cowan dynamics

SIL Safety Guide

Series AT

Double-Acting Pneumatic Actuators

cowan dynamics

Table of Contents

1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the *Series AT pneumatics cylinders.* 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 Series AT cylinders 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 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 safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year and no greater than twice the proof test frequency.
High demand mode	Mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year or greater than twice the proof test frequency.
Continuous Mode	Mode where the safety function maintains the EUC in a safe state as part of normal operation.

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.
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:

Cowan Dynamics Inc.

6194 Notre Dame West

Montreal, QC, Canada H4C 1V4

Phone:514-341-3415

Fax:514-341-0249

WEB site : www.cowandynamics.com

Email: SIL@cowandynamics.com

1.4 Related Literature

Hardware Documents:

- *Maintenance Manual for Pneumatic Valve Actuators Series AT*
- *Series AT Product brochure*

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 Series AT are pneumatic actuators with integrated position transducer. Series AT actuators are designed with a dual or triple gland seals and high strength carbon fiber barrel. The retaining bushing is removable without dis-assembling the actuator. The Series AT is available with piston rod diameters from 1" to 5-1/2".
See Installation and Maintenance Manual for additional setup and configuration details.

3 DESIGNING A SIF USING MANUFACTURER PRODUCT

3.1 Safety Function

The safety function of the double acting linear pneumatic actuator is to mechanically move the attached field device based on the application of pressure at one port and exhaust to the other.

The *Series AT* 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.

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 *Maintenance Manual for Pneumatic Valve Actuators Series AT* for environmental limits.

3.3 Application Limits and Restrictions

The materials of construction of a *Series AT* are specified in the Cowan Dynamics Inc. Series AT Brochure. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the *Series AT* 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 *Cowan Dynamics Inc.* 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 *Series AT* and its failure rates.

When using *Series AT* 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 are only valid for the useful life time of *Series AT.* 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.

3.5 SIL Capability

3.5.1 Systematic Integrity

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

3.5.2 Random Integrity

The *Series AT* is a Type A Element. Therefore, a design can meet SIL 2 @ HFT=0 when the *Series AT* is used as the only component in a SIF subassembly.

When the SIF consists of many components 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 *Series AT.*

3.6 General Requirements

The system's response time shall be less than the process safety time.

All SIS components including the *Series AT* must be operational before process start-up.

User shall verify that the *Series AT* is suitable for use in safety applications by confirming the *Series AT*'s nameplate is properly marked.

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

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

4 INSTALLATION AND COMMISSIONING

4.1 Installation

The *Series AT* 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 *Series AT* location and placement must be accessible for physical and/or visual inspection and allow for manual proof testing.

5 OPERATION AND MAINTENACE

Your Cowan Dynamics Inc. actuator has been designed to give you trouble free performance with a minimum of maintenance. Periodic inspection and replacement of seals, when required, is recommended in order ensure continuing product safety and reliability. Inspection and seal replacement intervals depend on your specific operating conditions.

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within *Series AT* 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 *Series AT* 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.

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 *Cowan Dynamics Inc.* The suggested proof test consists of a full stroke of the valve, see Table 1. For the 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.

This test will detect 90% of possible DU failures in the Series AT.

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

It is recommended that a physical inspection (Step 3 from Table 1) be performed on a periodic basis with the time interval determined by plant conditions.

Table 1: recommended proof test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the signal/supply to the actuator to force the actuator and valve to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time.
3.	Re-store the supply/signal to the actuator and inspect for any visible damage or contamination and confirm that the normal operating state was achieved.
4.	Inspect the valve for any leaks, visible damage or contamination.
5.	Remove the bypass and otherwise restore normal operation.

5.2 Repair and replacement

Repair procedures in the *Maintenance Manual for Pneumatic Valve Actuators Series AT* must be followed.

5.3 Useful Life

A useful life period of approximately 10 years is expected for the Series AT. Based on general filed data a product life of approximately 20 years is expected for the Series AT if the lower level components are renewed before the end of their useful life and the device is maintained per manufacturer's instructions.

5.4 Manufacturer Notification

Any failures that are detected and that compromise functional safety should be reported to *Cowan Dynamics Inc.* Please contact *Cowan Dynamics Inc.* customer service.

SIL@cowandynamics.com