3}	2
		Duplex w/ SFF > 60%		1	91.8%	2.87×10^{-5}	3	1.32×10^{-4}	3

1. All configurations assume redundant power supplies for monitors.
2. All sensors are assumed to meet SIL 2 and Type A criteria with HFT=0, MTBF > 50 yrs, and SFF > 60%.
3. These final elements are assumed to meet SIL 2 and Type A criteria with HFT=0, MTBF > 228 yrs, and sufficient diagnostic coverage for SFF > 60%.
4. These final elements are identical to note 3 above, but are assumed to have no diagnostic coverage (SFF=50%).
5. Per IEC 61508-1 Table 2 and 61508-2 Table 3; Type B Safety System; Low demand mode of operation.

SIL Criteria per IEC 61508[5]			
SIL	**HFT**	**SFF**	**PFD_{avg}**
1	0	60% < SFF < 90%	$10^{-2} \le PFD_{avg} < 10^{-1}$
2	0	SFF > 90%	$10^{-3} \le PFD_{avg} < 10^{-2}$
	1	60% < SFF < 90%	$10^{-3} \le PFD_{avg} < 10^{-2}$
3	1	SFF > 90%	$10^{-4} \le PFD_{avg} < 10^{-3}$
	2	60% < SFF < 90%	$10^{-4} \le PFD_{avg} < 10^{-3}$

4 Scope

Functional Safety includes all aspects of the safety function over the full lifecycle. These activities extend beyond any one part of the system and must be considered as a whole. For this reason, any individual part of the system may be considered as "Functional Safety Capable" and may be analyzed individually, but full functional safety certification cannot be provided unless all required activities are address per the required IEC standards.

The list below is an example of some of the components for the safety function of returning a machine to a safe state when excessive vibration is detected:

1. Monitoring System (i.e., MX2020/RCK)
2. Sensors
3. Emergency Shutdown System (ESD)
4. Final Elements
5. Installation, Commissioning, Verification
6. Operator Training and Periodic Retraining
7. Maintenance and Proof Testing
8. Modification
9. Decommissioning and Disposal

This analysis is limited to the MX2020/RCK system with allocations for the sensors and final elements. Other items above may be contracted through SETPOINT or managed by the user.

NOTE: This assessment was performed by the manufacturer, competent in the field of functional safety, and uses reliability numbers calculated by a competent third party. However, this assessment has not yet been certified by an outside agency.

The MX2020/RCK was designed by SETPOINT Vibration, comprised of individuals familiar with vibration monitoring systems and functional safety. The MX2020/RCK includes many safety improvements over previous systems including:

1. Elimination of communication networks between the alarm processing and the relay.
2. Minimization of complex microprocessor systems in the path between sensor and relay.
3. Use of windowed watch-dog timers.
4. A flexible design that allows the use of the same signal processing firmware for many measurement types without recompiling the system firmware or digital signal processing firmware.

There are many ways to organize the system in terms of redundant sensors, alarm voting, redundant relays, and layering of systems to alter the overall system probability of failure on demand and diagnostic coverage. This document discusses the MX2020/RCK's reliability and how various system architectures affect the probability of failure on demand. It provides numbers that can be used when performing total safety loop SIL calculations.

5 Reference Documentation

Table 2: Reference Documentation

Document Number	Title	Company Confidential?
1079330	SETPOINT MPS Operation and Maintenance Manual	N
1077785	DATASHEET: MPS System Overview	N
1077787	DATASHEET: Universal Monitoring Module	N
1077788	DATASHEET: Temperature Monitoring Module	N
1077786	DATASHEET: System Access Module	N
1078950	DATASHEET: Rack Connection Module	N
XXXXXXX	SETPOINT Functional Safety Management Plan	Y*
XXXXXXX	SETPOINT Safety Requirement Specification	Y*
XXXXXXX	SETPOINT Safety Impact Checklist	Y*
TQAP110	Dsgn/Development Planning, Dsgn Input, And Dsgn Output Procedure (CCC)	Y*
XXXXXXX	Product Development Processs (METRIX)	Y*
IEC 61508 Parts 1 to 7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems	N
N/A	Safety Instrumented Systems, Manual for Plant Engineering and Maintenance, GM International, 2nd Edition	N
N/A	SETPOINT System MTBF Calculations, T-Cubed Systems, June 2012	Y*

* Denotes documents that contain proprietary design and/or other details.

6 Analysis Methodology

This section includes the analysis methodology used by SETPOINT Vibration when assessing the MX2020/RCK.

6.1 Product

The SETPOINT MX2020/RCK is a machinery protection system consisting of a rack, power supply(ies), and monitoring module(s).

The Monitoring Modules:

- Provide power to sensors
- Condition sensor signals
- Extract machine measurements from the signals
- Compare measurements to configured alarm set-points
- Perform alarm status voting logic
- Drive alarm relays
- Drive Analog 4 to 20 mA outputs
- Supply data to the System Access Module for use by an external display, Modbus communication devices, configuration software, and condition monitoring software.

Figure 1 shows the functional safety scope. The functional safety path includes:

- The Rack Connection Module (Connector Card)
- The Backplane
- UMM or TMM monitor cards
- Sensors
- Final Elements

Specifically excluded from the safety path:

- System Monitor card
- Configuration computer and software
- Condition monitoring computer and software
- Computer display
- Digital communications (e.g., Modbus) with external control/automation systems
- Buffered outputs (used for connection to external calibration, diagnostic, and other instruments)

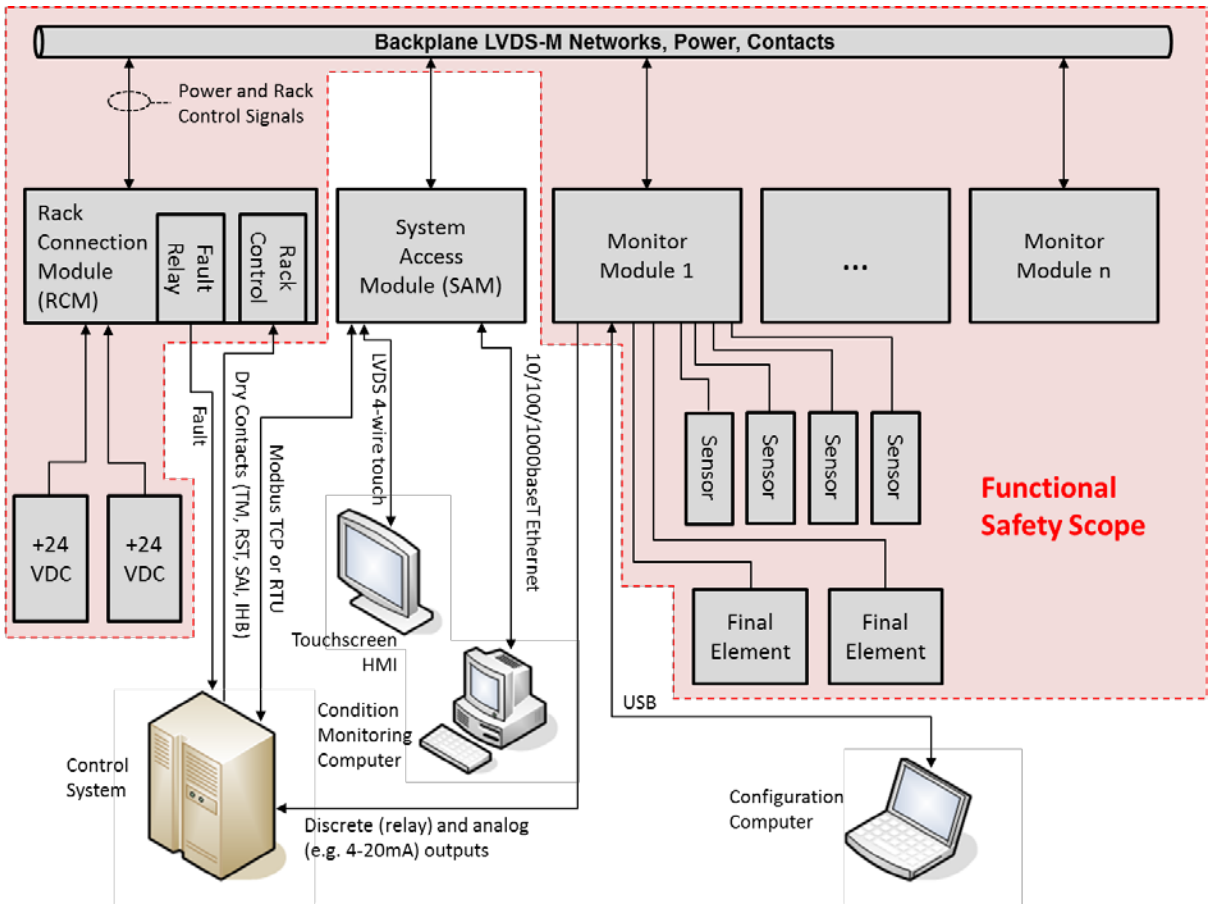

Figure 1: Functional Safety Scope

6.2 Operating Modes

The SETPOINT MPS has several modes of operation. The safety function is only valid in Normal Operation Mode. When operating in a mode other than Normal Operation, the user must provide a means of annunciation.

6.2.1 Normal Operation

In normal operation the SETPOINT system conditions the sensor input signals, filters and extracts the machine related measurements, compares the measured parameters to user configured alarm set-points, performs alarm voting, and activates relays based on the voting. The machine is protected in this mode. The Fault relay is in the OK state during Normal Operation mode.

6.2.2 Boot Up

Upon applying power, the monitors will boot up. The boot up cycle last approximately 60 seconds. During this time the monitor is not protecting the machine. The Fault relay is in the Not-OK state during Boot Up.

6.2.3 Timed Fault Defeat

After boot up, if the Timed Fault Defeat option is enabled, the monitor will incur a delay (the Fault Defeat Time) to allow the peak detectors to discharge after the jump in transducer output caused by power up. The Timed Fault Defeat cycle also occurs after SETPOINT detects a transducer fault. Alarming is inhibited and machinery protection is not enabled when SETPOINT is in Timed Fault Defeat. The Fault relay is in the Not-OK state during Timed Fault Defeat.

6.2.4 Inhibit and Bypass

Inhibit prevents alarm annunciation on the inhibited modules, channels, or relays. Bypass drives values to the clamp values and thereby also inhibits alarms but also inhibits data value changes on the Analog 4-20 outputs and Industrial Communication Link. The machine is not protected by Inhibited or Bypassed components.

6.2.5 Trip Multiply

Trip Multiply temporarily increases the alarm set-points on vibration channels by a configured multiplier (e.g. 2X or 3X). Trip Multiply is typically used to allow the machine to pass through a critical region during start-up or coast-down without alarming. The safety function is altered during Trip Multiply.

6.2.6 Configuration Mode

The monitor is processing a new configuration. This occurs after a configuration has been downloaded from the software. The level of loss of protection is a function of what objects in the configuration have changed. Some changes result in a monitor reboot. The Fault relay is in the Not-OK state when a module is reconfiguring.

6.3 Safety Information

6.3.1 Type

MX2020 is a Type B subsystem.

6.3.2 Demand Mode

MX2020 operates in Low Demand Mode. Low demand mode, as defined in 3.5.16 of IEC 61508-4, is where the frequency of demands for operation made on a safety-related system is no greater than one per year.

6.3.3 Safe State

The tripped state is considered the safe state. The system transitions to the safe state after the alarm delay. The alarm delay is user-configurable, but cannot be set less than 100ms (i.e., the fastest the system can achieve the safe state after detecting an alarm is 100ms).

6.3.4 Software/Hardware Interactions

The rack configuration must be downloaded to the rack as a whole. Individual monitors cannot be configured and hot inserted for the purpose of the functional safety analysis of multi-monitor systems.

6.3.5 Safety Allocation

Table 3 summarizes the probability of failure on demand allocation for the safety system as derived from Table 2 in IEC61508-1, Low demand mode of operation.

Table 3: Probability of Failure on Demand

SIL Level	System Average Probability of Failure on Demand	FITs
3	$\geq 10^{-4}$ to $< 10^{-3}$	≥ 100 to < 1000
2	$\geq 10^{-3}$ to $< 10^{-2}$	≥ 1000 to < 10000
1	$\geq 10^{-2}$ to $< 10^{-1}$	≥ 10000 to < 100000

6.3.6 Hardware Fault Tolerance

Per IEC 61508-2 Table 3, Type B Safety System, MX2020/RCK is suitable for use in the following SIL applications when applied according to Table 4 below.

Table 4: SIL Level and Hardware Fault Tolerance (HFT)

SIL Level	Monitor Redundancy	HFT	Safe Failure Fraction (SFF)
1	Simplex (1oo1)	0	60% < SFF < 90%
2	Simplex (1oo1)	0	SFF > 90%
2	Dual Redundant (1oo2)	1	60% < SFF < 90%
3	Dual Redundant (1oo2)	1	SFF > 90%
3	Triple Redundant (2oo3)	2	60% < SFF < 90%

6.3.7 Proof Testing

Proof Test Interval: 1 Year (8760 hours)

Proof testing the monitoring system will include, as a minimum:

1. Alarm verification for each channel type according manual 1079330, SETPOINT MPS OPERATION AND MAINTENANCE.
2. Verification of the alarm relay contacts.
3. Verification of the Fault relay and annunciation system.
4. Verification that both redundant power supplies are showing OK.

Proof testing must be performed by authorized, trained personnel.

Proof testing equipment calibration certificates must be valid.

6.3.8 Mean Time to Restoration (MTTR)

System restoration including module installation, configuration, and test is less than 8 hours. This assumes that spare modules are available on-site for replacement.

6.3.9 Environment

All system components must be maintained within their environmental specifications during all lifecycle phases. Refer to the datasheets for environmental specifications.

At temperatures outside the operating specifications, the system microprocessors will halt causing a watchdog reset. A processor reset will cause de-energize to trip relays to activate causing the machine to transition to the safe state.

Further protection against temperature excursions can use the Temperature Monitor Module (TMM) to measure and alarm on excessive temperature in the system enclosure.

6.3.10 Electromagnetic Immunity

The SETPOINT MPS system meets or exceeds CE mark EMI directives (refer to datasheet 1077785) when installed per manual 1079330. Certificates are available on-line at www.setpointvibration.com.

6.3.11 LEDs and Front Panel Indicators

Although some faults such as stuck Inhibit, Trip Multiply, and modules left in Bypass are indicated on the system LEDs or front panel, it is *not* assumed that these are acknowledged by the user in a timely manner. These faults are assumed to be detected at the proof test interval.

6.3.12 Configuration

Configuration is only performed by skilled operators.

OK limits must be configured. Some failure detection depends on the monitor checking the transducer OK limits. Each monitor must have one or more channels with active OK limits.

The SETPOINT MPS Setup and Maintenance software are not considered part of the safety path. Upon commissioning, all configured scale factors and alarms are loop tested thereby verifying correct system configuration.

6.3.13 Acceptance Testing

The system is acceptance tested at commissioning to verify correct configuration and wiring by appropriately trained personnel.

7 Analysis Data

This section includes a discussion of service hours, field return data, and reliability numbers calculated for each module.

The reliability numbers presented are based on the MTBF calculation performed T-Cubed Systems, June 2012. Rack temperature 35°C, 90% Confidence Level.

7.1 Service Hours and MTBF by Module

The Service hours were determined for units shipped between July 2011 and January 2014.

Units in service for less than 1 year were omitted per IEC 61508-2.

It was assumed that the units were not placed into service for 3 months after shipment.

Table 5: Service Hours and Calculated MTBF by Module

Module	Service Hours	Calculated MTBF per Telcordia SR-332, Issue 2
RCM	>3.2 x 10^6 Hours	3.16 x 10^6 Hours
Backplane	>3.2 x 10^6 Hours	5.75 x 10^6 Hours
Universal Monitoring Module (UMM)	>11 x 10^6 Hours	6.03 x 10^5 Hours
Temperature Monitoring Module (TMM)	>1.8 x 10^6 Hours	1.27 x 10^6 Hours

7.2 Reliability by Module

7.2.1 Power Supply

The SETPOINT standard power supply (part number 100411SP) has a rated MTBF of 900,000 hours. Per annex B.1 of 61508-6, when the relays are configured for de-energize to trip and loss of power causes a trip to a safe state, the power supplies are omitted from the calculation.

The status of each SETPOINT power supply is available via Modbus from the SETPOINT System Access Module (SAM) or from relay contacts on the power supply. Using the Modbus status is advantageous in that it also detects wiring faults or internal rack faults that open the SETPOINT internal safety fuse.

When the relays are configured for normally energized (de-energize to trip), monitoring the power supplies does not improve the PFD numbers as loss of power causes a trip to the safe state, but does decrease the likelihood of a nuisance trip and therefore is highly recommended.

Loss of power will cause the system Fault relay to transition to the faulted (not OK) state.

7.2.2 RCM

As of 9 Feb 2015, there were no known RCM field failures returned with failed components. All units sent back were returned to the customer without requiring repair. Using field data, the FITs would be 0. For the purpose of this analysis we will use the calculated MTBF.

Table 6: RCM Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	29.8
Fail Dangerous Undetected (λ_{du})	4.2
Fail Safe Detected (λ_{sd})	147
Fail Safe Undetected (λ_{du})	145

Table 7: RCM Safety Reliability Numbers

Reliability Calculated Values	
Total Safety Related Failure Rate	316 FITs
MTBF	360.7 Years
Diagnostic Coverage ($\sum\lambda_{dd}$ / $\sum\lambda_{d}$)	69%
Safe Failure Fraction (SFF) ($\sum\lambda_{s}$ + $\sum\lambda_{dd}$) / ($\sum\lambda_{s}$ + $\sum\lambda_{d}$)	97%

Comment: RCM dangerous faults are caused by stuck Trip Multiply and Inhibit states. If the Trip Multiply function is not used (Multiplier set to 1 in the UMMs) then the Trip Multiplier faults do not apply.

7.2.3 Backplane

There are no electronic components on the backplane that affect the safety function. The portion of the backplane failure rate is included in the analysis for each module. The diagnostic coverage for each pin, the number of pins used, and whether a pin fault is safe or dangerous depends on the module type.

Table 8: Backplane Reliability Numbers

Reliability Calculated Values	
Total Safety Related Failure Rate	112 FITs
MTBF	657 Years

7.2.4 UMM

As of 9 Feb 2015, there were no UMM field failures found that were not detected and resolved at commissioning. The calculated reliability numbers are based on the FMEDA and MTBF numbers for a signal path from one sensor through to one relay and exclude non-safety path components used for analog outputs and communication to the software.

Table 9: UMM Common Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	391
Fail Dangerous Undetected (λ_{du})	54
Fail Safe Detected (λ_{sd})	113
Fail Safe Undetected (λ_{du})	120
Total Safe Failures (λ_s)	233
Total Dangerous Failures (λ_d)	445

Table 10: UMM Signal Process Path Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	51
Fail Dangerous Undetected (λ_{du})	6.2
Fail Safe Detected (λ_{sd})	11
Fail Safe Undetected (λ_{du})	15.5
Total Safe Failures (λ_s)	26.5
Total Dangerous Failures (λ_d)	57.2

Table 11: UMM Relay Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	0
Fail Dangerous Undetected (λ_{du})	13.3
Fail Safe Detected (λ_{sd})	3.9
Fail Safe Undetected (λ_{du})	10.4
Total Safe Failures (λ_s)	14.3
Total Dangerous Failures (λ_d)	13.3

Table 12: UMM Common Safety Reliability Numbers (one signal path, one relay)

Reliability Calculated Values	
Total Safety Related Failure Rate	678 FITs
MTBF	168 Years
Diagnostic Coverage ($\sum\lambda_{dd}$ / $\sum\lambda_{d}$)	88%
Safe Failure Fraction (SFF) ($\sum\lambda_{s}+\sum\lambda_{dd}$) / ($\sum\lambda_{s}+\sum\lambda_{d}$)	92%

Table 13 below summarizes the various UMM block failure rates. The total sums up to the FIT rate and MTBF calculated by T-cubed.

Table 13: UMM Reliability Number Summary

Reliability Calculated Values		**Comment**
UMM Common Failure Rate	678 FITs	Always included
3 Additional Signal Paths	251 FITs	Include when using multiple channels
3 Additional Relays	84 FITs	Include when using multiple relays
Phase Trigger Path Failure Rate	63 FITs	Include if alarming on speed or vectors.
Indicators Failure Rate	67 FITs	Not used for safety
Buffered output Failure Rate	248 FITs	Not used for safety
Other Non-safety related failure rate	266 FITs	Output recorders, CMS components, and configuration port.
Total UMM Failure Rate	**1657 FITs**	**Per T-cubed MTBF analysis**
Total UMM MTBF	**68.9 years**	**Per T-cubed MTBF analysis**

7.2.5 TMM

As of 16 Feb 2016, there were only 2 TMM field failures found that were not detected and resolved at commissioning. The calculated reliability numbers are based on the FMEDA and MTBF numbers for a signal path from one sensor through to one relay and exclude non-safety path components used for analog outputs and communication to the software.

During the evaluation it was determined that addition of a firmware diagnostic check could significantly improve detecting dangerous faults. The tables below show the numbers with firmware older than revision 4.01 without the additional check and for firmware revision 4.01 or newer with the additional check.

Table 14: TMM Common Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	271 (firmware older than 4.01) 366 (firmware 4.01 or newer)
Fail Dangerous Undetected (λ_{du})	158 (firmware older than 4.01) 63 (firmware 4.01 or newer)
Fail Safe Detected (λ_{sd})	100
Fail Safe Undetected (λ_{du})	134
Total Safe Failures (λ_s)	234
Total Dangerous Failures (λ_d)	429

Table 15: TMM Signal Process Path Reliability Numbers (less common components) per channel

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	11.7
Fail Dangerous Undetected (λ_{du})	7.9
Fail Safe Detected (λ_{sd})	2.9
Fail Safe Undetected (λ_{du})	0.9
Total Safe Failures (λ_s)	3.8
Total Dangerous Failures (λ_d)	19.6

Table 16: TMM Relay Reliability Numbers

Category	FITs (Failures per 10^9 hours) using calculated MTBF
Fail Dangerous Detected (λ_{dd})	0
Fail Dangerous Undetected (λ_{du})	15.7
Fail Safe Detected (λ_{sd})	3.9
Fail Safe Undetected (λ_{du})	10.4
Total Safe Failures (λ_s)	14.3
Total Dangerous Failures (λ_d)	15.7

Table 17: TMM Common Safety Reliability Numbers (one signal path, one relay)

Reliability Calculated Values	
Total Safety Related Failure Rate	662 FITs
MTBF	172 Years
Diagnostic Coverage ($\sum\lambda_{dd}$ / $\sum\lambda_d$)	63% (firmware older than 4.01) 85% (firmware 4.01 or newer)
Safe Failure Fraction (SFF) ($\sum\lambda_s + \sum\lambda_{dd}$) / ($\sum\lambda_s + \sum\lambda_d$)	76% (firmware older than 4.01) 90% (firmware 4.01 or newer)

8 System Arrangements and Associated SIL

There are various methods for redundancy within the SETPOINT MPS system. This section discusses the various arrangements and the impact on probability of failure on demand. All architectures assume redundant input power. The PFD and SFF numbers shown used the UMM calculations. The TMM numbers (using FW revision 4.01 or newer) are better than the UMM numbers but not by a significant amount so are not shown. The TMM cannot be used with paralleled sensors.

8.1.1 Fault Relay Annunication

The SETPOINT Diagnostic Coverage relies on the Fault relay being wired to an annunciator and acknowledged in a timely manner. All architectures assume the Fault relay state is annunciated.

8.1.2 Normally Energized vs. De-Energized Relays

According to IEC 61508 when relays are normally energized (de-energize to trip) the power supplies do not need to be included in the SIL calculation since loss of power causes a trip to the safe state.

When using normally de-energized relays (energize to trip), the power supplies must be included in the calculation because loss of power is a dangerous failure. With a single simplex power supply, loss of power will activate the Fault relay making it detectable if the rack Fault relay is annunciated. A better solution is to use redundant power supplies and to annunciate loss of each power supply. Power supply status is available via Modbus or from relay contacts on the power supply units.

8.1.3 Transducers

Transducers are assumed to be type A simple safety related subsystems and to have an MTBF > 50 years (< 2200 FITs). Greater than 60% of the faults cause the sensor to transition to outside the configured OK limits resulting in detection by the SETPOINT UMM. It is assumed that all sensor components are dedicated to the measurement and that the sensor does not contain other unrelated measurements or configuration circuitry. 50% of faults are assumed dangerous, causing the sensor to read low and miss a machine malfunction. 50% of faults are assumed safe, increasing the measurement in the direction towards trip to the safe condition.

The TMM must be used with RTDs or isolated tip thermocouples. The grounded tip thermocouple option causes the TMM to turn off bias currents required for detecting transducer faults.

Per IEC 61508-2 Table 2, a type A safety-related subsystem with safe failure fraction > 60% is suitable for use in SIL 1 or SIL 2 applications with simplex sensors (HFT= 0).

8.1.4 Final Elements

The final elements are assumed to be type A simple safety related subsystems and have an MTBF > 228 years (<500 FITs) and that 50% of the faults cause the element to fail to activate (dangerous) and 50% cause the element to activate prematurely (safe).

8.1.5 Simplex (1oo1)

A Simplex system has one sensor passing through one monitor that is driving the output relay to the final element. Other than the redundant input power, no blocks are redundant.

- Normally Energized Relays
- No feedback on Relay or Final Element

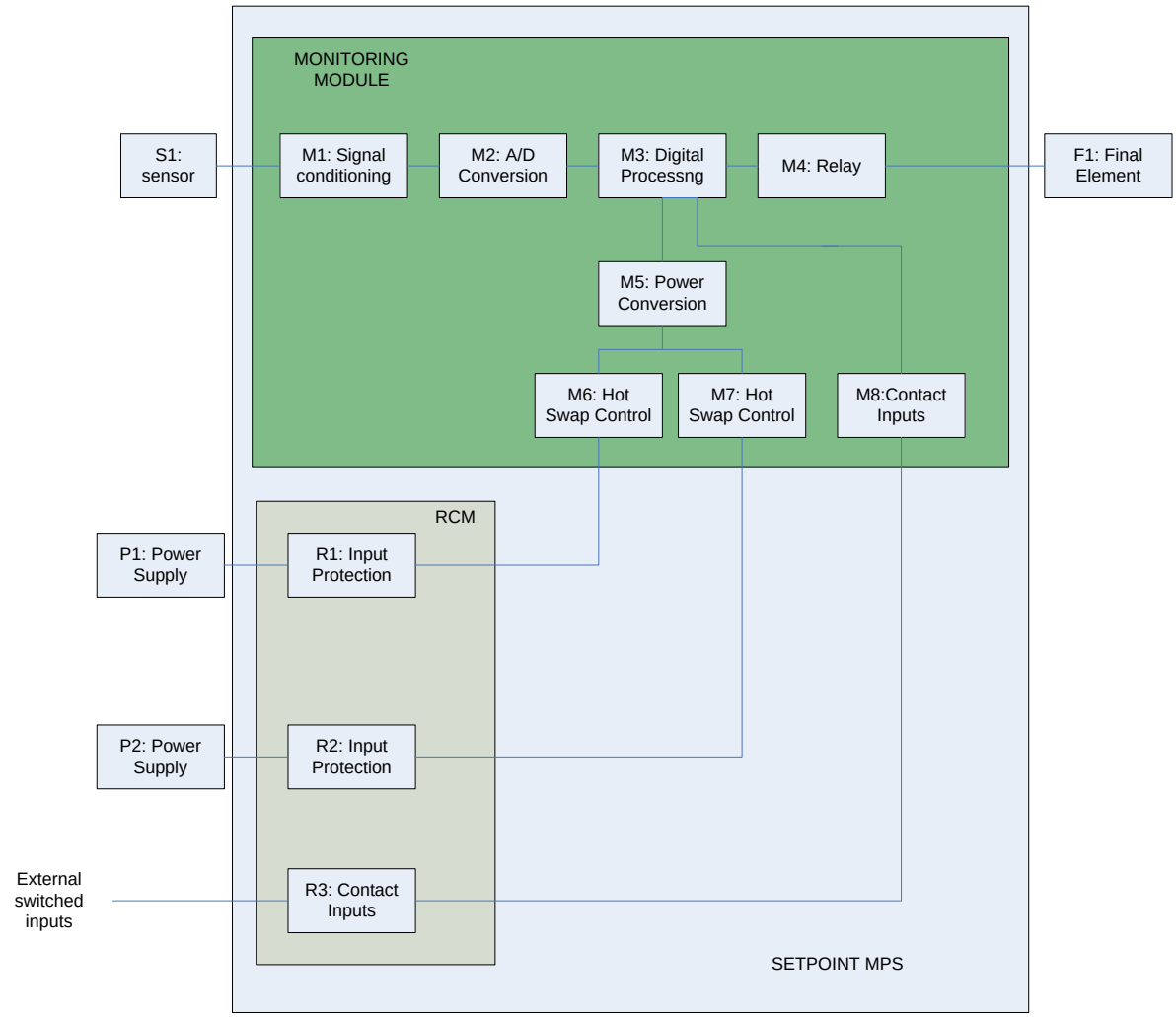

Figure 2: 1oo1 Simplex System

SETPOINT PFD_{avg}: 2.22×10^{-4} SFF = 95% **Meets SIL 1 and SIL 2 requirements**

System: **Meets SIL 1 and SIL 2 requirements**

$PFD_{avg=}$ 3.25×10^{-3}

Since the SETPOINT SFF > 90% and PFD_{avg} meets SIL 2, and the sensors and final elements are type A devices (HFT = 0) and meet SIL 2, the system meets SIL 2 requirements as long as the final element has SFF > 60%.

8.1.6 Redundant Sensors (1oo2D), One Monitoring Module

This architecture uses two sensors connected to the same monitoring module voted using one-out-of-two dependent voting logic. Dependent voting logic removes detected failed channels from voting logic allowing the remaining channel to determine whether to trip. Since X and Y probes are installed on the same bearing, the two probes when cross-voted in a dependent manner (also called Normal And) fall under this scenario. This scenario also applies to dual axial position probes.

NOTE: Since Axial Position channels alarm on a fault condition, failure of one sensor causes the alarming to depend on the remaining sensor so AND voting two Axial Position alarms results in 1oo2D voting.

NOTE: Since true 2oo2 voting requires both sensors to be valid and in alarm to trip, true 2oo2 voting worsens the PFD value and is not discussed in this document.

The sensors are separate and can be repaired individually and so are combined using the 1oo2D equations in IEC 61508. The signal paths are on the same board, have high common cause beta and so are not just summed into the reliability of the monitoring module.

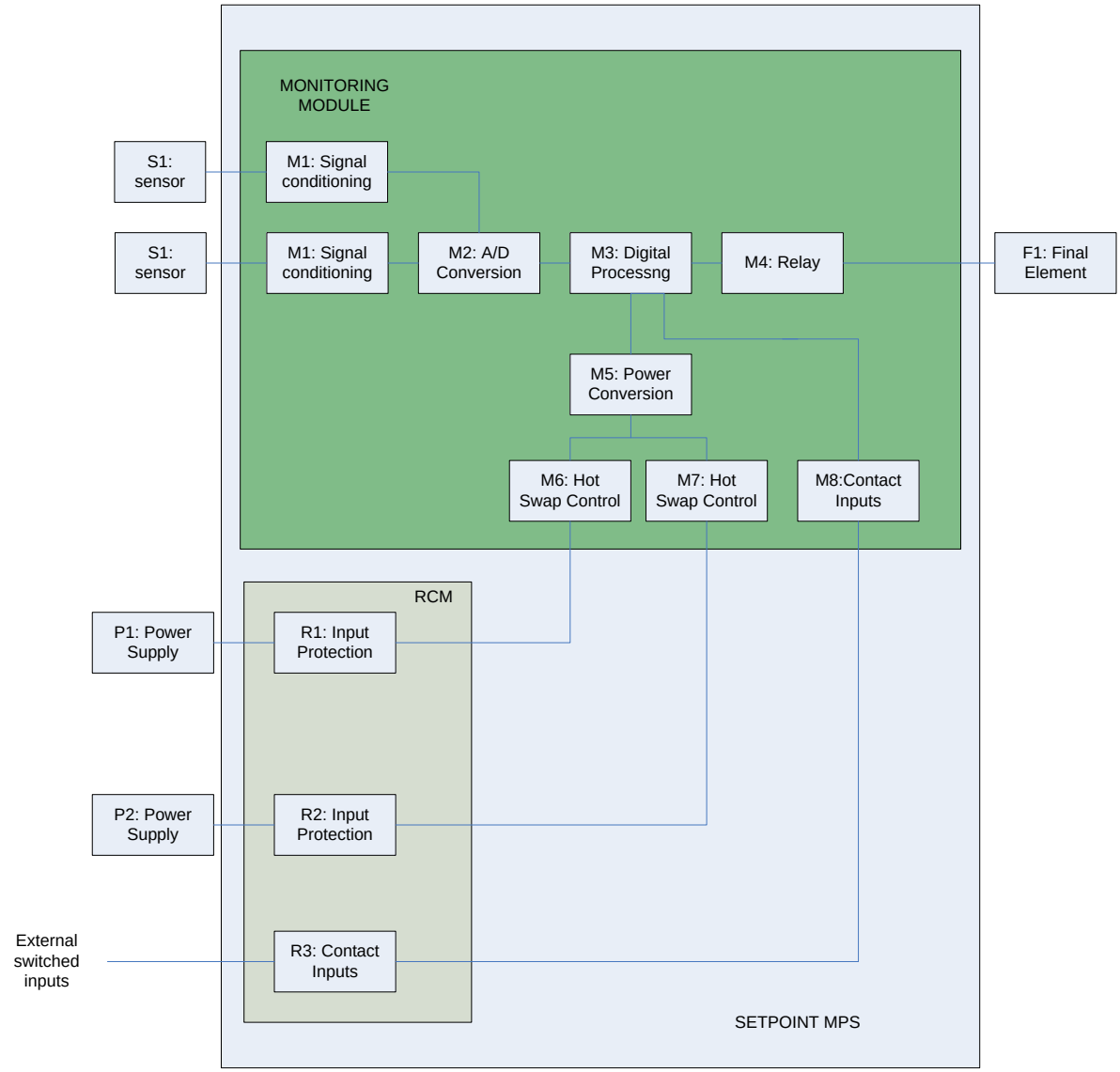

Figure 3: 1oo2D Redundant Sensor System

SETPOINT PFD_{avg}: 2.49×10^{-4} SFF = 94.0% **Meets SIL 1 and SIL 2 requirements**

System: **Meets SIL 1 and SIL 2 requirements**
$PFD_{avg=}$ 1.74×10^{-3}

Since the SETPOINT SFF > 90% and PFD_{avg} meets SIL 2, and the sensors and final elements are type A devices (HFT = 0) and meet SIL 2, the system meets SIL 2 requirements as long as the final element has SFF > 60%.

8.1.7 Simplex Sensor, Redundant Monitoring Modules

It is often not practical to install multiple sensors. The SETPOINT system supports connecting sensors between multiple monitoring modules without requiring additional hardware.

In this case each monitoring module evaluates the input sensor signal to the alarm settings and drives its own relay on alarm. The relays are wired in an OR configuration such that either can drive the final element.

Given that the sensor and final element are simple type A safety-related subsystems, per IEC61508 these elements can be used in a SIL 2 application with HFT of 0 as long as the safe failure fraction exceeds 60%.

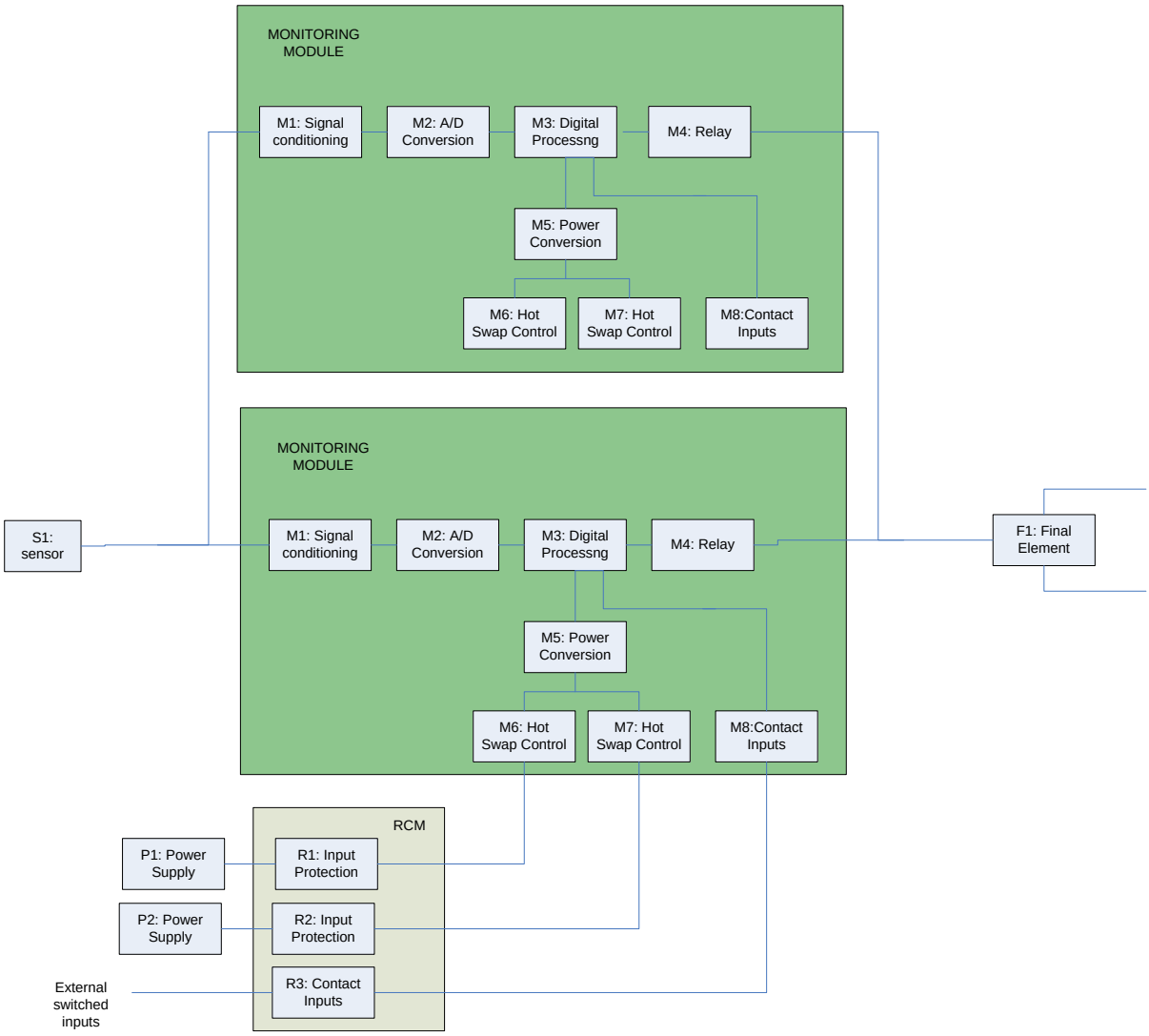

Figure 4: Simplex Sensor, Redundant Monitor System

SETPOINT

PFD_{avg}: 5.1×10^{-5} **Meets SIL 1,2 and SIL 3 requirements**
SFF = 94.8%
HFT = 1

System: **Meets SIL 1 and SIL 2 requirements**
$PFD_{avg=}$ 3.03×10^{-3}

NOTE: Because of SETPOINT's higher diagnostic coverage vs. the sensor, redundant sensors result in a larger decrease in PFD_{avg} than redundant UMMs.

8.1.8 1oo3 Redundant

The one-out-of-three redundant system uses three sensors, three modules and three final elements. Any one of the three systems can perform the safety function. The calculations assume there is no external device monitoring the three modules to remove an errant module from the voting.

The RCM and Backplane remain common but these modules have very few components and do not contribute significantly to the probability of failure on demand. The resulting system is suitable for use up to SIL 3.

Figure 5 shows the block diagram for a 1oo3 redundant system.

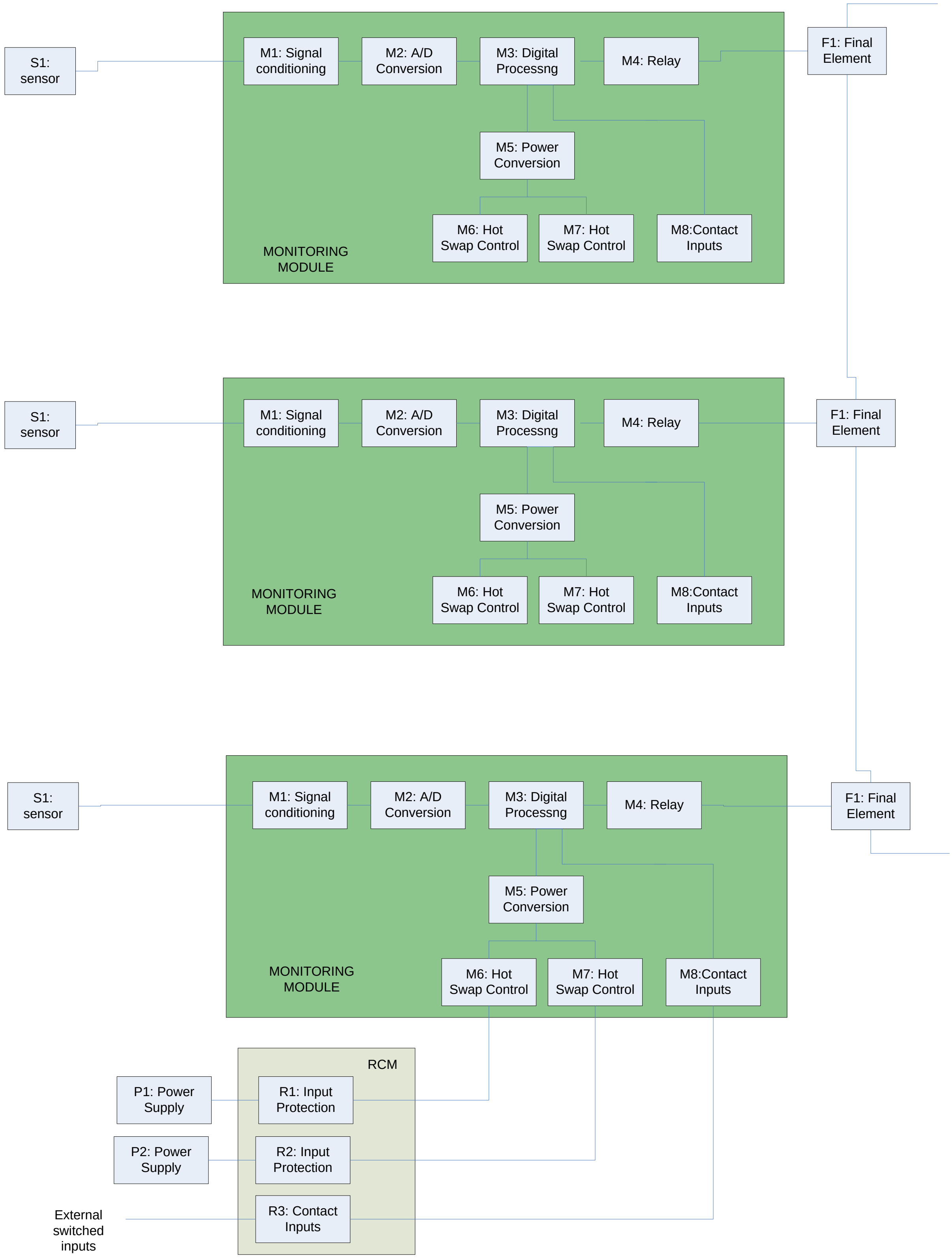

Figure 5: 1oo3 Fully Redundant System

SETPOINT

PFD_{avg}: 3.44 x 10^{-5} **Meets SIL 1,2 and SIL 3 requirements**
SFF = 92%
HFT = 1

System: **Meets SIL 1,2 and SIL 3 requirements**
$PFD_{avg=}$ 9.49 x 10^{-5}

8.1.9 2oo3 Redundant

This scenario uses two sensors (typically X-Y Radial Vibration probes or dual thrust position probes) connected to three UMMs. Internal to each UMM, the two sensors are voted in a 1oo2D method such that a failure on one sensor reverts the system to 1oo1 voting on the remaining good sensor.

The three UMMs use 3 SETPOINT MPS internal voting lines to vote the modules in a 2oo3 arrangement as shown in Figure 6.

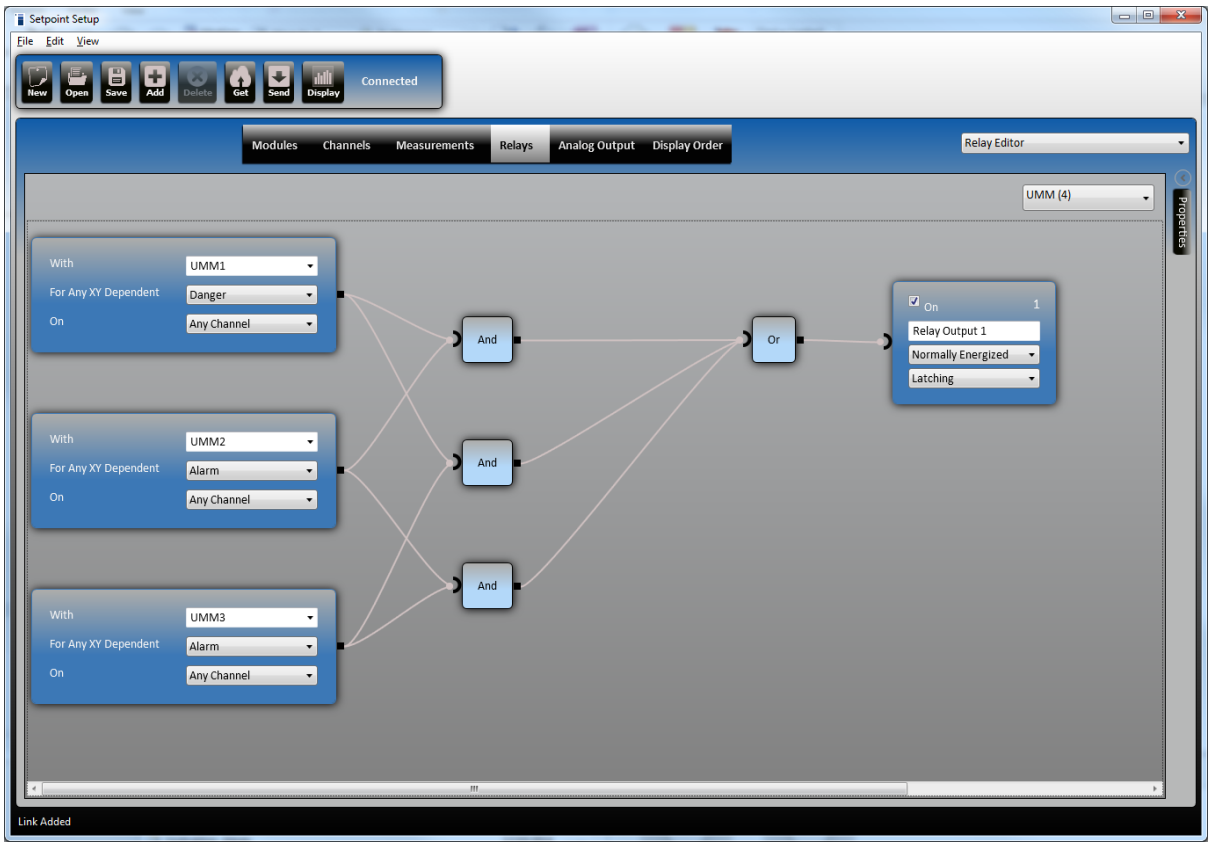

Figure 6: 2oo3 Alarm Voting

Note: Since Axial Position channels alarm on a fault condition, failure of one sensor causes the alarming to depend on the remaining sensor so AND voting two Axial Position alarms results in 1oo2D voting.

Each UMM drives two relays that are wired using 2oo3 as shown in Figure 7.

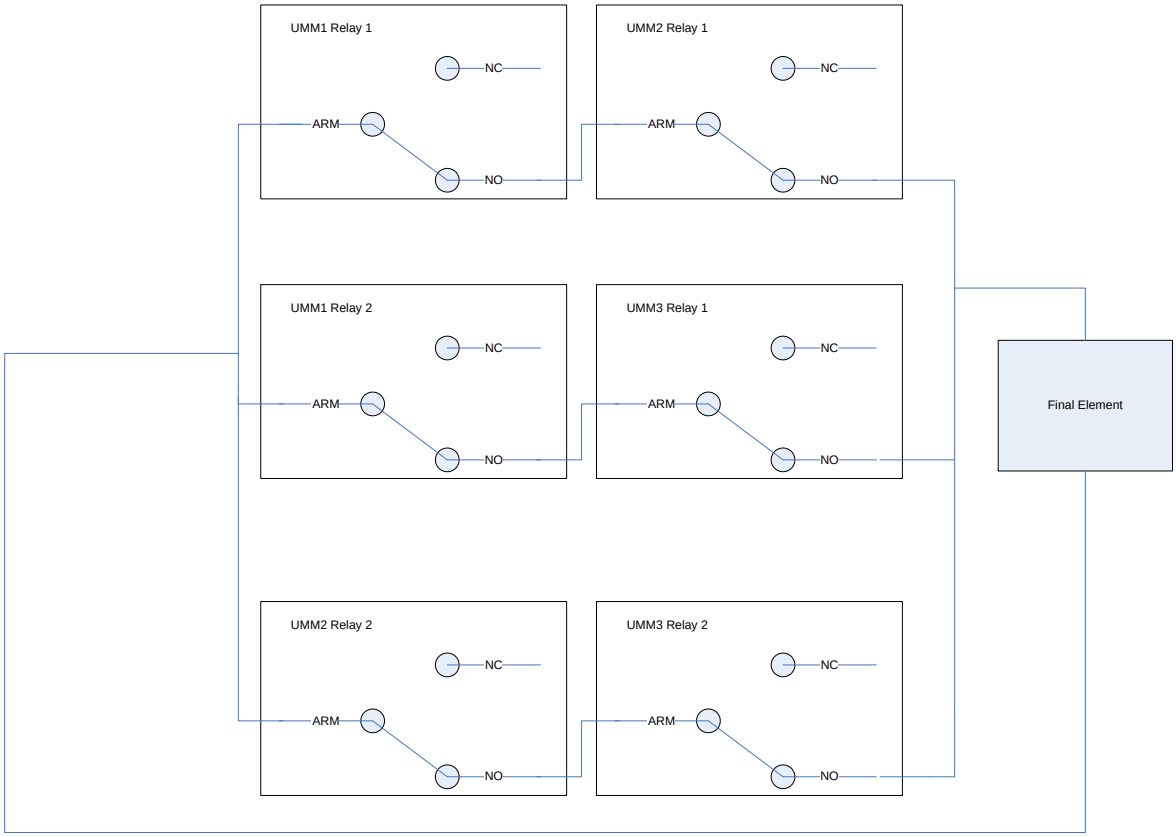

Figure 7: 2oo3 Relay wiring

Note: Since each UMM is performing 2oo3 logic, you can just connect the 3 relays in series. However, series wiring does not allow hot swap or reconfiguration on-line servicing of UMMs since disconnection of the relay will cause a trip.

SETPOINT

2oo3 Relay Voting:

PFD_{avg}: 7.44 x 10^{-5} **Meets SIL 1 and SIL 2 requirements**
SFF =91.8%
HFT = 1

1oo3 Relay Voting:
PFD_{avg}: 6.14 x 10^{-5} **Meets SIL 1, 2, and SIL 3 requirements**
SFF = 93.3%
HFT = 1

Although there are three UMMs, the HFT = 1 because 2 out of 3 UMMs must be operational to trip. In the 2 out of 3 relay voting scenario, the SFF drops because of the relay diagnostic coverage of the added relays. The 1oo3 relay voting has better reliability and SFF, but is difficult to service on-line.

System: **Meets SIL 1, 2 and SIL 3 requirements**
$PFD_{avg=}$ 1.43 x 10^{-4}

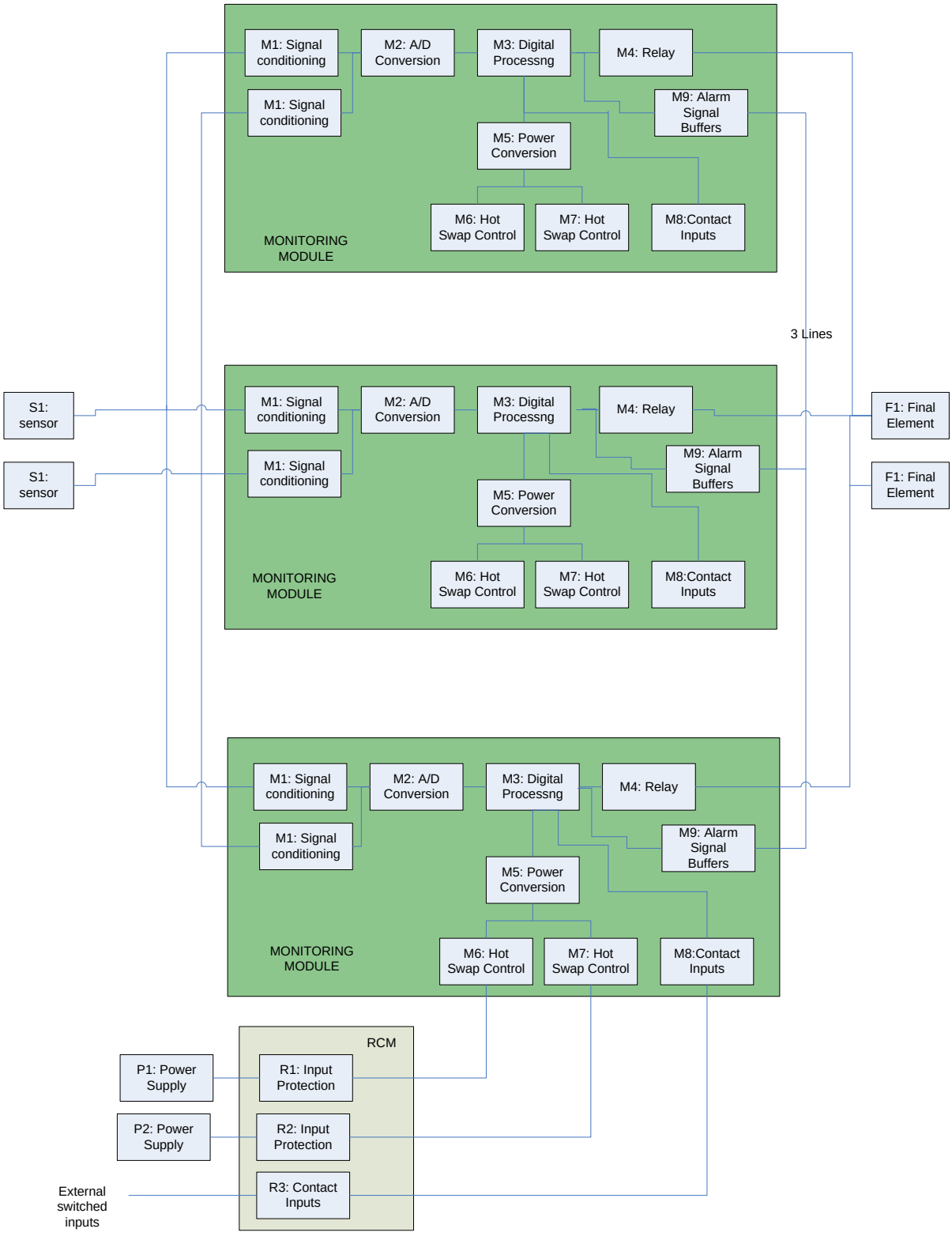

Figure 8: Two Sensors with 2oo3 Voting UMMs, Duplex Final Elements

8.1.10 Redundant Sensors, 1 UMM, With Feedback

In this scenario, a feedback path is provided from the machine back to the monitoring module, allowing the monitoring module to determine if the machine actually shut down. This could be a UMM discrete input connected to the final element or a contact from the motor controller. Alternatively, it could be a speed value. The feedback allows the monitor to verify the machine was shut down and provides diagnostics on the relay, final element, and output wiring. On detecting a feedback failure, the system activates a relay to warn the operator that an alarm has occurred but the machine failed to go to the safe state. While the added elements decrease the reliability, the detection increases. *The equations in IEC61508 are not applicable to this design because it does not determine if the relay and final element failed until there is demand. This application is more layering protection rather than detection as the annunciator out would be used to activate another layer of protection to shut down the machine.*

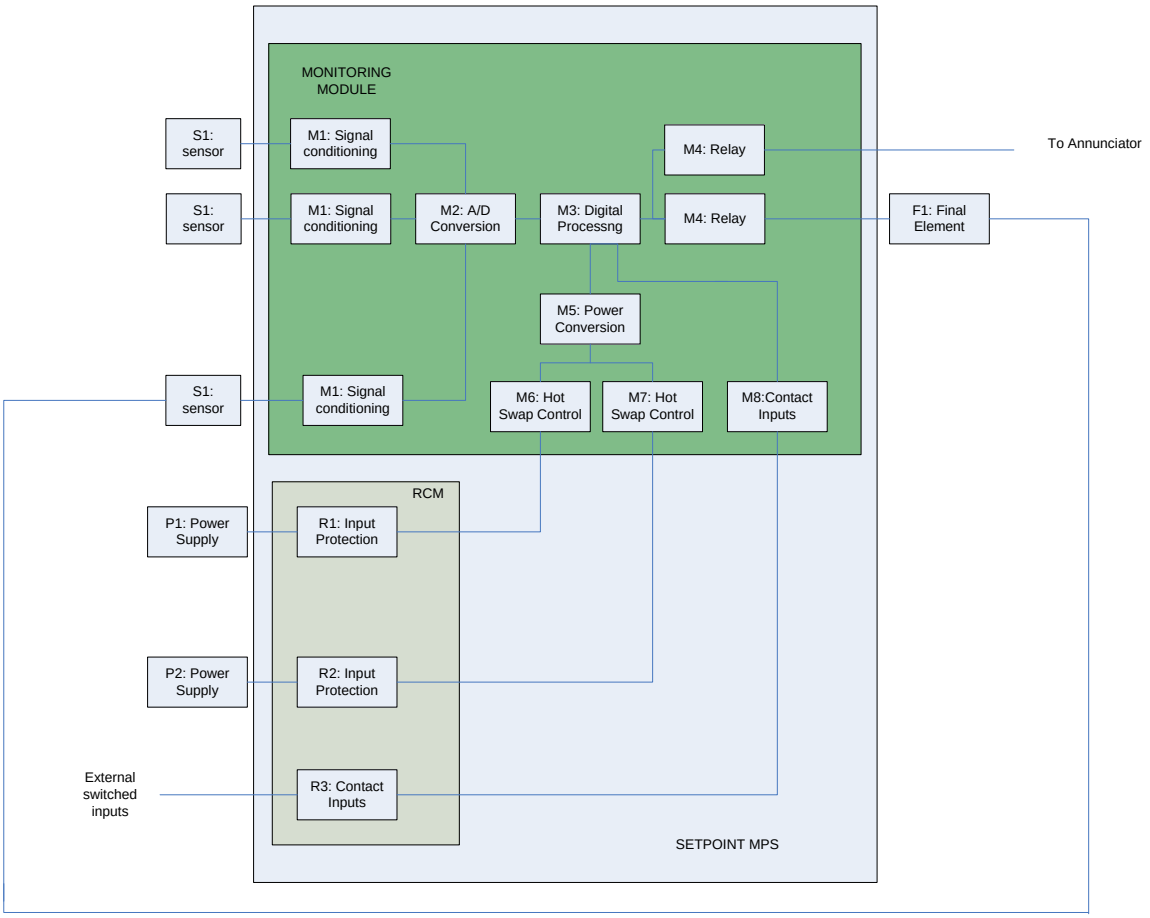

Figure 9: Feeding Back Machine Speed

8.2 Management

Much of IEC 61508 involves proper practices over the product lifecycle. This section provides a brief overview of some of the techniques used by SETPOINT Vibration to manage the safety lifecycle.

8.2.1 Project management

The SETPOINT platform was designed under Metrix Instrument Company, L.P. (ISO 9000-1 certified) procedures and guidelines. SETPOINT is currently sustained and manufactured following Compressor Controls Corporation (ISO 9000-1 certified) procedures and guidelines. Both companies follow the Product Development and Design Process common to all businesses within Roper Technologies' Energy Systems & Controls group.

The project management requirements per IEC 61508 exceed the requirements of ISO 9000-1. The additional requirements are listed in the SETPOINT Functional Safety Management Plan.

8.2.2 Safety Lifecycle

8.2.2.1 Safety Requirements

System requirements are documented in a database. Requirements pertaining to safety are tagged as safety requirements. The SETPOINT Safety Requirements Specification lists the specification required to achieve the target SIL ratings.

8.2.2.2 Safety Validation Planning

Requirements tagged as safety are linked to safety test plans that define the test procedures to validate the safety requirement.

8.2.2.3 Design and Development

All designs were performed by qualified engineers with a Bachelor of Science degree or higher. Average experience level in machine protection systems was > 5 years.

Techniques for detecting and annunciating faults are listed in the SETPOINT Functional Safety Management Plan.

All SETPOINT MPS electrical designs are de-rated for voltage and power per established de-rating guidelines derived from *Reliability Design Handbook (RDH-376)*.

All designs are reviewed by another engineer against the safety requirements, product requirements, and component datasheets. Many were reviewed by qualified Field Application Engineers employed by the Integrated Circuit OEMs providing the circuits and references designs used in SETPOINT MPS.

8.2.2.4 Installation, Commissioning, Operation, and Maintenance Procedures

Manual 1079330 describes the requirements for installing, commissioning, operating, and maintaining the SETPOINT MPS. It is the user's responsibility to verify their procedures are in line with manual 1079330.

8.2.2.5 Validation

Proper validation testing of the alarming safety function is discussed in the 1079330 SETPOINT MPS Operation and Maintenance Manual. The configuration software is not part of the SIL system so it is required to validate the safety function after configuration. Validation must be performed by trained personnel.

8.2.2.6 Operation

Document 1079330 SETPOINT MPS Operation and Maintenance Manual lists proper operation. The system is only to be operated by trained personnel.

8.2.2.7 Modification

Modifications involving the safety functionality are reviewed per the safety impact checklist. The safety checklists were created according to IEC 61508.

8.2.2.8 Verification

Each product change requires test runs performed according to the test plans discussed in section 8.2.2.2.

8.2.2.9 Assessment

This assessment was performed internally by SETPOINT Vibration using typical allocations for sensors and final elements. A final assessment should be performed using probability of failure data for the actual sensors and final elements used.

8.2.2.10 Decommissioning

SETPOINT MPS has no special decommissioning requirements.

9 Disclaimer

SETPOINT Vibration prepared this document based on data collected from field return data using generally accepted calculation methods. SETPOINT Vibration accepts no liability for the use of these numbers or the correctness of the generally accepted calculation methods.

10 Revision History

CR Number	Change Description	Revision
NONE	Initial Release	A
3835	Add TMM information	B