WESTLOCK
CONTROLS

QUANTUM Valve Control Monitor & Falcon V Solenoid Valve Safety Manual

With Magnum XT 90 Proximity Switches, SPDT/DPDT Mechanical Switches and Inductive Proximity Sensor (NJ2-V3-N)

exida CERTIFIED IEC 61508 SIL 3 CAPABLE

Safety Manual: SMAN-005		**Revision: C**	
Prepared By: Anthony Paolini	**Date:** 2/8/16	**Drafting Work Order:** 24857	**ECN:** 13712
Reviewed By: Terrence Lee	**Date:** 7/15/21	**Approved By:** Mita Patel	**Date:** 7/15/21

WESTLOCK CONTROLS
280 N. MIDLAND AVE., STE. 258, SADDLE BROOK, NJ 07663 TEL: 201-794-7650 FAX: 201-794-0913

www.westlockcontrols.com

1. Status of the document

1.1 Revision History

Revision	Rev. A	Rev. B	Rev. C
February 8, 2016	03/20/2020	04/26/2021	06/04/2021
Initial release			

Westlock Controls Offices

Americas: +1 201 794 7650

Europe, Middle East & Africa: +44 (0) 1892 516277

Asia Pacific: +65 6869 8909

Website address: www.westlockcontrols.com

Table of Content
Section 1 Switches

Table of Content
Section 2 Quantum Valve Control Monitor & FALCON V

2. Purpose and Scope

This document provides an overview of the user responsibilities for installation, operation and maintenance of an QUANTUM Control Monitor containing the Magnum XT-90 proximity switch, V3 SPDT/DPDT Mechanical switch and Inductive Proximity Sensor in order to maintain the designed Safety Integrity level. Items that will be addressed are proof testing, repair and replacement of the related components, lifetime, environment application limits, parameter settings and replacement of the related component , lifetime, environmental and application limits and parameter settings using a QUANTUM assembled with either V3 SPDT Mechanical Switches or Magnum XT-90 Proximity switches.

3. Diagnostic Response Time.

A QUANTUM that contains either V3 SPDT mechanical or Magnum XT-90 proximity switch, when used in a SPDT wiring configuration, has automatic diagnostic abilities by monitoring of the both the open and closed contacts.

The actual response time for the action of either type of switch is immediate and the diagnostic response time is related to the refresh rate of the host interface.

3.1 Installation and Maintenance

The installation of this QUANTUM Control monitor shall be to the I.O.M supplied (TECH-382 and TECH-382Q). It is essential that the QUANTUM is used within the environmental and certification parameters. It is recommended that a periodic visual and operation evaluation is carried at least once a year or every 1 million cycles.

When using the QUANTUM product within a safety system it should be noted that switch contact ratings should be no more than 60% of the switch vendors ratings, and that any non-resistive load must have transient protection added by the end user.

3.2 Proof test

The objective of proof testing is to detect failures within the QUANTUM that are not detected by any automatic diagnostics of the system. The concerns are undetected failures that prevent the Safety Instrumented Function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which either switch type maybe applied. The proof tests must be performed more frequently or as frequently as specified in the calculation in order to maintain the required safety integrity of the Safety Instrumented Function.

The following proof test is recommended.

Step	Action
1.	Following Management of Change procedures for the site, take note of the switch Contact status (COM- N/O or COM - N/C).
2.	Stroke the actuator and / or the valve to a desired position and check the opposite contacts from STEP 1 for continuity or electrical parameters.
3.	Adjust cam position if necessary and take corrective action to ensure that the installation is carried out using the service air pressure.
4.	Records any failures in the SIF inspection database. Restore the loop to full operation.

This test will detect approximately 99% of possible DU failures in the QUANTUM (Proof Test Coverage). The person(s) performing the proof test on the QUANTUM proximity switch should be trained in SIS operations, including bypass procedures, position monitor maintenance and company Management of Change procedures. Tools required are: Refer to the I.O.M supplied with the QUANTUM (TECH-382 and TECH-382Q).

3.3 Repair and replacement

When replacing either switch type it is essential that the instructions for that specific QUANTUM variation are followed. Failure to follow these instructions may impair the reliability.

3.4 Reliability data and lifetime limit

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Westlock Controls Corporation. This report details all failure rates and failure modes, common cause factors for applications with redundant devices and the expected lifetime of a QUANTUM.

- A Quantum with either switch type is intended for low demand mode applications up to SIL3 for use in a simplex (1oo1) configuration, depending on the PFD_{AVG} calculation of the entire Safety Instrumented Function.

- The development process of an QUANTUM containing either switch type is suitable up to SIL3, allowing redundant use of the transmitter up to this Safety Integrity Level, depending the PFD_{AVG} calculation of the entire Safety Instrumented Function.

- When using an QUANTUM containing either switch type in a redundant configuration, a common cause factor should be included in reliability calculations. For details see the FMEDA report.

- The reliability data listed in the FMEDA report is only valid for the useful life time of an QUANTUM containing either switch type. The failure rates of an QUANTUM containing either switch type may increase sometime after this 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 calculated Safety Integrity Level will not be achieved.

The Safety Function of the QUANTUM's switch(s) will change its output when the attached valve moves to the configured position.

Table 1 below details the failure rates for the V3 SPDT mechanical switch (M02), DPDT Mechanical switch (M04), Proximity Sensor (M08) NJ2-V3-N and Magnum XT-90 proximity switch (M06) all of which can be used within the following series of enclosures: 360, 366, 711, 722,764,765,784,789,811,864,777,877.

Table 1 Failure rates according to IEC 61508 in FIT

QUANTUM Series: 360, 366, 711,722,764,765 784,789, 811, 864, 777, 877. **Switch Circuit Qty. (all switch codes)**	λ_{SD}	λ_{SU1}	λ_{DD}	λ_{DU}	
1 Switch Circuit	0	11	0	94	
2 Switches Circuit	0	23	0	119	
3 Switches Circuit	0	34	0	149	
4 Switches Circuit	0	45	0	174	
1 Switch Circuit w/PVST	11	0	86	8	
2 Switches Circuit w/PVST	22	0	110	9	
3 Switches Circuit w/PVST	34	0	139	10	
4 Switches Circuit w/PVST	45	0	163	11	

The architectural constraint type for the QUANTUM Valve Position Monitor 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 as well.

[1] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, edition 2: 2010.

[2] Safe Failure Fraction needs to be calculated on (sub) system level.

3.5 Environmental and Application limits

QUANTUM position monitors are certified to various protection methods and environmental temperature limitations. These can be found on the product label (found on the outside of the cover) and on the supporting IOM delivered with each unit. If the QUANTUM position monitor is used outside of the application limits then the reliability data listed in Section 2.5 becomes invalid.

3.6 Reporting a failure

Any failures that are detected and that compromise functional safety should be reported to the Safety Office / QA Supervisor within Westlock Controls. It is recommended that customers and end users register the SIL product with Westlock Controls using the unique serial number located on the Identification Label.

4.Terms and Abbreviations

Safety Freedom from unacceptable risk of harm.

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.

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.

Safety Assessment The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.

Further definitions of terms used for safety techniques and measures and the description of safety related systems are given in IEC 61508-4.

FMEDA Failure Modes, Effects and Diagnostic Analysis.

HFT Hardware Fault Tolerance.

Low demand mode Mode , where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.

PFD_{AVG} Average Probability of Failure on Demand.

SFF Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe 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 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.

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 Product Description

The Westlock Controls Quantum Valve Control Monitor & FALCON V Series Solenoid Valves are a TYPE A device with a Hardware Fault Tolerance of 0.
The series is comprised of 3-way and 4-way, 2 control pilot operated pneumatic valves. A pilot supply can be either Internal or External pilot for all valves. A low power solenoid controls the pilot signal which provides the positive force for shifting the valve spool. The Safety Function of this valve will move to the designed safe position when de-energized / energized within the specified safety time per the system design. The table 2, 3 and 4 below defines the solenoid coils and FALCON V valves that are covered by the FMEDA and SIL certificate.

Westlock Controls: Quantum Valve Control Monitor Coil Designation			
Series	**Coil Type Code**	**Coil Voltage**	**Coil Description**
711, 722 & 811	I	24VDC (1.5W)	Coil Falcon Ex ia / Intrinsically Safe
	P	24VDC (1.6W) - Standard	
764, 784 & 864 765, 789 & 865	D	24VDC (0.84W)	Coil Falcon Ex nA / Non Incendive
	C	24VAC (4.9VA)	
	A	120VAC (6.5VA)	
	V	125VDC (1W)	
	H	220VAC (4.5VA)	
777 & 877 360 & 366	X	24VDC (0.7W)	Coil Falcon Ex d / Flame-Proof
	Y	120VAC (5.8VA)	

Table 2

Westlock Controls Falcon V Solenoid Coil Designation					
First position		Second position		Third position	
Coil Type Code	Description	Voltage Code	Description	Coil Option Code	Description
D	FLCNV S/A Class 1 Div 1, Class 1 Div. 2 and GP 1/2"NPT fly lds & stainless fully potted hub	A	90-120 VAC for X, 120VAC 6.5V-A for F	L	Low temp coil seals (below -40C)
E	Global XP nipple-on with 1/2NPT female conduit, are C1D1 BCD, II 2 G Ex d IC T*Gb, CL I Zone 1 Aex d e IIC T*	B	12 VAC (<10VA)	O	No options
F	Coil in encl. w/9.5" fly lds	C	24 VAC (4.9VA)	R	ELR0100 mtg
H	FLCNV S/A ½NPT TS w/18" fly lds attached (F coil with separate conduit hub attached)	E	48 VDC		
P	Parker A00 coil in enclosure	F	48 VAC (<10VA)		
X	EXD/Div 1 M32 thd in encl. w/7-8" fly lds	H	220/240 VAC (4.7VA)		
		I	24 VDC (1.5W)		
D/C - dual coil		J	12 VDC		
S/A - standalone		P	24 VDC (1.6W)		
		S	24 VDC (0.84W)		
		T	24 VDC (1.8W)		
		V	125 VDC (1W)		
		X	125 VDC (3W)		
		Y	24 VDC (0.7W to 1.3W)		
		Z	110/120 VAC (1.8W)		

Table 3

Valve Designation for Quantum Valve Control Monitor & Falcon V Solenoid Valve					
First position-Basic Material of Construction		Second position- Style	Third Position-Flow Path Type		Fourth position-Options	
Material Code	Description	Style Code	Config Code	Description	Option Code	Description
2	Brass	V	Coil in Enclosure		0	NO OPT
3	Aluminum		3	1.4Cv 3-way 1 Coil	1	OPT-N + OPT-I
5	SS316		7	1.4Cv 4-way 1 Coil	2	NACE MR-01-75 SS
			Y	1.4Cv 4-way Dual Coil	3	Speed Controls
			4	4.3Cv 3-way 1 Coil	4	Opposite side mount
			8	4.3Cv 4-way 1 Coil	5	Opp. Side Mt.+OPT-I
			Z	4.3Cv 4-way Dual Coil	6	OPT-R + OPT-I
					7	OPT-L + OPT-X
					8	OPT-M + OPT-X
					9	OPT-R + OPT-X
					A	OPT N+OPT E
					B	OPT R+OPT E
					C	OPT L+OPT E
					D	OPT M+OPT E
					E	External pilot
					F	OPT-R+OPT-4
					G	Normally Open (plug 2 ports on 4-way)
					H	"Screw Driver Type" Locking Guarded Manual Override
					I	No indicator
					L	Man override maintained
					M	Man override momentary
					N	Manual reset latching
					R	Manual reset non-latch
					X	Low Temp Seals

Table 4

2 Purpose and Scope

This document provides an overview of the user responsibilities for installation, operation and maintenance of a FALCON V Solenoid in order to maintain the designed Safety Integrity Level. Items that will be addressed are proof testing and lifetime environmental and application limits and parameter settings.

3 Using a FALCON V Solenoid

3.1 Diagnostic Response Time

A FALCON V Solenoid does not perform an automatic diagnostic function by itself and there is no diagnostic response time. Automatic diagnostics of a FALCON V solenoid may be performed by a partial valve stroke testing device. It is recommended that any solenoid be tested at least once a month with a cycle of de-energize and energize.

3.2 Setup and Installation

No special installation is required in addition to the standard installation practices outlined in the Installation Manual.

3.3 Proof test

The objective of proof testing is to detect failures within a FALCON V Solenoid that are not detected by any automatic diagnostics of the system. The concern is undetected failures that prevent the safety instrumented function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a FALCON V Solenoid is applied. The proof tests must be performed as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. Any failures that are detected and that compromise functional safety should be reported to a FALCON V Solenoid Safety Officer within Westlock.

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip, following Management of Change procedures
2	Interrupt or change the signal to the Falcon V to perform a Safe trip and ensure that the final element Actuator and Valve achieve the Fail Safe state (defined by the application) and within the correct amount of time. **Note: This tests for all failures that could prevent closure of the valve as well as the final control valve and actuator faults.**
3	Inspect the Falcon V for any visible damage, signs of leaks or contamination.
4	Re-store the original input to the Falcon V and ensure that the attached final control element returns to it's normal operating state (defined by the application) and within the specified amount of time.
5	Remove the bypass and otherwise restore normal operation.

This test will detect approximately 96% of possible DU failures as listed in the FMEDA report. It will also cover 45-60% if credit for PVST is being used (ref table 11 in FMEDA).

The person(s) performing the proof test of a FALCON V Solenoid should be trained in SIS operations, including bypass procedures, solenoid maintenance and Company Change Out Procedures.

3.4 Repair and replacement

Any failures that are detected and that compromise functional safety should be reported to a FALCON V Solenoid Safety Officer within Westlock Controls. When replacing a FALCON V Solenoid the procedures in the installation manual should be followed (see TECH 486).

3.5 Reliability data and lifetime limit

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Westlock Controls upon request. This report details all failure rates and failure modes, common cause factors for applications with redundant devices and the useful lifetime of a FALCON V Solenoid.

- A FALCON V Solenoid is intended for low demand mode applications for use in a simplex (1oo1) configuration, depending on the PFD_{AVG} calculation of the entire Safety Instrumented Function.

- The development process of a FALCON V Solenoid is certified up to SIL3, allowing redundant use of the transmitter up to this Safety Integrity Level, depending the PFD_{AVG} calculation of the entire Safety Instrumented Function.

- When using a FALCON V Solenoid in a redundant configuration, a common cause factor should be included in reliability calculations. For details see the FMEDA report.
- The reliability data listed the FMEDA report is only valid for the useful life time of a FALCON V Solenoid. The failure rates of a FALCON V Solenoid may increase sometime after this 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 calculated Safety Integrity Level will not be achieved.

3.6 Environmental limits

The environmental limits of a FALCON V Solenoid are specified in the user manual TECH 486.

3.7 Application limits

The application limits of a FALCON V Solenoid are specified in the user manual TECH 486. If a solenoid is used outside of the application limits the reliability data listed in the FMEDA report becomes invalid.

3.8 The Product Safety Officer

Any failures that are detected which can compromise functional safety should be reported to the WESTLOCK CONTROLS Safety Coordinator through Customer Service at the phone numbers and email address listed on page 2.

Terms and Abbreviations

Safety	Freedom from unacceptable risk of harm
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
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
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems

Further definitions of terms used for safety techniques and measures and the description of safety related systems are given in IEC 61508-4.

FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on safety related system is greater than twice the proof test interval.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state plus the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
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 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
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).