FISHER 785C Series – Double Acting Pneumatic Actuators -

FISHER 785C SIL Safety Manual

INDEX

1. INTRODUCTION 3
2. ACRONYMS 3
3. FUNCTIONAL SPECIFICATION 4
4. PRODUCT DESCRIPTION 5
4.1 FISHER 785C double acting pneumatic linear actuator general description 5
4.2 FISHER 785C actuator working principle 6
5. SERVICE CONDITION LIMITATIONS (LIMITATION OF USE) 7
6. EXPECTED LIFETIME 8
7. FAILURE MODES AND ESTIMATED FAILURE RATES 9
8. PERIODIC TEST AND MAINTENANCE REQUIREMENTS 10
8.1 General 10
8.2 Full Stroke Test (Proof Test) 10
8.3 Diagnostic Coverage / Proof Test Coverage 13
8.4 Partial Stroke Test 13
8.5 Partial Stroke Diagnostic Coverage / Test Coverage 16
8.6 Periodic Maintenance 16
9. CLASSIFICATION 17
10. MRT 17
11. ARCHITECTURAL CONSTRAINTS 17
12. COMMON CAUSE FACTORS 18
13. SYSTEMATIC CAPABILITY 18
14. MANUFACTURER NOTES 18

1. INTRODUCTION

This safety manual provides essential information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing Actuator Series FISHER 785C. This manual provides necessary requirements for meeting the IEC 61508:2010 (parts 1 to 7) or IEC 61511 functional safety standards.

2. ACRONYMS

FMEDA: Failure Modes, Effects and Diagnostic Analysis

HFT: Hardware Fault Tolerance (ref: 7.4.4 of IEC 61508-2:2010)

PFD_{AVG}: Average Probability of dangerous Failure on Demand (ref: 3.6.18 of IEC 61508-4:2010)

SFF: Safe Failure Fraction, property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures (ref: 3.6.15 of IEC 61508-4:2010)

SIF: Safety Instrumented Function, safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

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. (ref: 3.5.8 of IEC 61508-4:2010)

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).

3. FUNCTIONAL SPECIFICATION

The safety function performed by Fisher actuator series FISHER 785C is defined as follows:

1. *The actuator performs the safety function on demand if it delivers a full stroke (± tolerance) driven by the piston of cylinder, powered by the specified medium working pressure.*

NOTES:

- considering the functioning of the actuator to perform the safety function(s), the safety functions "stem extended" and "stem retracted" can be considered equivalent.

The choice of the safety function to be implemented is responsibility of the system integrator.

FISHER 785C actuator is intended to be part of the final element subsystem as defined per IEC 61508:2010. The achieved SIL level of the designed function must comply with the project specification and must be submitted to the system integrator.

The final control element subsystem needs to be sized properly to assure that its operating time is equal or less than the time required to reach a safe state.
FISHER 785C actuator will move the valve to its safe state in equal or less than the required SIF's response time under the specified conditions.

4. PRODUCT DESCRIPTION

4.1 FISHER 785C double acting pneumatic linear actuator general description

FISHER 785C low pressure pneumatic double acting linear actuator series is engineered and is manufactured to provide safe operation for any linear application such as wedge gate and through conduit gate valves, in both On-Off and Modulating Heavy duty service. Simplicity, reliability and economy are at the top of the list of design parameters.

Supply pressure is maximum 12 bar-gauge, accepting air, nitrogen or sweet gas.

Supported standard ambient temperature ranges from -30°C to +100°C, special versions are available for applications outside this temperature range.

The actuator is composed of a pneumatic cylinder and a mounting pedestal complete with a joint for the coupling to the valve stem of actuator output stem. The actuator pedestal has a flange with threaded holes to fix the actuator to the valve.

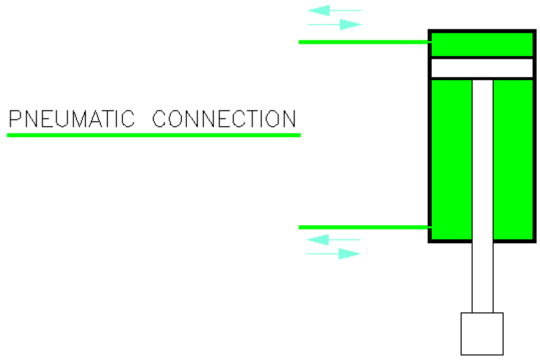
FISHER can supply different types of control system following Customer's requirements.

Picture 1: FISHER 785C Actuator Overview

4.2 FISHER 785C actuator working principle

FISHER 785C actuator working principle is simplified in the following Picture 2.

In the normal operating situation instrument air is supplied to the actuator's open (close) chamber of the pneumatic cylinder: the cylinder piston stroke causes the actuator operation and the consequent valve movement to the open (close) operational position. Upon a demand, the pneumatic air is exhausted from the open (close) chamber of the cylinder to the ambient, and the close (open) chamber of the cylinder is fed by instrument air: the actuator performs the closing (opening) operation driven by the cylinder piston, and the valve moves from the open (close) position to the close (open) position (safety-related position).



Picture 2: FISHER 785C actuator working principle scheme

5. SERVICE CONDITION LIMITATIONS (LIMITATION OF USE)

The designer of an SIF must check that the product is rated for use within the expected application limits. The operating conditions limits strongly depend on the actuator type and on its construction materials.

Operating pressure values are defined for each actuator.

Temperature limits are the following:

- Standard ambient temperature range: -30°C to +100°C
- Extended ambient temperature range: -60°C to +180°C (special versions)

Supply medium: instrument air, nitrogen or sweet gas (sour gas special version is available).

If FISHER 785C actuator is intended to be used outside the application limits or with incompatible materials, the reliability data provided in the present document are invalid.

- The actual environmental conditions are included on the actuator nameplate
- The chose values are valid for the lifetime specified in par. 6.

Manual override

Normally, for larger valves, the FISHER 785C actuators can be fitted with one of the following types of manual overrides:

- MHW jackscrew manual override type (direct action) that it can be engaged/disengaged by manual lever
- MHP Hydraulic manual override that it can be engaged/disengaged by manual lever

With reference FISHER 785C actuator, the mechanical manual override can be done with three configuration depending of the actuator size.

The use of a manual override is not recommended in a SIL classified application, as it results in a bypass of the safety function.

In case the manual override is used, the following requirements must be fulfilled, or the Functional Safety Certification will become invalid:

1. The users authorized to operate on the actuator shall be skilled personnel;
2. The maximum duration of bypass shall be defined (responsibility of the final user).
3. If necessary, compensatory measures to allow the safe operation of the process shall be defined (responsibility of the final user).
4. Before selecting remote operating mode control of actuator, the manual override must be disengaged according to IOM Manual.

The position selected (remote/automatic control or local / manual control) can be achieved with a specific technical solution that does not allow to reach an intermediate position lever's and avoids unintentional activation.

5. The engagement of the manual override shall be signalled, at least locally, according to IOM Manual. As optional request from final user, to determine if the manual override is engaged, an electrical signal using contact switching can be provided to communicate the status to the control room.

Manual handwheell	
Hydraulic manual hand pump	

To ensure that the hand pump has been correctly disengaged after a manual override operation, the following test shall be completed:

- restore the manual lever to remote position;
- verify the functionality performing a test from remote control (es. partial stroke test).

6. EXPECTED LIFETIME

Actuators lifetime strongly depends on operating conditions and on construction materials.
For normal service conditions the expected lifetime of FISHER 785C actuators can be estimated in approximately 25 years with planned maintenance.

7. FAILURE MODES AND ESTIMATED FAILURE RATES

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) integrated with field feedback according to IEC 61508-2 par 7.4.4.3.3. has been carried out in order to detail all failure rates and failure modes of FISHER 785C actuators.

According to D.2.2 of IEC 61508-2:2010 Annex D, the estimated failure rates of the failure modes that result in a failure of the safety function are quoted in the SIL certificate(s)

Please refer to the values included in the latest valid version of SIL certificate(s) (available upon request sent to Fisher)

Notes:

- No internal diagnostic is included in the device
- The failure rates are guaranteed:
    - For the service conditions listed in par. 5
    - For the expected lifetime declared in par. 6
    - Considering the periodic test and maintenance included in par. 8

The failure rates are determined performing a FMEDA based on the failure rates of components taken from industrial databases (NPRD-2016/FMD97/2016, EXIDA E&MCRH and NSWC-2011), integrated with field feedback using the Bayesian statistical approach mentioned in IEC 61508-2 Par. 7.4.4.3.3.

The system for reporting failures is based on field feedback from end users, with:

- identification of the claim/failure
- root cause analysis to identify cause and responsibility of the failure
- identification of the possible effect of the failure on the Safety Function
- classification
- improvement design
- of the failure considering the failure categories of IEC 61508-2 (Safe, Dangerous, No Effect)

Customer Service, Quality and Technical Department are responsible for the procedure, according to the respective role.

The requirements in IEC 61508-2 paragraphs 7.4.10.1 – 7.4.10.7 are fulfilled and assessed by Third Party.

8. PERIODIC TEST AND MAINTENANCE REQUIREMENTS

8.1 General

Installation, commissioning and maintenance and repair works should be carried out by qualified staff. A non-conforming assembly could be the source of serious accidents.

Please consider that the information in this paragraph are relevant only to reliability tests; please refer to FISHER 785C *Double acting pneumatic linear actuator Use and maintenance manual* (Fisher document D104483X012) for detailed information about product maintenance, handling and storage.

Diagnostic tests may be executed to increase the system reliability.

"On site" tests depend on Project/Plant facilities/requirements; however, a functional test must be executed on site, before actuator usage.

8.2 Full Stroke Test (Proof Test)

The "Full Stroke Test" ("On line") must be performed to satisfy the PFD_{AVG} value.

The Full Stroke Test frequency has to be defined by the final integrator according to the PFD_{AVG} value to be achieved.

Full Stroke Test procedure:

1. Operate the actuator to perform No. 2 complete open/close cycles (operate the actuator to perform a full stroke);
2. Check that the actuator operates the valve correctly and within the required operating times (e.g. check automatically via Logic Solver the correct movement of the actuator);
3. Compare the results with the ones stored during SAT activities;
4. Record the test results in your company's SIF database;
5. Restore the normal operation.

The procedure can be performed manually or automatically. In the following, for both cases, the following points are listed:

- Parameters to be measured
- Instruments to be used
- Failure modes detected
- Diagnostic coverage/proof test coverage

Parameters to be measured:

The following parameters have to be measured for an effective Full Stroke Test:

- linear position of the shaft;
- Time necessary to reach to final position;
- Output thrust (as indirect measure, by means of the of pressure measurement in the cylinder chamber)

NOTE:

- Not all parameters are needed, but the following combinations can be used:
  1. Measurement of linear position as function of time (pressure measurement is optional)
  2. Measurement of cylinder chamber pressure as function of time
  3. Verification of final position achievement in the established maximum time.

Instruments / equipment to be used for the test:

Quantity	**Instruments / equipment** **Automatic Procedure**	**Manual Procedure**
Linear position of the shaft	Case A: use of a Logic Solver: 1. Limit switches box, or 4÷20 mA position transmitter 2. Digital Input Module / Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 4. Limit switches box, or 4÷20 mA position transmitter 5. PST device with integrated SW function	1. Limit switches box, with visual indication 2. Skilled and trained personnel
Time necessary to reach the final position	As above	1. Chronometer 2. Skilled and trained personnel

Quantity	Instruments / equipment	
	Automatic Procedure	**Manual Procedure**
Actuator thrust (Pressure in the cylinder)	Case A: use of a Logic Solver: 1. Pressure transmitter connected to the cylinder chamber 2. Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Pressure transmitter connected to the cylinder chamber 2. PST device with integrate SW function	Skilled and trained personnel (to check audible partial sticking)

Failure mode detectable by the test:

Component	Detectable failure modes	
	Automatic Procedure	**Manual Procedure**
Head/end flange / bolts	Breakage Unscrewing	As per automatic procedure
O-Rings	Breakage => External leakage	As per automatic procedure
Pneumatic Cylinder		
Piston	Sticking	As per automatic procedure
Rod	Breakage	As per automatic procedure

NOTES:

- The ones listed above are the major failure modes of the main components
- In case of manual procedure, the detectable failure modes are the same as per automatic procedure. The test coverage is lower than the one for automatic mode, due to the human factor.
- The manual procedure cannot be considered as diagnostic.

8.3 Diagnostic Coverage / Proof Test Coverage

Considering the application of the above described Full Stroke Test procedure, the "Test Coverage", in case of automatic procedure, can be considered > 99%.

In case of manual procedure the "Test Coverage" shall take into account also the test imperfection and the reliability/competence of the operator.

Note:

- if the test is automatic, then the Test Coverage is PTC, but can also considered as DC
- if the test is manual, then the Test Coverage is PTC, but cannot be considered as DC

8.4 Partial Stroke Test

The "Partial Stroke Test" ("On line") can be performed to improve the PFD_{AVG} value.

For the execution of a partial stoke test the actuator performs a partial open-close cycle operation, typically a 15 %-25% of trip of the valve, in order to check the correct functioning of the actuator and the correct movement of the valve (not sticking and able to move).

In case of FISHER 785C, a specific operating diagram can be used, to allow the performing of PST without testing the pneumatic quick exhaust valve.

The PFD_{AVG} values quoted in SIL certification document are relevant to indicated "Partial Stroke Test" intervals.

Partial Stroke Test procedure:

1. Operate the actuator to perform N°2 partial open/close cycles, to verify the correct functioning of the actuator/valve assembly;
2. Verify that the partial stroke manoeuvre was performed correctly and within the expected time;
3. Inspect the actuator components for any leakages (internal and external).

The procedure can be performed manually or automatically. In the following, for both cases, the following points are listed:

- Parameters to be measured
- Instruments to be used
- Failure modes detected
- Diagnostic coverage/proof test coverage

<u>Parameters to be measured:</u>

The following parameters have to be measured for an effective Partial Stroke Test:

- Linear position of the shaft;
- Time necessary to reach to final position;

- Output thrust (as indirect measure, by means of the of pressure measurement in the cylinder chamber)

NOTE:

- Not all parameters are needed, but the following combinations can be used:
  1. Measurement of linear position as function of time (pressure measurement is optional)
  2. Measurement of cylinder chamber pressure as function of time
  3. Verification of final position achievement in the established maximum time.

The parameters to be measured depends upon the partial stroke test system available.

<u>Instruments / equipment to be used for the test:</u>

The Partial Stroke Test can be executed in the following way:

1. Using commercial PST device, such as Biffi IMVS, measuring/verifying:
   a) Measurement of linear position as function of time (pressure measurement is optional)
   b) Measurement of cylinder chamber pressure as function of time
   c) Verification of final position achievement in the established maximum time.
2. By means of Logic Solver, measuring/verifying:
   a) Measurement of linear position as function of time (pressure measurement is optional)
   b) Measurement of cylinder chamber pressure as function of time
   c) Verification of final position achievement in the established maximum time.
3. By means of a manual PST system manufactured by Fisher (slightly different systems can be available: please make reference to the documentation of the specific project)

Quantity	Instruments / equipment	
	Automatic Procedure	**Manual Procedure**
Linear position of the shaft	Case A: use of a Logic Solver: 1. Limit switches box, or 4÷20 mA position transmitter 2. Digital Input Module / Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 4. Limit switches box, or 4÷20 mA position transmitter 5. PST device with integrate SW function	1. Limit switches box, with visual indication 2. Skilled and trained personnel
Time necessary to reach the final position	As above	1. Chronometer 2. Skilled and trained personnel
Output thrust (Pressure in the cylinder)	Case A: use of a Logic Solver: 1. Pressure transmitter connected to the cylinder chamber 2. Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Pressure transmitter connected to the cylinder chamber 2. PST device with integrate SW function	Skilled and trained personnel (to check audible partial sticking)

Failure mode detectable by the test:

Component	Detectable failure modes	
	Automatic Procedure	**Manual Procedure**
Head/end flange / bolts	Breakage Unscrewing	As per automatic procedure
Rod	Breakage	As per automatic procedure
Container	Total Breakage	As per automatic procedure
Pneumatic Cylinder		
Piston	Sticking	As per automatic procedure
O-Rings	Breakage => External leakage	As per automatic procedure

NOTES:

- The ones listed above are the major failure modes of the main components
- In case of manual procedure, the detectable failure modes are the same as per automatic procedure. The test coverage is lower than the one for automatic mode, due to the human factor
- The manual procedure cannot be considered as diagnostic. The test can be considered as "non-perfect Proof Test", and can be considered in the estimation of PFD_{AVG}, while it is not considered for the estimation of SFF

8.5 Partial Stroke Diagnostic Coverage / Test Coverage

Considering the application of the above described Partial Stroke Test procedure, for all automatic methods indicated, the "Diagnostic Coverage" can be considered >90%.

In case of manual procedure the "Test Coverage" shall take into account also the test imperfection and the reliability/competence of the operator.

8.6 Periodic Maintenance

FISHER 785C actuators are designed to operate long-term in heavy-duty operating conditions, without maintenance needs. Periodicity and regularity of inspections is particularly influenced by specific environmental and working conditions. They can be initially determined experimentally and then be improved according to actual maintenance conditions and needs.

Anyway, every two years of operation an inspection is required: for the relevant procedures please refer to FISHER 785C *Double acting pneumatic linear actuator Use and maintenance manual* (Fisher document D104483X012).

9. CLASSIFICATION

FISHER 785C actuators are classified **Type A** according to 7.4.4.1.2 of IEC 61508-2:2010.

10. MRT

The MRT of the device is 24 hours.

Note: The MRT is estimated considering that the required spare parts are available on site, and considering the availability of skilled personnel for maintenance equipped with adequate tools and materials.

11. ARCHITECTURAL CONSTRAINTS

For the evaluation of the conformity to the requirement of Hardware safety integrity architectural constraints of the standard IEC 61508, both Route 1H and Route 2H are used.

<u>Route 1H</u>

- The device has a single channel configuration, HFT=0
- According to IEC 65108 definitions (in particular definitions 3.6.8 and 3.6.13 of IEC 61508-4), no Safe Failures are possible in a Single Acting actuator: each failure mode of the actuator itself shall be classified as "Dangerous" or "No Effect" (failures which can generate the spurious operation of the safety function are only external to the actuator itself, or are related to components that "plays no part in implementing the safety function", e.g. components of the pneumatic cylinder, and so, according to definition 3.6.13 of IEC 61508- 4, they cannot be used for the calculation of the SFF): hence <u>λ_S=0 for each type of Single Acting actuator</u>.

For this reason, according to definition 3.6.15 of IEC 61508-4, we have:

- SFF=0 without external diagnostic tests;
- SFF>0 with external diagnostic tests, carried out according to definition 3.8.7 of IEC 61508-4, and according to what written in Par. 8 above[1] (see the same paragraph for the SFF / DC reachable).

<u>Route 2H</u>

The application of Route 2H ("proven in use approach") is evaluated according paragraphs 7.4.10.1÷7.4.10.7 of IEC 61508-2. Evidence was identified for each specific point.

As the device is classified "Type A", no requirements for SFF are given for Route 2H.

[1] The diagnostic test shall be performed considerably more often (at least 10 times) than the demand of the safety function.

In conclusion:

The device can be used in single channel configuration up to:

- SIL 2 without external diagnostic tests
- SIL 3 considering external diagnostic tests

12. COMMON CAUSE FACTORS

The product has a single channel configuration, HFT=0.

The β factors can be used when performing PFD_{AVG} calculations for redundant architectures.

The estimated values for the Common Cause factors are:

- $\beta=\beta_D=0{,}05$

NOTES:

The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to IEC 61508 Part 6, Table D.5.

The above value is calculated in the hypothesis of redundancy without diversity

13. SYSTEMATIC CAPABILITY

The systematic capability[2] of FISHER 785C actuators is **3**.

This systematic capability is guaranteed only if the user:

1) uses the actuator according to the instructions for use;
2) uses the device in appropriate environment (limitation of use).

14. MANUFACTURER NOTES

1) 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} 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.
2) When using a FISHER 785C actuator in a redundant configuration, a common cause factor of 5% should be included in the Safety Integrity calculations.
3) Any failures that are detected and that compromise functional safety should be reported to Fisher. Please contact Fisher customer service or your local service representative.

[2] For the definition of systematic capability see 3.5.9 of IEC 61508-4:2010

FISHER™

EMERSON™