USER INSTRUCTIONS

D30 Compact Digital Positioner

Safety Manual

FCD PMENDS0030-01-A5 09/19

Experience In Motion

Contents

Version history

Version	Date	Author	Comment
V1R0	27 May 2014	DAJ	Exida template
V1R1	29 June 2019	ALN	PMV D30 safety manual, Ver 1, Rev 1
V1R2	5 August 2019	ALN	Update using document field codes

1. Introduction

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the D30 valve positioner with 4-20 mA current loop control. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 Terms

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
Fail-Safe State	State where solenoid valve is de-energized and spring is extended.
Fail Safe	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not 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 stroke testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic stroke testing.
Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Annunciation Detected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.

1.2 Abbreviations

FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
MOC	Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFDavg	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).

1.3 Product Support

Product support can be obtained from:

PMV Automation AB
+46 8 555 10 600
pmv.se

1.4 Related Literature

Hardware Documents:

- D30 Installation, Operation and Maintenance Instructions

Guidelines/References:

- Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis, ISBN 1-55617-777-1, ISA
- Control System Safety Evaluation and Reliability, 2nd Edition, ISBN 1-55617-638-8, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2000 Functional safety of electrical/electronic/ programmable electronic safety-related systems
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector

2. Device Description

The components of the Safety Instrumented Function are described in this section.

The device is a current-controlled valve positioner used to control an automation or process valve, which in turn controls fluids and flows. The valve positioner is available with or without HART capability and is designed to meet international standards for pressure and temperature ratings, shell thickness, and bore diameters. The valve positioner provides VDI/VDE and Namur mounting for simple actuator mounting. The valve positioner includes IP66 sealing and protection of air vent ports.

3. Designing a SIF Using a Customer Product

3.1 Safety Function

The valve positioner, when electrically de-energized (input current on terminal slot 1 less than 0.2 mA), moves its internal air pilot valve to its failsafe position, which means that the C+ port is vented (depressurized) and the C- port is pressurized.

Depending on the air tube connection to the valve actuator, the valve will be Fail – Closed or Fail - Open. The valve will rotate the valve plug to close off the flow path through the valve body or open the flow path through the valve body.

If the valve actuator contains a return spring intended for pneumatic safety, care should be taken when tubing the actuator so that the spring does not counter the valve positioner failsafe action.

The valve is intended to be part of final element subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer. PMV Automation AB is not liable for damages occuring as a result of incompatible or inaccurate valve system design, or any valve system design incorporating any PMV Automation valve positioner.

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 PMV Automation AB D30 Brochure for environmental limits.

3.3 Application limits

The materials of construction of a D30 are specified in the PMV Automation AB brochure. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the D30 is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from PMV Automation AB. This report details all failure rates and failure modes as well as the expected lifetime.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDAVG considering architecture, proof test interval, proof test effectiveness, any automatic diagnostics, 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.

When using D30 in a redundant configuration, a common cause factor of at least 5% should be included in safety integrity calculations.

The failure rate data listed the FMEDA report is only valid for the useful life time of a D30. 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 calculated Safety Integrity Level will not be achieved.

3.5 SIL Capability

3.5.1 Systematic Integrity

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3 Capability. These 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 end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

The product is a Type A Device. Therefore based on the SFF between 60% and 90%, when it is used as the only component in a final element subassembly, a design can meet SIL 2 @ HFT=0.

When the final element assembly consists of many components (this device, actuator, valve body, quick exhaust valve, etc.) 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 D30.

3.6 Connection of the D30 to the SIS Logic-solver

The device is connected to the safety rated logic solver which is actively performing the safety function as well as automatic diagnostics designed to diagnose potentially dangerous failures within the SIF, (i.e. partial valve stroke test).

3.7 General Requirements

The system’s response time shall be less than process safety time. The device will move to its safe state in less than 3 seconds under specified conditions.

All SIS components including the D30 must be operational before process start-up.

User shall verify that the D30 is suitable for use in safety applications by confirming the D30 nameplates are properly marked.

Personnel performing maintenance and testing on the D30 shall be competent to do so.

Results from the proof tests shall be recorded and reviewed periodically.

The useful life of the D30 is discussed in the Failure Modes, Effects and Diagnostic Analysis Report.

4 Installation and Commissioning

4.1 Installation

The valve positioner must be installed per standard practices outlined in the Installation Manual.

The environment must be checked to verify that environmental conditions do not exceed the ratings.

The valve positioner must be accessible for physical inspection.

4.2 Physical Location and Placement

The valve positioner shall be accessible with sufficient room for pneumatic connections and shall allow manual proof testing.

Pneumatic piping to the valve shall be kept as short and straight as possible to minimize the airflow restrictions and potential clogging. Long or kinked pneumatic tubes may also increase the valve closure time. Electrical leads should not be excessively long, thin, or segmented, nor inappropriately connected to the D30 circuit board resulting in excessive effective lead impedance.

The valve positioner shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of pneumatic and electrical connectors and the integrity of the valve positioner subsystem. One solution is to use remote mounting of the D30 with a remote mount bracket and a PMV F5 potentiometer/transmitter box on the valve actuator. Another solution is that the vibration should be reduced using appropriate damping mounts.

4.3 Pneumatic Connections

Recommended piping for the inlet and outlet pneumatic connections to the valve positioner is 1/2" stainless steel or PVC tubing. The length of tubing between the valve and the valve positioner, shall be kept as short as possible and free of kinks.

Only dry instrument air filtered to 50 micron level or better shall be used.

The process air pressure shall meet the requirements set forth in the installation manual.

The process air capacity shall be sufficient to move the valve within the required time.

5 Operations and Maintenance

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within D30 that are not detected by any automatic diagnostics of the system. The primary 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 D30 is applied. The proof tests must be performed more frequently than 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. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to PMV Automation AB.

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Send a signal to the final element configuration to perform a full stroke and verify that this is achieved.
3	Inspect the valve for any visible damage or contamination.
4	Record any failures in your company's SIF inspection database.
5	Remove the bypass and otherwise restore normal operation.

Table1: Recommended Proof Test

This test will detect >70% of possible DU failures in the valve for the Full Stroke options. (For the Tight Shutoff and Open to Trip options the proof test coverage is >25%, and > 90% respectively).

The person(s) performing the proof test of a D30 should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures. No special tools are required.

5.2 Proof test with automatic partial valve stroke testing

An automatic partial valve stroke testing scheme that performs a full stroke of the isolation valves and measures valve movement timing will detect most potentially dangerous failure modes. It is recommended that a physical inspection (Step 2 from Table 1) be performed on a periodic basis with the time interval determined by plant conditions. A maximum inspection interval of five years is recommended.

5.3 Repair and replacement

Repair procedures in the D30 Installation, Operation and Maintenance manual must be followed.

5.4 Useful Life

The useful life of a typical valve body and actuator is 10 to 15 years, or 10,000 cycles. The valve positioner has a shorter life time due to environmental factors, but a higher cycle limit due to the robustness of the positioner circuit board and the positioner air pilot valve.

5.5 Manufacture Notification

Any failures that are detected and that compromise functional safety should be reported to PMV Automation AB. Please contact PMV Automation AB customer service.

6. Status of the Document

6.1 Releases

Version:	1
Revision:	2
Version History:	V1, R1: Released, June 27, 2019
	V1, R2: Released, August 5, 2019
Authors:	alundgren@flowserve.com
Review:	V1, R1: R. Wedin; June 27, 2019
Release status:	Released

6.2 Future Enhancements

At request of project.

6.3 Release Signatures

S. Anders Lundgren, R&D Engineer, PMV Automation AB

Name, Title

R. Wedin, R&D Engineer, PMV Automation AB

Name, Title

Name, Title

FCD PMENDS0030-01-A5 09/19

To find your local Flowserve representative:

To find your local Flowserve representative please use the Sales Locator

System found at www.flowserve.com

PMV Automation AB
Korta Gatan 9
SE-171 54 SOLNA
SWEDEN
Phone: +46 (0)8-555 106 00
E-mail: infopmv@flowserve.com

PMV USA
14219 Westfair West Drive
Houston, TX 77041, USA
Phone: +1 281 671 9209
Fax: +1 281 671 9268
E-mail: pmvsales@flowserve.com

Flowserve Flow Control
Burrell Road, Haywards Heath
West Sussex RH16 1TL
Phone: +44(0)1444 314400
E-mail: pmvuksales@flowserve.com

Flowserve Flow Control Benelux
Rechtzaad 17
4703 RC Roosendaal
THE NETHERLANDS
Phone: +31 (0) 30 6771946
Fax: +27 (0) 30 6772471
E-mail: fcbinfo@flowserve.com

Flowserve Flow Control GmbH
Rudolf-Plank Strasse 2
D-76275 Ettlingen
GERMANY
Phone: +49 (0) 7243 103 0
Fax: +49 (0) 7243 103 222
E-mail: argus@flowserve.com

Flowserve Corporation
No. 35, Baiyu Road
Suzhou Industrial Park
Suzhou 215021, Jiangsu Province,
PRC
Phone: +86-512-6288-1688
Fax: +86-512-6288-8737

Flowserve (China)
585, Hanwei Plaza
7 Guanghau Road
Beijing, China 100004
Phone: +86 10 6561 1900

Flowserve Pte Ltd
No. 12 Tuas Avenue 20
Singapore 638824
Phone: +65 6879 8900
Fax: +65 6862 4940

Flowserve do Brasil Ltda
Rua Tocantins, 128 - Bairro Nova Gerti
São Caetano do Sul,
São Paulo 09580-130 Brazil
Phone: +5511 4231 6300
Fax: +5511 4231 6329 - 423