SIL SAFETY MANUAL

Table of Contents

1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the *Moniteur VPT*. This manual provides necessary user information and requirements for meeting the IEC 61508 and/or IEC 61511 functional safety standards.

1.1 Terms and Abbreviations

Safety	Freedom from unacceptable risk of harm
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems
Element	Part of a subsystem comprising a single component or any group of components that performs one or more element safety functions
Fail-Safe State	State of the process when safety is achieved
Fail Safe	Failure that causes the Moniteur VPT to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not permit the SIF to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state)
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic testing
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic testing.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.

1.2 Acronyms

EUC	Equipment Under Control
FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
MOC	Management of Change. These are specific procedures to follow for any work activities in compliance with government regulatory authorities or requirements of a standard.
PFDavg	Average Probability of Failure on Demand
PFH	Probability of Failure per Hour

SFF	Safe Failure Fraction, the fraction of the overall failure rate of an element that results in either a safe fault or a diagnosed dangerous fault.
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 is the highest level and Safety Integrity Level 1 is the lowest level.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

1.3 Product Support

Product support can be obtained from:

Moniteur Devices, Inc

36 Commerce Road.

Cedar Grove, NJ 07009 USA

Contact sales@moniteurdevices.com

1.4 Related Literature

Hardware Documents:

- *Moniteur VPT* Installation, Operation and Maintenance Instructions

Guidelines/References:

- Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, ISBN 978-1-934977-03-3, exida
- Control System Safety Evaluation and Reliability, 3rd Edition, ISBN 978-1-934394-80-9, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems
- IEC 61511:2003 Functional Safety – Safety Instrumented Systems for the Process Industry Sector (or ISA 84.00.01 if it is more appropriate)

2 PRODUCT DESCRIPTION

The VPT Series Indicator is a mechanical device that graphically displays the angular displacement of a quarter turn valve or any other device operating between 0 and 90 degrees. The Moniteur Indicator represents a true indication of valve position. It is infinitely adjustable and delivers a 100% change of indication, displaying 90 degrees of rotation by utilizing either an amplified mechanical drive or rotating barrel. On linear valves, the VPT Series is a mechanical device that detects linear position of the valve.

The Safety Function for the VPT Series is to have the device's switch(es) change state when the attached valve is rotated to the device's preset position or with a linear valve when the valve moves to the device's preset position. The FMEDA considers only that the opening / closing of the electrical switches are part of a Safety Function, no consideration is given to any visual indication that the VPT Series may also provide. Note that while devices are available with from 1 to 6 Switches, it is assumed that the Safety Function is only using a single switch.

See Installation and Maintenance Manual for additional setup and configuration details.

2.1 Hardware and Software Versions

The table below gives an overview of the different models and switch type combinations that are included in the VPT Series.

Table 1 - Version Overview

Series	Housing Code	Part Number Suffix	Switch Type (Switch Code)	Switch Qty
Sentinel	A	XSIL	SPDT, Mechanical (1, C, 10) SPDT Gold Plated, Mechanical (3, 30) DPDT Mechanical (4, 40) SPDT Tungsten, Proximity (2, 21, 22) SPDT Tungsten I-IV, Proximity (E, 21, 22) SPST Rhodium, Proximity (7, 70, 71) SPDT Rhodium, Proximity (T, T0, T1) NJ2-V3, Inductive (8, 80)	1 to 6
Sentinel-S3	S	(none)		
Sentinel-II	C	(none)		
Watchman	F	XSIL		
Watchman II	H	XSIL		
Survivor	P	XSIL		
Survivor-II	Q, R	(none)		
Companion	X	(none)	SPDT Tungsten, Proximity (2, 21, 22) SPDT Tungsten I-IV, Proximity (E, 21, 22) SPDT Rhodium, Proximity (T, T0, T1)	1 to 2

FMEDA Group	Switch Description	Applicable Switch Codes
Group 1	NAMUR Proximity Sensors	8, 80
	MicroSwitches* and Proximity Reed Switches*, rated up to 3 Amps and external Current Limiting / Protection	2, 21, 22, 3, 30, E, 7, 70, 71, T, T0, T1
Group 2	MicroSwitches (Applications with Switches rated up to 15 Amps)	1, C, 10, 4, 40
Group 3	Companion Series, Proximity Reed Switches rated up to 3 Amps and external Current Limiting / Protection	2, 21, 22, E, T, T0, T1

*Switch contact's current is limited to 60% of the switches rated capacity and the end user has added external transient protection if being used with non-resistive loads

The VPT Series Indicator is classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

3 DESIGNING A SIF USING A MANUFACTURER PRODUCT

3.1 Safety Function

The product will sense valve position by the device switch change state when the attached actuator and or valve is rotated to the devices preset position.

The *Moniteur VPT* is intended to be part of a SIF subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer.

The Moniteur VPT can operate in low, high, or continuous demand modes.

3.2 Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the *Moniteur VPT* I&M and the equipment's nameplate for environmental limits.

3.3 Application limits & restrictions

The *Moniteur VPT* is intended for use in any application requiring the sensing of valve position for on-off valves**.**

The materials of construction of a *Moniteur VPT* are specified in the *Moniteur VPT* Brochure and I&M. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the *Moniteur VPT* is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of **IEC** 61508-2, ed2, 2010.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Moniteur. This report details all failure rates and failure modes as well as the expected lifetime. Assumptions made during the FMEDA are listed in the FMEDA report.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFD_{avg} or PFH, considering safety architecture, proof test interval, proof test effectiveness, any automatic diagnostics and worst case fault detection interval, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the *Moniteur VPT* product and its failure rates.

The failure rate data listed in the FMEDA report are only valid for the useful lifetime of *Moniteur VPT*. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the required Safety Integrity Level will not be achieved.

An appropriate MTTR shall be selected based on plant operation and maintenance procedures.

3.5 SIL Capability

3.5.1 Systematic Integrity – Meets SIL 3

The *Moniteur VPT* product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These requirements are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by the end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

The *Moniteur VPT* is a Type A Element. Therefore, based on the SFF between 60% and 90%, a design can meet SIL 2 @ HFT=0 and SIL 3 @ HFT=1 when the *Moniteur VPT* is used as the only component in a SIF subassembly.

The architectural constraint type for the *Moniteur VPT* Series Indicator is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

When the SIF consists of many components (list components if applicable) the SIL must be verified for the entire assembly using failure rates from all components. This analysis must account for any hardware fault tolerance and architecture constraints.

3.5.3 Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the *Moniteur VPT*.

3.6 Connection of the *Moniteur VPT* to the SIS Logic-solver

The *Moniteur VPT* is connected to the safety rated logic solver according to the wiring diagram supplied in the I&M or on the inside of the product cover.

3.7 General Requirements

The system's response time shall be less than the process safety time. The *Moniteur VPT* will move to its safe state with the valve and or actuator package it is mounted on, and the switch feedback, bring hardwired, will respond immediately according to its set point.

All SIS components including the *Moniteur VPT* must be operational before process start-up.

User shall verify that the *Moniteur VPT* is suitable for use in safety applications by confirming the *Moniteur VPT*'s nameplate is properly marked for its intended use and hazardous area.

Personnel using and performing maintenance and testing on the *Moniteur VPT* shall be competent to do so.

Proof tests should be performed at a minimum 6 months interval. Results from the proof tests shall be recorded and reviewed periodically.

4 INSTALLATION AND COMMISSIONING

4.1 Installation

It is the responsibility of the end user to maintain and operate the *Moniteur VPT* Series Indicator per manufacturer's instructions. The *Moniteur VPT* must be installed per standard practices outlined in the Installation Manual.

The environment where the Moniteur VPT is installed must be checked to verify that environmental conditions do not exceed the *Moniteur VPT* ratings.

The *Moniteur VPT* location and placement must be accessible for physical and or visual inspection and allow for manual proof testing.

Furthermore, regular inspection of the *Moniteur VPT* should show that all components are clean and free from damage.

5 OPERATION AND MAINTENANCE

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within *the Moniteur VPT* that are not detected by any automatic diagnostics of the system. Of main concern are undetected failures that prevent the Safety Instrumented Function from performing its intended function.

The frequency of proof testing, or proof test interval, is to be determined in reliability calculations for the Safety Instrumented Functions for which *the Moniteur VPT* is applied. The proof tests must be performed at least as frequently as specified in the calculation in order to maintain the required safety integrity of the Safety Instrumented Function. At a minimum Moniteur recommends once every 6 months.

The suggested Proof Test consists of a full stroke of the Moniteur VPT Series and actuator and or valve, see the Table 2 below for the Suggested Proof Test. Refer to Table 3 for the Proof Test Coverages.

Table 2 - Suggested Proof Test — *Moniteur VPT* Series Indicator

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the air supply to the Actuator to force the Actuator/Valve assembly to travel to (or past) the position that the *Moniteur VPT* Series is set to detect. Confirm that the Switch / Proximity Sensor's output changed states and confirm the position is within the desired position accuracy. The time required for the Actuator/Valve to travel to this position should also be monitored to confirm that this was achieved within the correct amount of time.
3.	Re-store the air supply to the Actuator, allow the assembly to return to the original position before the proof test began and inspect the *Moniteur VPT* Series, Actuator and Valve for any leaks, visible damage or contamination. Also confirm that the normal operating state was achieved.
4.	Remove the bypass and otherwise restore normal operation.

For the suggested proof test to be effective the movement of the Valve must be confirmed. To confirm the effectiveness of the test both the travel of the Valve and slew rate must be monitored and compared to expected results to validate the testing.

The Proof Test Coverage for the various device configurations are given in Table 3.

Table 3 - Proof Test Results — VPT Series Indicator

Device	ÅDUPT7 (FIT)	Proof Test Coverage
		No PVST
Group 1 — NAMUR Proximity Sensors, Micro Switches, or Proximity Reed Switches	5.0	94%
Group 2 — Micro Switches (Applications with Switches rated up to 15 Amps)	5.3	96%
Group 3 — Companion Series, Proximity Reed Switches rated up to 3 Amps and external Current Limiting	0.4	98%

7 ÅDUPT = Dangerous undetected failure rate after performing the recommended proof test.

The person(s) performing the proof test of the *Moniteur VPT* should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures.

It is recommended that a physical inspection be performed on a periodic basis with the time interval determined by plant conditions. A maximum inspection interval of 1 year is recommended.

5.2 Repair and replacement

Repair and replacement procedures in the *Moniteur VPT* Installation, Operation and Maintenance manual must be followed.

5.3 Useful Life

The useful life of the *Moniteur VPT* is 10 years, or 10,000 cycles, whichever occurs sooner.

5.4 MANUFACTURER Notification

Any failures that are detected and that compromise functional safety should be reported to Moniteur Devices. The contact information is listed below:

Moniteur Devices, Inc

36 Commerce Rd.

Cedar Grove, NJ 07009 USA

www.moniteurdevices.com

Contact sales@moniteurdevices.com

Appendix A Sample Start-up Checklist

This appendix provides Sample Start-up Checklist for a *Moniteur VPT*. A Sample Start-up Checklist will provide guidance during site acceptance testing.

1 SAMPLE START-UP CHECKLIST

The following sample start-up checklist may be used as a guide to employ the Moniteur VPT in a safety critical SIF compliant to IEC61508.

#	Activity	Result	Verified	
			By	Date
	Design			
	Target Safety Integrity Level and PFDavg determined			
	Correct product configuration mode chosen (Fail-closed, Fail-open, etc.)			
	Design decision documented			
	Product compatibility and suitability verified			
	SIS logic solver requirements for valve tests defined and documented			
	Routing of pneumatic and electrical connections determined			
	SIS logic solver requirements for proof tests defined and documented			
	SIS Design formally reviewed and suitability formally assessed			
	Implementation			
	Physical location appropriate			

#	Activity	Result	Verified	
			By	Date
	Pneumatic and electrical connections appropriate and according to applicable codes			
	SIS logic solver valve actuation test implemented			
	Maintenance instructions for proof test released			
	Verification and test plan released			
	Implementation formally reviewed and suitability formally assessed			

#	Activity	Result	Verified	
			By	Date
	Verification and Testing			
	Electrical connections verified and tested			
	Pneumatic connection verified and tested			
	SIS logic solver valve actuation test verified			
	Safety loop function verified			
	Safety loop timing measured			
	Bypass function tested			
	Verification and test results formally reviewed and suitability formally assessed			
	Maintenance			
	Tubing blockage / partial blockage tested			
	Safety loop function tested			

Rev.	DATE	SECTION	CHANGE
A	05/27/2020	All	Initial Issue